UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO
LARYSSA MACEDO BRAGA

POSSÍVEIS OBSTÁCULOS LEGAIS À BLOCKCHAIN E ALGUMAS PERSPECTIVAS DIANTE DO GDPR

Juiz de Fora
2020

LARYSSA MACEDO BRAGA

POSSÍVEIS OBSTÁCULOS LEGAIS À BLOCKCHAIN E ALGUMAS PERSPECTIVAS DIANTE DO GDPR

Artigo científico apresentado à Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial à obtenção do grau de Bacharela na área de concentração de Direito, sob orientação da Profª Dra. Eliana C. Perini.

Juiz de Fora
2020

FOLHA DE APROVAÇÃO

LARYSSA MACEDO BRAGA

POSSÍVEIS OBSTÁCULOS LEGAIS À BLOCKCHAIN E ALGUMAS PERSPECTIVAS DIANTE DO GDPR

Artigo científico apresentado à Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial à obtenção do grau de Bacharela na área de concentração de Direito, submetido à Banca Examinadora, composta pelos membros:

Orientadora: Profª Dra. Eliana C. Perini

Universidade Federal de Juiz de Fora - UFJF

Prof. Dr. Wagner Silveira Rezende

Universidade Federal de Juiz de Fora - UFJF

Me. Jordan Vinícius de Oliveira

Universidade do Estado do Rio de Janeiro - UERJ

PARECER DA BANCA:

(X) APROVADA

( ) REPROVADA

Juiz de Fora, 19 de março de 2021

POSSÍVEIS OBSTÁCULOS LEGAIS À BLOCKCHAIN E ALGUMAS PERSPECTIVAS DIANTE DO GDPR

Laryssa Macedo Braga[1]

RESUMO

O Regulamento Geral sobre a Proteção de Dados (GDPR) entrou em vigor em 2018, dez anos após o advento do sistema Blockchain como uma tecnologia promissora de registro distribuído. Este artigo visa analisar esse sistema, relacionando-o com a aplicação do GDPR dada pela CNIL, autoridade administrativa francesa. Para tanto, utilizou-se pesquisa bibliográfica exploratória e dialética com análise qualitativa. Os resultados alcançados sugerem que há diversos pontos divergentes entre a Blockchain e o GDPR, demonstrando um atraso da norma em relação às tecnológias já desenvolvidas.

Palavras-chave**:** Regulamento Geral sobre a Proteção de Dados, Comission Nationale de L'Informatique et des Libertés, Blockchain, Blockchain pública, Tratamento de dados pessoais.

RÉSUMÉ

Le Règlement Général sur la Protection des Données (RGPD) est entré en vigueur en 2018, dix ans après l'avènement du système Blockchain en tant qu'une technologie prometteuse de registre distribué. Cet article a pour objectif d'analyser ce système en le reliant à l'application du RGPD donnée par la CNIL, autorité administrative française. Pour cela, une recherche bibliographique exploratoire et dialectique avec analyse qualitative a été utilisée. Les résultats obtenus suggèrent l'existence de plusieurs points divergents entre la Blockchain et le RGPD, ce qui démontre un retard de la norme par rapport aux technologies déjà développées.

Mots-clés**:** Règlement Général sur la Protection des Données, Comission Nationale de L'Informatique et des Libertés, Blockchain, Blockchain publique, Traitement de données personnelles.

SUMÁRIO

1 INTRODUÇÃO. 2 BLOCKCHAIN. 2.1. Algumas considerações. 2.2. Caracterização e funcionalidade da Blockchain. 3 PONTOS DETERMINANTES NA LEGISLAÇÃO EUROPEIA. 4 PONTOS DIVERGENTES. 5 CONCLUSÃO. REFERÊNCIAS.

[1] Graduanda em Direito pela Universidade Federal de Juiz de Fora.

1 INTRODUÇÃO

O presente artigo apresenta os pontos divergentes entre a estrutura de uma Blockchain e as disposições do Regulamento Geral sobre a Proteção de Dados (GDPR). A Blockchain, tecnologia de registro distribuído que investe na descentralização para validar transações, foi popularizada com o advento das moedas virtuais "bitcoin", em 2008, e logo atraiu a atenção dos indivíduos por conceder-lhes maior controle sobre seus dados, sem depender da confiança em um sistema financeiro equilibrado.

Dez anos depois, em 2018, entrou em vigor o regulamento europeu que dispõe sobre a proteção de dados na União Europeia. Apesar de seu objetivo ser proteger os dados pessoais dos indivíduos, concedendo-lhes maior controle sobre sua utilização, o regulamento foi concebido com base em um sistema centralizado de uso das informações.

Desse modo, a presente pesquisa procurou analisar se o sistema Blockchain e os termos do GDPR são compatíveis ou se, diversamente, existem pontos divergentes que impedem a coexistência entre eles. Essa situação é juridicamente relevante, pois ambos tratam sobre dados pessoais, que permitem identificar e discriminar os indivíduos. Destaca-se a proteção dos dados como um direito fundamental conforme o artigo 8º da Carta dos Direitos Fundamentais da União Europeia (EUROPA, 2012).

Quanto à metodologia, foi adotado o método dedutivo, conjuntamente à pesquisa bibliográfica exploratória e dialética, com análise qualitativa. Nesse sentido, a pesquisa explorou e selecionou obras que tratassem sobre o funcionamento da Blockchain e sobre as disposições do regulamento europeu. Como o GDPR é amplo e possui lacunas a serem preenchidas com a legislação de cada país, optou-se pela abordagem francesa do regulamento, dada pela *Comission Nationale de L'Informatique et des Libertés* (CNIL), autoridade administrativa independente. Tal escolha se justifica pelo fato de o regulamento ser um aperfeiçoamento da Diretiva Europeia 95/46/CE, que se inspirou na lei da França para sua estruturação.

No mais, importa destacar a preferência em caracterizar e explicar a estrutura e o funcionamento da Blockchain em benefício das demais partes do texto. A intensa dedicação ao item 2, no qual são estabelecidas as características do sistema, presta-se a auxiliar e a conduzir o leitor à compreensão do debate trazido a seguir.

2 BLOCKCHAIN

O ato de vontade geral, como a lei, abarca a formação do contrato social (ROUSSEAU, 2012). Essa é uma compreensão tradicionalmente bem tolerada em alguns estudos políticos na formação em Direito. Ainda assim, a humanidade alcança, atualmente, um momento histórico no qual o poder da tecnologia ultrapassa a regulação existente e nem toda possibilidade tecnológica é permitida ou considerada pelos legisladores.

Segundo o CEO da Sinovation Ventures e cientista da computação Kai-Fu Lee (LEE, 2019), a evolução tecnológica global passou por duas principais transições: i) da era da descoberta à era da implementação; ii) da era da especialidade à era dos dados. Na primeira grande transição, os cientistas se dedicaram a pesquisar o campo das redes neurais e a tentar reproduzir o cérebro humano em máquinas, que se traduz no aprendizado profundo e sua implementação subsequente. A partir disso, algoritmos foram utilizados de forma simples, reconhecendo padrões e aplicando esses poderes em diversas áreas.

Na segunda transição, pela qual a ciência passa neste momento, a tecnologia se especializou, e os dados têm se tornado seu aspecto central. Conforme menciona Lee, quando o poder da ciência e dos cientistas atinge seu ponto máximo, a quantidade de dados passa a determinar a potência algorítmica (LEE, 2019). Desse modo, quanto mais dados estiverem à disposição de um algoritmo, fornecendo mais exemplos de um fenômeno, mais preciso ele será. A partir dessa lógica deu-se origem ao brocardo "Data is the new oil"[2], comparando a aquisição de dados como uma nova forma de riqueza.

Em meio a esse cenário surgiu a Blockchain, uma tecnologia de registro público distribuído (*Distributed Ledger Technology*), que se popularizou com o advento dos bitcoins, uma moeda virtual idealizada por Satoshi Nakamoto como resposta à crise econômica de 2008. Para seu idealizador, o sistema financeiro precisa de um mecanismo no qual a confiança não seja seu elemento principal para processar e validar transações, como ocorre com instituições financeiras (NAKAMOTO, 2008). A partir de então, foram criados não só os bitcoins, mas também o sistema pelo qual trafegam, a Blockchain.

Para compreender a relação da Blockchain com os dados, especialmente os dados pessoais, será necessário proceder a uma breve análise do histórico desse mecanismo, bem como à sua caracterização e ao estudo de sua funcionalidade.

---

[2] "Dados são o novo petróleo", em tradução dada pela autora deste artigo. A frase foi cunhada por Clive Humby, matemático e empreendedor em ciência de dados (ARTHUR, 2013).

2.1 Algumas considerações

Conforme citado anteriormente, a tecnologia Blockchain surgiu em 2008, ano da crise do *subprime,* que iniciou nos Estados Unidos e logo causou uma onda de desemprego, alastrando-se para outros países (FRANCO e BAZAN, 2018). Como o colapso econômico foi essencial para o advento da Blockchain, faz necessário contextualizar esse período histórico.

Nos anos anteriores à crise de 2008, os bancos começaram a encontrar dificuldades para conceder empréstimos hipotecários a pessoas cujo histórico de crédito fosse bom, já que esse perfil se tornava cada vez mais raro (ANTONOPOULOS, 2014). A partir disso, começou a haver uma concessão desenfreada de créditos imobiliários para pessoas com alto risco de inadimplemento, como pessoas sem emprego fixo e sem qualquer bem registrado em seu nome (ANTONOPOULOS, 2014). Tais empréstimos eram concedidos sob a justificativa de que, caso os devedores não pagassem suas dívidas, os bancos tomariam seus imóveis (TEIXEIRA e RODRIGUES, 2019).

Os títulos de dívida hipotecária resultantes dessa operação eram, então, classificados conforme o grau de risco à inadimplência por agências de classificação ao crédito como a Moody's e a Standard & Poor's, que mantinham acordos com os bancos, e atribuíram a esses títulos a classificação de "AAA", indicando terem as dívidas alta probabilidade de serem quitadas, ou seja, indicando que os títulos eram seguros (TEIXEIRA e RODRIGUES, 2019). Consequentemente, não só pessoas físicas como também fundos de investimentos e de pensão compraram essas dívidas, que logo se revelaram ser títulos podres (TEIXEIRA e RODRIGUES, 2019).

Diante desse cenário, os devedores dos empréstimos não tiveram como quitar suas dívidas, e o inadimplemento em massa tornou impossível o pagamento aos credores-investidores (ANTONOPOULOS, 2014). A crise gerada a partir de então causou enorme desconfiança para com o sistema financeiro devido à sua falta de transparência, corroborando para a ideia de que essas instituições seriam frágeis demais para existirem em um sistema pautado na confiança (ANTONOPOULOS, 2014). Percebeu-se, portanto, que a sociedade seria refém da confiança tanto nas instituições financeiras, cuja função seria de não emprestar dinheiro para pessoas sem garantias, quanto nas agências classificadoras, que deveriam ser honestas em suas categorizações.

Visando à mudança desse sistema, Satoshi Nakamoto – que não se sabe ser o nome ou o pseudônimo de uma pessoa real – publicou um documento chamado Bitcoin: A Peer-to-

Peer Electronic Cash System[3]. Nesse documento, Nakamoto propôs, a um só tempo, a criação do bitcoins e da Blockchain. No texto, bitcoin é apresentado como um dinheiro eletrônico que permitiria pagamentos online enviados de uma parte para a outra (ponto-a-ponto), sem passar por uma instituição financeira (NAKAMOTO, 2008).

Destaca-se o fato de o bitcoin, bem como outras moedas surgidas a partir do sistema de Blockchains, ser uma moeda virtual, o que cabe conceituar. Segundo a Autoridade Bancária Europeia[4], moedas virtuais são definidas como:

> [...] uma representação digital de valor que não é emitida por um banco central ou autoridade pública nem necessariamente ligada a uma moeda fiduciária, mas é usada por pessoas físicas ou jurídicas como um meio de troca e pode ser transferida, armazenada ou negociada eletronicamente. [...] Embora alguns dos recursos se assemelhem a atividades ou produtos que já estão sob a alçada da Diretiva Europeia sobre Moedas Eletrônicas, esses produtos não se destinam a ser incluídos aqui, logo moeda eletrônica é uma representação digital de moeda fiduciária, que moedas virtuais não são. (EBA, 2014, p. 5)

As moedas virtuais como o bitcoin são, portanto, formas de pagamento sem status legal, logo não são emitidas por um banco central ou autoridade pública, tampouco são necessariamente vinculadas a moedas fiduciárias. Apesar de o sistema Blockchain ter sido descrito pela primeira vez em 1991, por Stuart Haber e W. Scott Stornetta, somente em 2008 suas características foram aperfeiçoadas de forma a permitir a transação da moeda virtual bitcoin. Apesar de os dois conceitos terem sido descritos conjuntamente, eles não se confundem. Ressalta-se, ainda, que será utilizado o termo "Bitcoin", em maiúsculo, para tratar da plataforma de pagamentos em Blockchain no qual se transfere a moeda virtual "bitcoin".

2.2 Caracterização e funcionalidade da Blockchain

Uma Blockchain, ou "cadeia de blocos", é um registro público distribuído baseado em uma estrutura de blocos encadeados por criptografia que confere imutabilidade aos dados inseridos (QUINIOU e DEBONNEUIL, 2019). Com isso, os dados gravados nesses blocos possuem a propriedade de, uma vez registrados, terem sua alteração dificultada, sendo uma ferramenta proveitosa para afastar a adulteração de documentos. Além de permitir registros e

[3] "Bitcoin: Um Sistema de Dinheiro Eletrônico Ponto-a-Ponto", em tradução dada pela autora deste artigo.
[4] "European Banking Authority" ou "EBA", em inglês.

transações de moedas, a Blockchain permite o desenvolvimento de *smart contracts*[5], contratos que se autoexecutam, conforme será tratado mais adiante.

Primeiramente, convém analisar a estrutura de um bloco. Cada bloco é composto por dados, seu código *hash* e o código *hash* do bloco anterior (FRANCO e BAZAN, 2018). Os dados inseridos na plataforma Bitcoin contêm, por exemplo, dados sobre a transação, como o remetente, o destinatário e a quantia transferida (FRANCO e BAZAN, 2018). Esses dados podem ser divididos em dados e metadados (ZAHAREWICZ, 2018). Os dados são as transações, enquanto os metadados são os códigos *hash* do bloco anterior, registros temporais, nonce – um número de 32 bits –, o *hash* do próprio bloco e a raiz da árvore de Merkle (ANTONOPOULOS, 2014). As informações inseridas em um bloco dependem do objetivo perseguido, podendo servir simplesmente para registrar atos, como para gravar um contrato que se autoexecuta.

Cada bloco contém também um código *hash*, uma mensagem criptografada cuja função é identificar um documento, como uma digital (FRANCO e BAZAN, 2018). Essa digital é composta por uma série de caracteres, com letras e números, de tamanho fixo, calculados a partir do que se consolidou chamar "função *hash*" (QUINIOU e DEBONNEUIL, 2019). Essa digital é única e visa identificar um bloco, bem como o seu conteúdo (QUINIOU e DEBONNEUIL, 2019). Por isso, toda vez que um bloco é criado, um novo *hash* é concebido e, devido ao seu papel identificador, quando alguma de suas informações é modificada, seu código *hash* também muda (FRANCO e BAZAN, 2018). Por isso, qualquer adulteração se torna explícita.

Outro elemento intrínseco a um bloco é o código *hash* do bloco anterior (NAKAMOTO, 2008). É esse elemento que cria uma "cadeia de blocos" segura, logo um bloco é conectado a outros por meio do *hash*. Em uma série de três blocos, por exemplo, existem, então dois códigos: o *hash* do bloco anterior e o seu próprio. Apenas o primeiro bloco possui um único código, o seu próprio, porquanto ele dá início a toda a cadeia, sendo também chamado de bloco "gênesis" (FRANCO e BAZAN, 2018). Não é possível, contudo, reverter um código *hash* para descobrir o conteúdo de uma mensagem original. O que se pode fazer é colocar o *hash* em um Explorador de Blockchain[6] e ter acesso os detalhes de uma transação (SOFTWARE TESTING HELP, 2021).

---

[5] "Contratos inteligentes", em tradução dada pela autora deste artigo.
[6] "*Blockchain Explorer*", em inglês.

A tentativa de adulteração do segundo bloco causaria a mudança de seu *hash*, então os blocos subsequentes se tornariam inválidos por conterem o código de um bloco não mais existente. Essa característica não é a única forma de impedir a adulteração dos blocos, posto que para computadores potentes seria muito fácil recalcular o *hash* dos blocos seguintes. Com o fim de mitigar esse incidente, as Blockchains possuem duas formas de frear a criação de novos blocos: *Proof-of-Work* (PoW)[7] e *Proof-of-Stake* (PoS)[8] (TEIXEIRA e RODRIGUES, 2019).

Essas duas formas são aplicadas através da "mineração", processo pautado na utilização de um computador com alto poder de cálculo para resolver um problema criptográfico (QUINIOU e DEBONNEUIL, 2019). Assim, minerador é a pessoa que recebe remuneração em moeda virtual – no caso da plataforma Bitcoin, o pagamento é efetuado na mesma moeda – toda vez que ele for o primeiro a resolver o quebra-cabeça criptográfico proposto pela mineração. Esse processo incidiu em uma situação na qual várias pessoas estão se juntando a piscinas de mineração[9] para aumentar sua probabilidade de resolver as criptografias propostas (WERBACH, 2018).

No PoW, como os mineradores necessitam de grande quantidade de energia e força computacional, eles recebem por utilizar seus equipamentos para validar as transações (FRANCO e BAZAN, 2018). Com isso, quanto mais potentes forem os equipamentos de uma pessoa, maior será seu "*hashrate*", que é a quantidade de *hashes* calculadas em determinado período de tempo (FRANCO e BAZAN, 2018). Com isso, quanto maior o *hashrate* de um nó-minerador (sendo "nó" um computador), maior será a probabilidade de aquele nó resolver o próximo bloco, recebendo mais recompensa. Para uma validação fraudulenta, seria necessário haver um nó-minerador com pelo menos 51% do poder computacional de todo o sistema, o que é praticamente impossível de ocorrer (WERBACH, 2018).

Apesar das vantagens do PoW, sua utilização acarreta muito uso de energia, levando os mineradores independentes a cederem cada vez mais às citadas "piscinas de mineração", juntando-se a outros mineradores. Toda a engenharia necessária pode incidir na centralização da mineração – justamente o que se pretende evitar ao retirar o poder de instituições centralizadas como os "terceiros confiáveis".

Visando escapar desse problema, o PoS se mostra como um modelo de consenso alternativo no qual os mineradores, aqui chamados de "validadores", são escolhidos

---

[7] "Prova-de-Trabalho", em tradução dada pela autora deste artigo.
[8] "Prova-de-Garantia", em tradução dada pela autora deste artigo.
[9] "*Mining pools*", em inglês, são grupos de mineradores que decidem cooperar seu poder de *hash* para aumentar suas possibilidades de receberem recompensas (WERBACH, 2018).

aleatoriamente para validar o próximo bloco (QUANTUMMECHANIC, 2011). Para se tornar um validador, o nó precisa depositar certa quantia de moedas na rede, como se fosse um depósito de segurança, e o valor depositado determina a chance de o validador ser escolhido para validar o próximo bloco (ANTONOPOULOS, 2014). A partir de então, após validar um bloco, o nó recebe taxas como recompensa. Nesse sentido, as punições por aprovar transações inválidas são maiores do que a recompensa, pois leva o nó-validador a perder parte de seu depósito.

Voltando à dinâmica dos blocos, no caso do Bitcoin, o PoW leva dez minutos para ser calculado e para adicionar um novo bloco à cadeia (NAKAMOTO, 2008). Esse mecanismo torna difícil a adulteração dos blocos posto que, ao corromper um bloco no meio da cadeia, será necessário recalcular o PoW de todos os blocos seguintes, cada um sendo calculado em dez minutos. Dessa forma, o sistema de códigos *hash* e de PoW torna difícil a fraude na Blockchain.

Além desses mecanismos, o fato de a Blockchain ser um sistema distribuído também impede atividades fraudulentas. Conforme citado no documento de Nakamoto, o sistema funciona de Ponto-a-Ponto, ou de Pessoa-a-Pessoa; então, ao entrar nele, cada nó recebe uma cópia íntegra da Blockchain (NAKAMOTO, 2008). Assim, quando alguém cria um novo bloco, é feita uma cópia para cada nó da rede (WERBACH, 2018). Nesse mecanismo, conhecido como "mecanismo de consenso", todos os nós verificam se não houve fraude no novo bloco e o adicionam à sua própria corrente (WERBACH, 2018).

Seguindo essa lógica, para uma fraude ser bem-sucedida, o fraudador terá de corromper todos os blocos da Blockchain, refazer o PoW de cada bloco e controlar mais de 51% da rede, algo praticamente impossível. É a partir de todo esse mecanismo que a Blockchain é tida como um sistema sem intermediários de confiança – uma vez que as operações ocorrem com base no consenso –, irreversível – devido à dificuldade para alterar um bloco no meio da cadeia –, compartilhado e descentralizado – já que todos têm acesso à íntegra do sistema –, além de transparente – pois todos os nós podem visualizar todos os dados inscritos nos blocos (CNIL, 2018).

É necessário, finalmente, mencionar as chaves públicas e as chaves privadas. Chave, no sistema proposto, é uma sequência de caracteres que permite assinar, criptografar e descriptografar mensagens (QUINIOU e DEBONNEUIL, 2019). Enquanto a chave pública pode ser divulgada a todos, a chave privada deve ser mantida em segredo (QUINIOU e DEBONNEUIL, 2019). Em um paralelo com o nosso sistema financeiro, a chave pública seria

representada pelos números da conta e da agência, que identificam um indivíduo, enquanto a chave privada seria a senha utilizada para acessar uma conta e transferir valores.

Superado o estudo técnico, faz-se necessário destacar a relação do Bitcoin com o anonimato das informações presentes nos blocos. Essa plataforma costuma ser amplamente difundida por conta da privacidade dos dados pessoais, uma vez que, mesmo cada bloco contendo informações sobre o remetente e o destinatário, esses dados são transformados em pseudônimos (FRANCO e BAZAN, 2018), dificultando o rastreamento da identidade dos envolvidos. É por esse motivo que a popularidade dos bitcoins se vinculou a pagamentos no mercado clandestino, notadamente na *Deep Web*[10] (FRANCO e BAZAN, 2018).

Apesar de ser, de fato, muito difícil localizar as pessoas a partir dos pseudônimos utilizados na Bitcoin, não é impossível (ANTONOPOULOS, 2014), pois sua identidade pode ser traçada através de análise forense (WERBACH, 2018). Pensando nisso, outras moedas foram e estão sendo desenvolvidas com mecanismos mais robustos no sentido de garantir o anonimato como Dash, Monero e Zcash (SETH, 2021). Ademais, mesmo utilizando a plataforma Bitcoin, outras formas foram desenvolvidas para que os usuários possam garantir o anonimato na Blockchain como a mistura de dinheiro, o roteador Tor/Onion[11] e o CoinJoin[12].

Na mistura de dinheiro é feita uma espécie de lavagem de dinheiro virtual (LEDGEROPS, 2019). Nela, os "tumblers" ou "misturadores" misturam o dinheiro de um usuário com o de outros (LEDGEROPS, 2019). Assim, após enviar seu dinheiro para o serviço, o usuário recebe de volta o dinheiro de outrem, quebrando o liame entre si e o registro originário daquela moeda.

No roteamento, por sua vez, o roteador Onion ofusca o endereço IP dos usuários quando estão online, então suas atividades ficam cobertas por camadas de criptografia (LEDGEROPS, 2019). Já Tor se trata de um software gratuito que permite a utilização do Onion não só

[10] "Internet Profunda", em tradução dada pela autora deste artigo. Trata-se de parte oculta da internet com páginas que não foram indexadas e são inacessíveis pelos mecanismos de busca (FRANKENFIELD, 2020).

[11] O roteador Tor, sigla para "The Onion Routing" ou "O Roteamento Cebola" em português, nasceu como um projeto nos anos 90 e foi registrado apenas em 2006 (TOR, 2021). Desenvolvido para funcionar em uma rede descentralizada, esse roteador se presta a camuflar as conexões dos usuários escondendo quem interage na rede (TOR, 2021). Seu objetivo é tornar as atividades privadas até mesmo de quem monitora a rede (TOR, 2021).

[12] CoinJoin é um serviço de transações idealizado pelo desenvolvedor Gregory Maxwell e publicado em um fórum em 2013. Nele, várias transações são enviadas em uma única remessa e redistribuídas para cada destinatário, tornando difícil apontar a quantia enviada por cada usuário (BINANCE, 2021).

escondendo o endereço IP do usuário, mas também bloqueando o rastreio de visitas em *websites* e a gravação de mensagens (LEDGEROPS, 2019), como se fosse um VPN[13].

Por fim, CoinJoin é um método que reúne vários pagamentos por bitcoin, de vários remetentes, em uma só transação e redistribui aos destinatários devidos (LEDGEROPS, 2019). Nesse método, a assinatura de cada transação permanece a mesma, mas como são feitas em grupos, com várias transações ao mesmo tempo, não se evidenciam a origem e o destino de cada uma. Assim, apesar de a criptografia não ser alterada, o fato de as transações se juntarem a várias outras torna mais difícil o rastreio.

Dependendo do objetivo de dado projeto, a Blockchain pode ser classificada em pública, privada ou permissionada. Conforme definição da *Comission Nationale de L'Informatique et des Libertés* ou CNIL[14] (CNIL, 2018), Blockchains públicas são abertas a todos, isto é, qualquer um pode efetuar transações e participar da validação ou mineração de blocos. Além de as transações serem transparentes para todos, o software envolvido é gratuito e de código aberto (WERBACH, 2018).

Diversamente, Blockchains privadas sofrem o controle de um ator que determina a participação e a validação em um sistema fechado (CNIL, 2018). Como Blockchains privadas são mantidas por uma autoridade, isto é, são centralizadas e seus nós devem receber permissão para participar, alguns experts entendem que o termo "Blockchain" é usado erroneamente. Para o pesquisador Konashevych (KONASHEVYCH, 2019), "Blockchain" e "privada" são oximoros, porquanto o primeiro significa "tecnologia pública descentralizada", e o segundo sugere centralização e não publicidade.

Existem também Blockchains permissionadas ou híbridas. Assim como as privadas, esse tipo de sistema define quais pessoas podem participar e validar transações, mas, conforme o caso, podem ter acesso disponível a todos ou limitado (CNIL, 2018). Diferentemente da Blockchain privada, que é controlada por uma autoridade central, nesse modelo as permissões são controladas por nós pré-definidos.

Todo esse sistema cria possibilidades para sua utilização em diversos domínios. Além da transferência global de dinheiro – em criptomoedas – sem a necessidade de câmbio, as Blockchains podem ser implementadas no que se consolidou chamar "*smart contracts*"[15]. Esses

---

[13] "*Virtual Private Network*" ou "Rede Virtual Privada", em tradução dada pela autora deste artigo, é um mecanismo que permite mascarar a atividade e a identidade de um computador escondendo seu endereço IP (KASPERSKY, 2021).
[14] "Comissão Nacional de Informática e Liberdade", em tradução dada pela autora deste artigo.
[15] "Contratos inteligentes", em tradução dada pela autora deste artigo.

instrumentos são assim chamados pois são como contratos embebidos de autoexecutoriedade, permitindo a troca de bens e serviços de forma autônoma (BARRAUD, 2018). Com isso, torna-se possível a transferência de títulos, obrigações e direitos por um meio digital seguro e imutável, como um registro administrativo.

Segundo seu idealizador, Nick Szabo, em artigo publicado originalmente na revista Extropy em 1994, a ideia de armazenar um contrato nessa plataforma é não só protegê-lo de alterações fraudulentas – em razão de um bloco não poder ser modificado –, mas também diminuir os custos de sua execução, que normalmente seria feita por terceiros (SZABO, 1994). Como esses contratos são armazenados em blocos criptografados em um sistema distribuído, qualquer tentativa de corrompê-lo seria sistematicamente invalidada pelos nós da rede.

Um contrato inteligente pode ser pensado para inúmeras situações como em um programa de financiamento conjunto. Nesse caso, um contrato receberia doações de financiadores para um determinado projeto. Caso o projeto receba a quantia esperada, o projeto é implementado. Se, ao contrário, o projeto não receber apoio suficiente, o contrato automaticamente retorna o dinheiro aos patrocinadores. Essa situação poderia ser, então, aplicada a vários negócios sem a necessidade de confiança como base para o negócio jurídico.

Outra possibilidade de aplicação do referido contrato é na compra de viagens aéreas: o indivíduo que adquire uma passagem e tem seu voo cancelado poderia receber o valor pago automaticamente, sem precisar cobrar à empresa ou iniciar uma disputa judicial. O mesmo conceito poderia ser aplicado a máquinas de vendas programadas para encomendar mais produtos após "x" compras. Ressalta-se, contudo, que até onde se desenvolveram, os *smart contracts* aplicam uma lógica simples de sistemas "se-então" (MÜLLER, 2018). Assim, o sistema aplica opções já programadas em que "se A ocorrer, então B será feito", sem abertura para subjetividades.

Além da possibilidade de autoexecução contratual, a Blockchain pode também servir para controlar informações como registros notariais, patentes, propriedades intelectuais e informações médicas (TEIXEIRA e RODRIGUES, 2019). No caso de registros, os blocos funcionariam como uma "certidão de nascimento" virtual, em que informações só poderiam ser adicionadas com novos blocos, mas não no mesmo, como já se observou por sua estrutura.

3 PONTOS DETERMINANTES NA LEGISLAÇÃO EUROPEIA

Para se compreender a legislação de proteção de dados na Europa será apresentado adiante o Regulamento (UE) 2016/679 ou Regulamento Geral sobre a Proteção de Dados (GDPR) (UNIÃO EUROPEIA, 2016). Apesar de extenso, o regulamento apresenta lacunas a serem completadas por cada país da União Europeia com suas respectivas leis nacionais. Ressalta-se que serão abordados somente os pontos do regulamento que apresentam impasses para a total utilização da tecnologia Blockchain.

O GDPR (UNIÃO EUROPEIA, 2016) foi concebido como uma evolução da Diretiva Europeia 95/46/CE (UNIÃO EUROPEIA, 1995), que reouve conceitos-chave da lei francesa *Loi Informatique et Libertés*[16] de 1978 (FRANÇA, 1978), com reforma em 2004. Por conta disso, a fonte utilizada no presente artigo para trabalhar os conceitos do GDPR é a *Comission Nationale de L'Informatique et des Libertés* (CNIL), autoridade administrativa independente responsável por regulamentar o uso de dados pessoais na França.

Primeiramente, cabe definir o que são dados pessoais no âmbito do tratamento de dados. O GDPR os define em seu artigo 4º, item primeiro como

> [...] informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular; (UNIÃO EUROPEIA, 2016)

Além disso, existe uma categoria especial de dados pessoais: os "dados sensíveis". O regulamento não os conceitua expressamente, contudo, seu artigo 4º diferencia os dados pessoais dos dados genéticos, dados biométricos e dados relativos à saúde, sendo estes dados sensíveis (UNIÃO EUROPEIA, 2016). Mais adiante, no artigo 9º, reforça-se a proteção sobre alguns dados identificados como sensíveis ao determinar que seu tratamento deva obedecer a uma segurança suplementar (UNIÃO EUROPEIA, 2016). Tais dados são relativos à origem racial ou ética, opiniões políticas, crenças religiosas ou filosóficas, adesão a sindicatos e dados genéticos ou biométricos.

[16] "Lei Informática e Liberdades", em tradução dada pela autora deste artigo.

O objetivo do regulamento, segundo sua ementa, é proteger as pessoas físicas no que tange a seus dados pessoais e seu tratamento (utilização ou consulta) por entes públicos ou privados cuja atividade alveje pessoas na União Europeia (CNIL, 2020). Para tanto, esses entes podem existir sob dois conceitos: i) responsáveis pelo tratamento e; ii) subcontratantes. O primeiro é a entidade que determina o motivo e a forma do tratamento, isto é, sua finalidade e meios. Já o segundo é quem trata dados pessoais por conta e a mando do responsável (UNIÃO EUROPEIA, 2016).

No que tange à responsabilização desses agentes, o item 2 do artigo 5º define que o responsável pelo tratamento dos dados pessoais (incluindo os subcontratantes) deve adotar, como padrão[17], medidas de proteção adequadas desde sua concepção[18], podendo demonstrar essa conformidade de forma documentada a qualquer momento (CNIL, 2020). Conforme o contexto, deverá ser tanto designado um encarregado de dados[19] quanto mantido um registro das atividades de tratamento, além de aplicada uma política de confidencialidade e uma análise de impacto na vida privada, dentre outros (CNIL, 2020). Cumpre destacar que o responsável pelo tratamento e o subcontratante são, perante quem se sinta lesado, solidariamente responsáveis. A lei francesa permite, contudo, a negociação entre esses entes, por contrato ou convenção, das responsabilidades de cada um. Assim, caso a pessoa lesada procure o ente que não se obrigou a responder por uma demanda, este poderá contactar o outro responsável para obter respostas (CNIL, 2020).

Uma das determinações legais importantes para análise é a minimização dos dados (UNIÃO EUROPEIA, 2016). Esse princípio define que os dados pessoais só devem ser tratados na medida em que forem adequados, pertinentes e limitados à necessidade para a qual foram coletados. Nenhum dado deve ser coletado e tratado, portanto, ao menos que seja estritamente necessário para a finalidade proposta.

Além disso, os dados devem ser conservados pelos responsáveis e subcontratantes por tempo limitado[20] à sua necessidade, conforme o artigo 5º do regulamento (UNIÃO EUROPEIA,

---

[17] "Privacidade por padrão", em tradução dada pela autora deste artigo para "Privacy by default" é a ideia introduzida no GDPR de que todo projeto deve ser estruturado de forma a garantir a privacidade como um padrão de funcionamento, de forma restritiva (CNIL, 2020).

[18] "Privacidade desde a concepção", em tradução dada pela autora deste artigo para "Privacy by design" é a ideia introduzida no GDPR de que todo projeto deve ser estruturado de forma a garantir a privacidade desde a sua concepção, e não apenas uma etapa a ser analisada ao final do processo (CNIL, 2020).

[19] Tradução dada pela Lei Geral de Proteção de Dados Pessoais, LGPD (BRASIL, 2018), para "*Data protection officer* (DPO)", profissional responsável por garantir a conformidade de um ente em relação à legislação de dados e atua como canal de comunicação entre os responsáveis de tratamento, os titulares dos dados e a autoridade administrativa nacional para proteção de dados.

[20] Princípio da limitação da conservação, disposto no artigo 5º do GDPR (UNIÃO EUROPEIA, 2016).

2016). A partir do momento em que os dados alcançarem seu tempo máximo de conservação para atingir finalidade previamente determinada e legítima – tempo esse que deverá também ser previsto expressamente –, eles devem ser arquivados, suprimidos ou anonimizados (CNIL, 2020). Apesar de alguns dados não poderem ser eliminados por razões de interesse público, históricos ou administrativos, cabe também à lei prever quais são essas exceções.

O indivíduo, ou "titular de dados", também faz jus a determinados direitos que garantem a ele o controle de seus próprios dados. Esses direitos são o direito de ser informado; o direito de acesso; o direito de retificação; o direito ao apagamento dos dados (ou ao esquecimento); o direito à restrição do tratamento; o direito à portabilidade; o direito de oposição e; outros direitos relativos a decisões automatizadas (SMITS, 2020). Dentre esses, são especialmente importantes o direito à retificação, o direito ao esquecimento e o direito de oposição.

O direito à retificação dos dados, disposto no artigo 16º do GDPR, dá ao titular o direito de retificar dados inexatos ou incompletos, sem demora injustificada, junto ao responsável pelo tratamento (UNIÃO EUROPEIA, 2016). O direito ao apagamento dos dados, por sua vez, dá ao titular o direito de solicitar a exclusão de seus dados pelos responsáveis, sem demora injustificada, no caso de: i) os dados deixarem de ser necessários para atingir a finalidade que motivou sua coleta; ii) o titular retirar seu consentimento, caso essa seja a principal base legal a justificar o tratamento; iii) o titular opor-se ao tratamento e não existir outra base legal que o imponha; iv) os dados forem tratados de forma ilícita; v) haver obrigação legal em apagar os dados; vi) os dados terem sido coletados em oferta de serviços a menores de idade (UNIÃO EUROPEIA, 2016).

Finalmente, o direito à oposição, disposto no artigo 21º, concede às pessoas o direito de se opor ao tratamento de seus dados a qualquer momento, por motivos particulares (UNIÃO EUROPEIA, 2016). Esse direito não significa, contudo, o direito à exclusão simples e definitiva dos dados de uma pessoa (CNIL, 2020). Se a objeção não se referir à prospecção comercial, o responsável poderá justificar eventual recusa nas seguintes situações: se houver motivo legítimo para o tratamento; se o titular tiver consentido (devendo-se retirar seu consentimento); se houver vínculo contratual entre as partes (devendo-se, então, proceder à rescisão); se houver obrigação legal para o tratamento ou se este for necessário para proteger os interesses vitais de uma pessoa natural (CNIL, 2020).

Mister salientar que, apesar de não tratar especificamente da proteção de dados, a legislação de origem romana, notadamente em sua vertente francesa, prevê a anulação de determinado negócio jurídico devido a vícios de consentimento como o erro e o dolo, dentre

outros (MÜLLER, 2018). Além do mais, não obstante o respeito às disposições contratuais se resumir ao princípio *pacta sunt servanda*, que concede segurança jurídica ao imputar força obrigatória aos contratos, esse princípio pode ser relativizado perante uma cláusula *rebus sic stantibus*, que retrata a Teoria da Imprevisão e permite adaptar contratos a acontecimentos posteriores (MÜLLER, 2018).

4 OS PONTOS DIVERGENTES

A partir da análise estrutural do sistema Blockchain e das determinações legais impostas pelo regulamento europeu, é possível perceber que ambas possuem o objetivo comum de devolver às pessoas naturais o poder sobre seus dados. Observou-se que a Blockchain – originalmente desenvolvida para ser pública – visa a suprir a necessidade de confiança dos indivíduos para com entes intermediários, indo ao encontro do regulamento europeu, cujo fim é justamente estabelecer os direitos aos quais as pessoas naturais fazem jus.

Em setembro de 2018, quatro meses após a entrada em vigor do regulamento europeu, a CNIL publicou um documento de dez páginas intitulado "Primeiros elementos de análise da CNIL | Blockchain"[21] no qual propôs soluções para a utilização de dados pessoais no contexto da Blockchain (CNIL, 2020). Como será visto adiante, as contribuições da CNIL auxiliam a conformidade do sistema no que concerne às Blockchains privada e permissionada. A forma pública, contudo, ainda se apresenta como um desafio para o Direito.

O primeiro ponto a ser tratado é a responsabilidade dos atores. Conforme anteriormente exposto, o GDPR vislumbra uma relação de duas partes, com os responsáveis pelo tratamento de dados e subcontratantes de um lado e, de outro, os titulares. Ao adaptar esses títulos, a CNIL definiu que, como os participantes de uma Blockchain inscrevem dados na cadeia de blocos e os submetem à mineração, eles podem ser considerados, nesse contexto, responsáveis pelo tratamento de dados (CNIL, 2020). Ressalta-se que a responsabilidade está atrelada somente aos nós de pessoas jurídicas e de pessoas naturais que incluam dados para fins profissionais ou comerciais. Assim, a pessoa natural a incluir dados da cadeia ignorando esses fins não é responsabilizada pelo regulamento.

A CNIL definiu, então, que todos os nós-participantes serão responsabilizados solidariamente, mas recomendou a produção de um acordo ou contrato definindo a responsabilidade pelo tratamento seja pela criação de uma pessoa jurídica comum seja pela

[21] "Premiers éléments d'analyse de la CNIL | Blockchain", em francês.

designação de um dos nós como responsável pelo grupo (CNIL, 2020). Ademais, definiu como subcontratante, por exemplo, o desenvolvedor de software, que trata os dados sob as ordens dos responsáveis (CNIL, 2020). Desse modo, em alguns casos, o minerador será considerado subcontratante, pois é ele quem valida as transações para os responsáveis (CNIL, 2020). Percebe-se, entretanto, que as soluções almejadas pela CNIL são tangíveis apenas na utilização de Blockchains privadas e permissionadas. Nas Blockchains públicas, tanto os nós são menos rastreáveis – pela utilização de pseudônimos e outras técnicas como roteadores anônimos –, como estão espalhados por vários países. Nem todo nó terá base física na União Europeia ou tratará dados de pessoas fixadas nela, isto é, nem todo nó estará em condição para que o GDPR seja aplicado.

O segundo ponto a ser examinado é o princípio de minimização dos dados juntamente à limitação temporal do tratamento. De acordo com o regulamento, só podem ser coletados os dados necessários para um objetivo definido e legítimo por tempo limitado, não se permitindo a coleta facultativa ou mesmo preventiva. No sistema Blockchain, conforme citado no item 2.2, os dados inseridos nos blocos não podem ser alterados ou excluídos, pois integram cópias em todos os nós da rede. Em sua análise, a CNIL reconhece que a Blockchain não é a tecnologia mais adaptada para tratar dados e aconselha a priorização ou de outras formas de registro ou de uma Blockchain permissionada (CNIL, 2020).

Nesse sentido, conforme já mencionado, os dados que identificam os nós-participantes, isto é, suas chaves públicas, apesar de serem pseudonimizadas, podem ser rastreadas. Por isso, a CNIL entende não ser possível minimizar ainda mais esses identificadores e que sua conservação está alinhada à duração de vida da própria Blockchain (CNIL, 2020). No tocante à carga útil dos blocos, como os documentos estocados, a CNIL apenas recomenda a aplicação da máxima "proteção de dados desde sua concepção (*by default*)" na maior medida possível para que o formato escolhido não viole direitos e liberdades individuais (CNIL, 2020).

Caso, ainda assim, dados pessoais tiverem de ser registrados em Blockchain, aconselha-se a utilização de métodos de criptografia, códigos *hash* protegidos por chaves, dentre outros meios de camuflar os dados. Não sendo essas soluções possíveis, os dados registrados poderão ser protegidos apenas por códigos *hash*, contanto que isso se justifique na finalidade do tratamento e que uma análise de impacto tenha demonstrado serem os riscos residuais aceitáveis (CNIL, 2020). Percebe-se, mais uma vez, que as recomendações da CNIL insistem ou no registro de dados pessoais fora de uma Blockchain, ou em um modelo de registro próprio de Blockchains privadas e permissionadas. Desse modo, o registro de dados pessoais ainda

apresenta desafios perante ao GDPR relativamente às Blockchains públicas, nas quais as informações podem ser vistas por todos os nós da rede, sem necessidade de uma chave privada passa conceder o acesso.

Passa-se, então, ao exame do terceiro ponto de divergência entre a norma e o sistema: os direitos dos titulares. Apesar de a Blockchain ter sido desenvolvida para restituir aos indivíduos o controle sobre seus próprios dados e o regulamento europeu conter previsões explícitas com o mesmo objetivo, o direito ao apagamento dos dados, o direito de retificação e o direito à oposição mostram-se como um impasse para a conformidade.

Em uma Blockchain, a CNIL reconhece ser tecnicamente impossível conceder o direito ao apagamento dos dados (CNIL, 2020), mas sugere a utilização de formatos que permitam tornar os dados quase inacessíveis pelos responsáveis de tratamento, como utilizar criptografia e códigos *hash* em conjunto com chaves privadas, deletando posteriormente a chave. Assim, as informações continuariam existindo, mas os responsáveis não teriam mais acesso a elas. Desse modo, aproxima-se dos efeitos da supressão de dados sem efetivamente fazê-lo.

Além disso, o direito de retificação também apresenta problemas por não ser possível alterar dados já inscritos em blocos. A CNIL orienta, então, incluir a correção dos dados em outro bloco da cadeia. Assim, um bloco posterior invalidaria o anterior (CNIL, 2020). O problema dessa solução é que os dados anteriores continuam disponíveis na cadeia, como ocorre com escrituras de imóveis. Por conta disso, a CNIL aconselha os responsáveis a recorrer ao mesmo procedimento da exclusão de dados: suprimir a chave de acesso para os dados incorretos e inserir os corretos em outra cadeia (CNIL, 2020). Essa saída também só é possível de ser implementada em Blockchains privadas ou permissionadas, pois em Blockchains públicas, como a plataforma Ethereum[22], os dados podem ser acessados por todos.

Já no que tange ao direito à oposição, a CNIL apenas sugere, mesmo em execuções automatizadas – como nos *smart contracts* –, a previsão de intervenção humana (CNIL, 2020). Com isso, os titulares de dados poderão se opor a um tratamento, e uma intervenção humana deverá tratar a questão, mesmo após inscrição de dados na cadeia e a execução contratual. O problema dessa medida é, mais uma vez, que não se adapta a Blockchains públicas. Como em Blockchains públicas os nós estão espalhados pelo mundo e não há um responsável definido pelo tratamento, a intervenção humana se torna praticamente impossível.

[22] Tanto a Bitcoin quanto a Ethereum são plataformas de Blockchain pública. A diferença entre elas é que a Bitcoin não oferece suporte para *smart contracts*, pois não faz parte de uma Blockchain programável. A Ethereum, por ser programável, possui suporte para a utilização desses contratos (OLIVA, HASSAN; JIANG, 2020).

Pode-se, pois, perceber que a recomendação principal da CNIL para a utilização de Blockchains é torná-la o mais semelhante possível ao sistema numérico centralizado já existente. Cabe lembrar, inclusive, que Blockchains privadas e permissionadas não são consideradas Blockchains por experts da área, pois se distanciam da proposta inicial de transferência Ponto-a-Ponto. Apesar de a CNIL ter tentado propor medidas para adequar o sistema à norma jurídica, essas sugestões mostram-se praticamente ineficientes por não resolverem o principal desafio jurídico para a proteção de dados: a Blockchain pública. É possível afirmar, portanto, que Blockchains privadas e permissionadas não causam grandes problemas de conformidade com o GDPR, enquanto as Blockchains públicas ainda constituem um desafio a ser ultrapassado.

Além da regulação em matéria de dados pessoais, cabe mencionar, quanto ao desenvolvimento de Blockchains para *smart contracts*, que sua natureza determinística "se-então" não deixa espaço para a ponderação de conceitos jurídicos indeterminados (MÜLLER, 2018). Por isso, além de a execução de um contrato inteligente não poder ser parada, esse sistema não consegue interpretar previsões como "dentro de um prazo razoável", "rescisão por justa causa" ou "boa-fé objetiva" (MÜLLER, 2018). Ainda não se pode conceber, portanto, a implementação desses contratos em situações que precisem considerar termos subjetivos ou mesmo a clausula *rebus sic stantibus*, ou seja, a adaptação a acontecimentos posteriores.

Por fim, a elaboração de contratos em Blockchain dificulta a proteção das partes em relação a eventuais vícios de consentimento (MÜLLER, 2018). Além de o sistema não conseguir analisar e desfazer, por si só, situações em que ocorra um vício de consentimento – dolo, erro etc. –, o fato de haver mecanismos para anonimizar os nós torna difícil ou até impossível identificar e responsabilizar pessoas físicas ou jurídicas que se utilizem desses métodos para induzir particulares em erro. Como a CNIL apenas oferece sugestões visando à proteção dos dados pessoais, caberá ao Direito, como um todo, desenvolver entendimentos específicos para salvaguardar demais direitos em uma Blockchain pública. Devido à incidência global do tema, nota-se necessária discussão jurídica de ordem internacional.

5 CONCLUSÃO

Diante das informações levantadas neste trabalho foi possível observar que, apesar de as Blockchains privadas e permissionadas não serem um impasse para a implementação do Regulamento Europeu, a Blockchain pública ainda apresenta uma estrutura difícil de ser

compatibilizada. Conforme os primeiros elementos de análise da CNIL, existem pontos nas Blockchains privada e permissionada que podem ser adaptados para se adequar ao GDPR, mas nada foi analisado em relação à Blockchain pública.

Nesse sentido, conforme a análise da CNIL, a responsabilização dos atores é possível em Blockchains privadas e permissionadas. Para tanto, os nós-participantes deverão dividir suas responsabilidades específicas em acordo ou contrato, mantendo responsabilidade solidária ante os titulares de dados. A solução não se aplica, entretanto, às Blockchains públicas, logo o rastreamento dos envolvidos é dificultado, além de os nós envolvidos poderem estar fora da jurisdição em que o GDPR é aplicável.

Ademais, ainda segundo a CNIL, relativamente à minimização e à limitação dos dados, não é possível minimizar ainda mais os dados pessoais, nem limitar seu tratamento. Por isso, devem-se priorizar outras formas de registro de dados pessoais, mas, caso não seja possível, sugere-se a utilização de uma Blockchain permissionada. Além disso, sugere-se atenção especial ao formato de registro que mais respeite a privacidade por padrão (*privacy by default*), e que, além disso, proteja os dados com criptografia e *hashes* providas de chaves privadas. Para tanto, antes da implementação do sistema escolhido, deverá ser feita uma análise de impacto. Percebeu-se que as medidas sugeridas mais uma vez não são aplicáveis às Blockchains públicas, logo os dados não são coordenados e protegidos por nós pré-estabelecidos.

No que se refere aos direitos dos titulares, como o direito ao apagamento dos dados, o direito de retificação e o direito de oposição, a análise preliminar da CNIL recomendou medidas satisfatórias para adoção em Blockchains privadas e permissionadas. Como providência análoga ao apagamento, os responsáveis devem procurar tornar os dados inacessíveis não só protegendo-os com criptografia, mas também com códigos *hash* que possuam chaves privadas, deletando as chaves em seguida. Para que se respeite o direito de retificação, deve ser feita a correção dos dados em outro bloco e devem ser tornados inacessíveis os blocos nos quais haja informação incorreta. Já quanto ao direito de oposição, propôs-se a obrigação de intervenção humana capaz de rever a utilização dos dados, mesmo que o sistema já os tenha utilizado. Tais prescrições são, mais uma vez, ineficazes para aplicação em Blockchains públicas.

Por fim, como os comandos via Blockchain são objetivos e irreversíveis, foi possível perceber sua incapacidade em interpretar conceitos jurídicos abstratos como “dentro de um prazo razoável”, além de não ser possível reverter comandos implementados por vícios de consentimento ou por respeito à cláusula *rebus sic stantibus*. Ainda há, portanto, um atraso da norma jurídica em relação às possibilidades tecnológicas já desenvolvidas. Para que esse

cenário seja superado, devem movimentar-se não só as autoridades incumbidas pela proteção de dados pessoais, mas também todo o Direito, em amplitude internacional.

REFERÊNCIAS

ABOUT: History. **Tor Project**, 2021. Disponível em: https://www.torproject.org/about/history/. Acesso em: 2 fev. 2021.

ANTONOPOULOS, Andreas. **Mastering Bitcoin.** Sebastopol: O'Reily Media, 2014. Disponível em: https://bitcoinbook.info/wp-content/translations/pt_BR/book.pdf. Acesso em: 26 jan. 2021.

ARTHUR, Charles. **Tech giants may be huge, but nothing matches big data.** The Guardian, 2013. Disponível em: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data. Acesso em: 2 mar. 2021.

BARRAUD, Boris. **Les blockchains et le droit.** Revue Lamy Droit de l'immatériel. [S.l.]: Wolters Kluwer, 2018, p.48-62. Disponível em: https://hal.archives-ouvertes.fr/hal-01729646/document. Acesso em: 7 fev. 2021.

BLOCKCHAINS Aren't Anonymous. But They Can Be. **LedgerOps**, 2019. Disponível em: https://ledgerops.com/blog/blockchains-arent-anonymous-but-they-can-be-05-01-2019/. Acesso em: 12 jan. 2021.

BLOCKCHAIN Explorer Tutorial – **What Is A Blockchain Explorer**. Software Testing Help, 2021. Disponível em: https://www.softwaretestinghelp.com/blockchain-explorer-tutorial/. Acesso em: 16 fev. 2021.

COIN Mixing and CoinJoins Explained. **Binance Academy**, 2021. Disponível em: https://academy.binance.com/en/articles/coin-mixing-and-coinjoins-explained. Acesso: em 7 mar. 2021.

COMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **Blockchain et RGPD :** quelles solutions pour un usage responsable en présence de données personnelles ? CNIL, 2018. Disponível em: https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles. Acesso em: 28 out. 2020.

COMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **L'Atelier RGPD**. Disponível em: https://atelier-rgpd.cnil.fr. Acesso em: 1 jun. 2020

COMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **Premiers éléments d'analyse de la CNIL.** CNIL, 2018. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf. Acesso em: 28 out. 2020.

EUROPEAN BANKING AUTHORITY. **EBA Opinion on 'virtual currencies'.** EBA, 2014. Disponível em:

https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1. Acesso em: 12 nov. 2020.

FRANCO, André; BAZAN, Vinícius. **Criptomoedas:** melhor que dinheiro. São Paulo: Empiricus, 2018. Disponível em: http://quartzoinvestments.com/wp-content/uploads/2019/04/Criptomoedas-ebook-v7-1.pdf. Acesso em: 14 nov. 2020.

HABER, Stuart; STORNETTA, W. Scott. **How to time-stamp a digital document.** Journal of Cryptology, Morristown, 3: 99–111, 1991. Disponível em: https://link.springer.com/article/10.1007/BF00196791#citeas. Acesso em: 9 dez. 2020.

KONASHEVYCH, Oleksii. **Why 'Permissioned' and 'Private' are not Blockchains.** SSRN, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3496468. Acesso em: 4 fev. 2021.

KRITIKOS, Mihalis. **What if blockchain offered a way to reconcile privacy with transparency?** European Parliamentary Research Service, 2018. Disponível em: https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/624254/EPRS_ATA(2018)624254_EN.pdf. Acesso em: 14 jan. 2021.

LEE, Kai-Fu. **Inteligência Artificial:** Como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos. 1ª Ed. Rio de Janeiro: Editora globo S.A.,2019.

LIPTON, Alex *et al.* **An Introduction to Smart Contracts and Their Potential and Inherent Limitations.** Harvard Law School Forum on Corporate Governance, 2018. Disponível em: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/. Acesso em: 4 mar. 2021.

MAXWELL, Gregory. **CoinJoin:** Bitcoin privacy for the real world. Bitcoin Talk, 2013. Disponível em: https://bitcointalk.org/index.php?topic=279249.0. Acesso em: 12 fev. 2021.

NAKAMOTO, Satoshi. **Bitcoin:** A Peer-to-Peer Electronic Cash System. Bitcoin, 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 7 de nov. 2020.

OLIVA, Gustavo A. *et al*. **An exploratory study of smart contracts in the Ethereum blockchain platform.** Empirical Software Engineering, 2020. Disponível em: https://link.springer.com/article/10.1007/s10664-019-09796-5. Acesso em: 22 fev. 2021.

O QUE é uma VPN e como funciona? **Kaspersky**, 2021. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn. Acesso em: 4 mar. 2021.

QUANTUMMECHANIC. **Proof of stake instead of proof of work.** Bitcointalk, 2011. Disponível em: https://bitcointalk.org/index.php?topic=27787.0. Acesso em : 8 jan. 2021.

QU'EST-CE que la blockchain ? **Blockchain France**, 2021. Disponível em: https://blockchainfrance.net. Acesso em: 18 dez. 2020.

QUINIOU, Matthieu; DEBONNEUIL Christophe. **Glossaire Blockchain.** Paris: Les Éditions de L'Immatériel, 2019. Disponível em: https://en.unesco.org/sites/default/files/blockchain_glossairefrn.pdf. Acesso em: 24 jan. 2021.

ROUSSEAU, Jean-Jacques. **Du contrat social.** Paris: Flammarion, 2012.

SETH, Shobhit. **6 Private Cryptcurrencies.** Investopedia, 2021. Disponível em: https://www.investopedia.com/tech/five-most-private-cryptocurrencies/. Acesso em : 15 jan. 2021.

SIDE, Audrey; MOLLET-VIEVILLE Benjamin; CORDIN, Augustin. **La Blockchain et la Protection des Données Personnelles.** Créteil : Université Paris Est Créteil, [2017-2018]. Disponível em: http://www.masterpia.com/wordpress/wp-content/upload/2018/06/LA-BLOCKCHAIN-ET-LA-PROTECTION-DES-DONNÉES-PERSONNELLES-VF.pdf. Acesso em: 17 jan. 2020.

SZABO, Nick. **Smart Contracts:** Building Blocks for Digital Markets. University of Amsterdam, [1996?]. Disponível em: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em: 3 fev. 2021.

TEIXEIRA, Tarcisio; RODRIGUES Carlos Alexandre. **Blockchain e Criptomoedas:** aspectos jurídicos. 1ª Ed. Salvador: Editora JusPODIVM, 2019.

UNIÃO EUROPEIA, Parlamento. Do Conselho. **Carta dos Direitos Fundamentais da União Europeia. (2016/C 202/02) do Parlamento Europeu e do Conselho**, de 07 de junho de 2016. Jornal Oficial da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em: 10 mar. 2021.

UNIÃO EUROPEIA, Parlamento. Do Conselho. **Regulamento Geral de Proteção de Dados. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Jornal Oficial da União Europeia, 2016. Disponível em: https://protecao-dados.pt/wp-content/uploads/2017/07/Regulamento-Geral-Prote%C3%A7%C3%A3o-Dados.pdf>. Acesso em: 11 dez. 2020.

VELES, Marcelo da Silva *et al.* **Bitcoin:** um Estudo sobre o Uso e Legalidade Jurídica. XVIII Mostra de Iniciação Científica, Pós-Graduação, Pesquisa e Extensão. Programa de Pós-Graduação em Administração – UCS. Universidade de Caxias do Sul, 2018. Disponível em: http://www.ucs.br/etc/conferencias/index.php/mostraucsppga/xviiimostrappga/paper/viewFile/5965/1969. Acesso em: 9 dez. 2020.

WALLACE, Amelia. **Protection of Personal Data in Blockchain Technology**. Tese (Mestrado em Direito e Informática) – Faculdade de Direito, Universidade de Estocolmo. Estocolmo, 2018. Disponível em: https://www.diva-portal.org/smash/get/diva2:1298747/FULLTEXT01.pdf. Acesso em: 1 fev. 2021.

WERBACH, Kevin. **Trust, But Verify:** why the blockchain needs the law. California: Berkeley Technology Law Journal, 2018. Disponível em: https://btlj.org/data/articles2018/vol33/33_2/Werbach_Web.pdf. Acesso em: 8 dez. 2020.

ZAHAREWICZ, Edmund J. **Blockchain and Bitcoin:** Impact on Insurance Industry. ACLI Financial & Investment Roundtable, 2018. Disponível em: https://www.acli.com/-/media/ACLI/Files/Events/FIR2018/Mon031918-BlockchainandBitcoin-EdZaharewicz.ashx?la=en. Acesso em: 1 mar. 2021.