Lei Geral de Proteção de Dados, direito ao apagamento, correção dos dados e blockchain: análise da pertinência tecnológica

Renata Barros Souto Maior Baião
Juíza de Direito no Estado de São Paulo

Sumário: 1. Introdução; 2. Lei Geral de Proteção de Dados – Lei n. 13.709, de 14 de agosto de 2018 – breves considerações; 3. Blockchain; 3.1. Qual problema a blockchain resolve?; 3.2. Classificação das redes blockchain; a) grau de centralização; b) grau de transparência; c) grau de autonomia; 3.3. Conteúdo do bloco; 4. Análise da pertinência tecnológica entre a blockchain e a Lei Geral de Proteção de Dados; 5. Sugestões para compatibilização tecnológica; 6. Considerações finais; 7. Referências bibliográficas.

Resumo: A Lei Geral de Proteção de Dados, a exemplo da *General Data Protection Regulation*, estabeleceu direitos ao titular de dados, tais como o de apagamento e correção. Paralelamente, desenvolve-se a tecnologia blockchain que, para além de viabilizar a individualização de ativos digitais como o bitcoin, registra transações de forma imutável, transparente, segura e auditável, características, em tese, incompatíveis com direitos franqueados ao titular de dados. Todavia, a depender da natureza da rede e das transações realizadas, é possível compatibilizar o exercício pleno dos direitos do titular de dados e a tecnologia blockchain.

Palavras-chave: Proteção de Dados. Tecnologia. Proteção. Apagamento. Correção. Blockchain. Compatibilidade.

1. Introdução

Dentro do universo da internet da informação, nunca foram registrados, publicados, armazenados e tratados tantos dados quanto atualmente[1].

Este universo criou um cenário no qual os indivíduos, a pretexto de uma "melhor experiência do usuário" são monitorados ao longo de seus dias e tais informações são retidas e utilizadas por empresas privadas que, com base nelas, disponibiliza publicidade direcionada ou, até mesmo, realiza experiências de cunho psicológico com seus usuários, tal como a que o Facebook fez (KRAMER; GUILLORY; HANCOCK, 2014).

Os usuários são estimulados a passar cada vez mais tempo conectados, e os dispositivos e aplicativos são especialmente desenhados para reter a atenção de cada indivíduo por longos períodos, viciando-o (ALTER, 2018, posição 157).

[1] Por exemplo, são carregadas, no Youtube, mais de 500 horas de vídeo por minuto (OSMAN, 2019).

Aos poucos, a internet da informação virou um modelo de negócio e seus usuários foram transformados em "ratinhos de laboratório", explorados para a obtenção de lucro, por meio de publicidade direcionada[2], dentre outros.

Entretanto, diversamente de um suporte físico impresso, tal como um livro, localizar informações na internet tornou-se ação simples, que possibilita a obtenção de resultados de forma instantânea e automatizada.

Com o aumento de informações disponibilizadas e da eficiência dos mecanismos de busca, identificar e acessar conteúdo de divulgação indesejada pelo particular tornou-se ação não só fácil como rápida. Além disso, em tempos de *big data*, qualquer dado é relevante, pois conversível em informação valiosa[3] para encetar os novos modelos de negócios.

Em razão disso, passou-se a questionar o universo de informações constantes na internet, o uso que poderia ser dado a ele, bem como os rastros digitais e o impacto que sua existência poderia causar na vida das pessoas.

Diante desse cenário, a teoria do direito ao esquecimento ganhou corpo e não foi ignorada pela legislação específica.

A Lei Geral de Proteção de Dados, apesar de não a referir expressamente, estabeleceu, em seu art. 18, IV e VI, o direito do titular de dados de ter seus dados eliminados por aqueles que, eventualmente, os tenham captado para tratamento, mediante o atendimento de certos requisitos.

Paralelamente e, fundado na liberdade de expressão, na liberdade financeira e no exercício do direito à privacidade, em plena crise econômica de 2008[4], Satoshi Nakamoto[5] publicou um *whitepaper* criando o bitcoin, um sistema de dinheiro eletrônico ponto a ponto (NAKAMOTO, 2008).

Satoshi Nakamoto estabeleceu, em seu *whitepaper*, os parâmetros iniciais de uma estrutura de dados organizada sob a forma de contabilidade de tripla entrada[6] que possibilitaria, a partir de 3 de janeiro de 2009[7], a transferência de um ativo digital individualizado, sem intermediação.

O *whitepaper* evidenciou ainda que os parâmetros criptográficos da rede do bitcoin, bem como a forma de realização de encadeamento das transações, tornaria seus registros imutáveis, transparentes, auditáveis, seguros, confiáveis, na medida em que são propagados para uma rede de computadores distribuída.

Os debates não tardaram a surgir, questionando a possibilidade de compatibilizar a tecnologia blockchain com alguns direitos atribuídos ao titular de dados pessoais,

[2] "Essa capacidade de identificar os mais diversos padrões de comportamentos e prever a sua recorrência no futuro é uma verdadeira 'mina de ouro' para a abordagem publicitária" (BIONI, 2018, posição 914).

[3] "Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação" (BIONI, 2018, posição 813).

[4] Em 2008, a crise financeira mundial "queimou as pontes de confiança" entre os "titãs" da indústria financeira e o público (BURNISKE; TATAR, 2018, p. 3).

[5] A identidade de Satoshi Nakamoto não é conhecida (EHA, 2017, p. 11). Apesar de pessoas se autoproclamarem Satoshi Nakamoto, nenhuma delas movimentou os bitcoins do criador do criptoativos, não sendo possível esclarecer a veracidade das informações daqueles que dizem ser Satoshi Nakamoto.

[6] Na contabilidade de tripla entrada, cada saída corresponde a uma entrada, assegurada por uma camada de validação.

[7] BLOCO gênese do Bitcoin. Disponível em: https://bit.ly/2R68Kqi. Acesso em: 7 ago. 2019.

notadamente o direito ao apagamento e o direito à correção de dados estabelecido na Lei Geral de Proteção de Dados.

É o que será enfrentado neste artigo.

2. Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018: breves considerações

O desenvolvimento de modelos de negócio voltados para a captação de dados e monitoramento de indivíduos, a fim de possibilitar uma propaganda direcionada e uma "melhor experiência do usuário", aliado às notícias de situações de monitoramento e vigilância determinaram uma maior urgência no exame do direito à privacidade e à proteção de dados e, em consequência, na elaboração da General Data Protection Regulation europeia e, no Brasil, da Lei Geral de Proteção de Dados (LGPD).

A LGPD foi claramente inspirada na legislação europeia (COTS; OLIVEIRA, 2019, p. 9), alinhando-se a um dos principais regramentos mundiais sobre o tema.

Houve um grande avanço legislativo, pois a LGPD modificou o viés interpretativo quanto à coleta de dados, concentrando na figura do titular os atos de disposição, atribuindo-lhes o caráter de irrenunciabilidade (COTS; OLIVEIRA, 2019, p. 154).

Salienta-se que, sob uma perspectiva tecnológica, a legislação é neutra. Entretanto, ao analisar-se os agentes de tratamento (art. 5º, IX, da Lei nº 13.709/2018), verifica-se que a LGPD foi elaborada considerando a centralização da operação de tratamento de dados em pessoa física ou jurídica e, em consequência, possibilitando a responsabilização na hipótese de afronta.

A tecnologia blockchain, por sua vez, é alicerçada em conceitos de distribuição e descentralização das informações como uma das formas de tornar as redes resilientes, o que, em última análise, permite que os registros nelas constantes sejam transparentes, imutáveis e auditáveis.

Tais atributos, por sua vez, levam a uma conclusão inicial — e, diga-se, precipitada — de que a tecnologia blockchain está inviabilizada pela Lei Geral de Proteção de Dados. Todavia, respeitadas as opiniões em sentido contrário, a tecnologia blockchain, observadas algumas cautelas, é sim compatível com a legislação protetiva.

3. Blockchain

Blockchain é tecnologia de propósito amplo, podendo compreender tanto o armazenamento de informações como a execução de protocolos.

Primavera de Filippi e Aaron Wright definem blockchain como banco de dados descentralizados, mantidos por uma rede distribuída de computadores, salientando a reunião de diferentes tecnologias (redes ponto a ponto, criptografia assimétrica e mecanismos de consenso) para tanto (2018, posição 234).

Michael Talbot conceitua blockchain como um banco de dados digital distribuído que utiliza tecnologia ponto a ponto, encadeada, combinada com chaves criptográficas para permitir o registro de um livro-razão de transações de forma segura, imutável, irretratável, confiável e transparente, sem ponto central de controle (2018, posição 450).

Malekan expõe uma visão sintética de blockchain, definindo-a como uma tecnologia que permite a existência de algo digital em apenas um lugar (2018, p. 2).

Paul Vigna e Michael Casey conceituam blockchain como um livro-razão digital compartilhado em uma rede descentralizada de computadores independentes, que o mantém atualizado de forma a permitir a comprovação de que os registros nele contidos são completos e incorruptíveis (2018, p. 12).

Kravchenko, Skriabin e Dubinina esclarecem tratar-se de um banco de dados que contém transações comuns entre todos os nós envolvidos na rede bitcoin, com a peculiaridade de que cada bloco confirma a integridade do bloco anterior, assegurando, em consequência, a integridade do histórico de todas as transações realizadas (2018, posição 2822).

Davis e Le Merle estabelecem que blockchains são livros-razão abertos, distribuídos e que podem registrar transações entre duas partes de forma eficiente, verificável e permanente (2019, p. 97).

Ressalve-se, entretanto, que a arquitetura peculiar da blockchain e seu estágio inicial de desenvolvimento tecnológico muitas vezes podem trazer alguma confusão entre seus conceitos e seus atributos.

Assim, a partir dos conceitos acima elencados, elabora-se uma definição mínima de blockchain[8]: conjunto de tecnologias que compõe uma estrutura de dados organizados sob a forma de contabilidade de tripla entrada[9]. Isso significa, essencialmente, que os registros desses dados são compostos pelos seguintes elementos mínimos: a) uma entrada que corresponde a uma saída; b) uma saída; c) uma camada de validação criada pela rede, que assegura a saída.

A denominação "blockchain" se originou justamente do fato de as transações serem agrupadas em blocos que, por sua vez, são encadeados de forma criptografada aos blocos anteriores. Esse recurso confere segurança às transações e imutabilidade aos registros.

Em razão de tais elementos, aliados a critérios criptográficos de encadeamento das operações, as informações registradas por meio da aplicação da tecnologia blockchain vêm revestidas de uma série de atributos, consistentes em imutabilidade, transparência, segurança e auditabilidade.

A partir de tais atributos, alcança-se o propósito da tecnologia: criar valor a partir da descentralização da criação, verificação, validação e armazenamento seguro de transações (CAMPBELL-VERDUYN, 2018, posição 1375), permitindo a individualização dos ativos digitais.

Trata-se de tecnologia em crescimento, tanto no desenvolvimento de novas soluções, como em adoção pelos mais diversos modelos de negócio, os quais, por sua vez, customizam aplicações.

Assim, diante do objeto deste estudo, é necessário ingressar também na natureza da informação armazenada na blockchain, salientando-se que há várias redes distintas, com objetivos peculiares.

[8] Frise-se: a conceituação apresentada é mínima, a fim de que possa ser aplicada nas distintas espécies de redes existentes. A tecnologia blockchain, para ser identificada como tal, deve ainda observar algumas estruturas tecnológicas que vão além do necessário para este estudo e que, por isso, não serão analisadas.

[9] Na contabilidade de dupla entrada, cada transação é representada por dois lançamentos, um a crédito, outro a débito (ETWARU, 2017, p. 41).

3.1. Qual problema a blockchain resolve?

Blockchain resolve o problema do gasto duplo no meio digital. Ou seja, desde a criação do bitcoin, é possível "gastar" um ativo digital, sem duplicá-lo. Assim, quando bitcoins são remetidos de um endereço para o outro, eles efetivamente saem da esfera de disposição do remetente, ou, em outras palavras, são "gastos".

Embora, como dito, trate-se de tecnologia ainda embrionária, os efeitos e possibilidades já se descortinam no horizonte, todas elas envolvendo um reposicionamento do intermediário.

Em comparação à transferência de bitcoins exemplificada acima – concretizada sem a interferência de intermediários –, uma transferência de quantia no sistema bancário seria realizada necessariamente mediante intervenção da instituição financeira, que verificaria a existência de saldos, regularidade documental etc.

O confrontamento das duas situações traz à luz um dos efeitos da adoção da blockchain: o reposicionamento do intermediário que, a depender do grau de centralização da rede, sequer será necessário.

3.2. Classificação das redes blockchain

Para este estudo, como não é possível analisar individualmente todas as redes existentes, será proposta classificação de redes ampla, permitindo o exame das principais questões por meio de grupos maiores, divididos conforme a seguinte classificação: a) o grau de centralização; b) o grau de transparência; c) o grau de autonomia.

a) grau de centralização:

Redes centralizadas: concentram a informação em um local, tais como aquelas que operam no sistema cliente-servidor, e, por isso, criam um ponto central de vulnerabilidade (WERBACH, 2018, posição 2472). O intermediário é mantido.

Redes descentralizadas[10]: as redes descentralizadas possuem pontos de concentração ou controle de informação. O intermediário é mantido, mas pode ser deslocado para ponta da cadeia, avaliando a informação recebida.

Redes distribuídas: as redes distribuídas não possuem pontos de concentração de informação ou centros de poder. Todos os nós da rede estão conectados entre si e atuam em conjunto, porém de forma independente e, na blockchain, possuem uma cópia do livro-razão atualizada com todas as transações (NORMAN, 2017, p. 32). O intermediário é excluído.

A distinção é relevante porque, apesar de amplamente propagado que blockchain é tecnologia que elimina o intermediário, isso não se verifica em todas as espécies de rede (WERBACH, 2018, posição 2399).

Embora exista uma clara proposta de valor na existência do intermediário para verificar a veracidade de uma informação, no caso de uma rede blockchain distribuída,

[10] Há autores que não diferenciam os termos descentralização e distribuição. Em uma perspectiva classificatória, a distribuição é a descentralização absoluta, com a remoção de todos os pontos de concentração da rede.

o intermediário será o *ledger*[11], não o criador do protocolo. Na rede blockchain distribuída, o intermediário como conhecemos é eliminado.

Já nas redes descentralizadas há pontos de controle e centralização que representam não só um intermediário como também pontos de fragilidade da rede.

Além disso, é muito comum encontrar, na literatura técnica, classificações que incluem, nas características de redes públicas, a possibilidade de qualquer pessoa delas participar, desempenhando qualquer atividade[12], elementos distintivos das redes não permissionadas. Isso ocorre porque para desempenhar todas as atribuições existentes em uma rede não permissionada é necessário ter acesso à integralidade do conteúdo do *ledger*, fazendo da rede não permissionada, assim, uma rede pública. Portanto, se qualquer pessoa pode ter conhecimento do conteúdo do *ledger* em uma rede não permissionada, a rede não permissionada é, também, pública.

b) Grau de transparência:

Redes públicas: redes cujo conteúdo pode ser acessado por qualquer pessoa.

Redes privadas: redes cujo conteúdo é restrito a usuários participantes da rede ou cujo acesso é de alguma forma controlado.

c) Grau de autonomia:

Redes permissionadas: apenas usuários autorizados podem participar da rede e é possível configurar o tipo de perfil que cada usuário terá (SWAN, 2015, p. 8). Nesta espécie, os participantes da rede já são conhecidos e "confiáveis" (BASHIR, 2018, p. 34), possibilitando-se inclusive a configuração de perfis distintos para cada um deles.

Redes não permissionadas: qualquer pessoa pode participar da rede, executar o protocolo, validar transações etc.

Tomando-se como exemplo a rede bitcoin, trata-se de rede pública, distribuída e não permissionada.

3.3. Conteúdo dos blocos

A rede blockchain é formada por blocos, que nada mais são que arquivos que registram transações realizadas em um intervalo de tempo, reunindo em sua estrutura outras informações (JUN, 2018, posição 543). Estes blocos são encadeados entre si criptograficamente, e as transações neles registradas podem variar de acordo com a destinação da rede.

Tendo em vista o estudo referente à proteção de dados, é necessário compreender o conteúdo dos blocos que compõem as redes.

Segundo Antonopoulos, o bloco do bitcoin[13] contém metadados (versão do protocolo, referência ao *hash* do bloco anterior, grau de dificuldade, *timestamp*, *nonce*, *merkle tree root*) e as transações, até o limite do tamanho do bloco (2017, p. 197).

Metadados são "marcos ou pontos de referência que permitem circunscrever a informação sob todas as formas" (WIKIPEDIA, 2019).

[11] *Ledger* pode ser compreendido como a consolidação de todos os registros de transações realizadas na blockchain.

[12] Confira-se Laurence (2017, p. 21).

[13] Primeira e mais conhecida rede blockchain e, por isso, aqui utilizada como exemplo.

As transações indicam os endereços de onde será remetido determinado saldo de bitcoins e qual endereço receberá tal saldo.

Como se vê, nenhum dos elementos do bloco corresponde objetivamente a um dado pessoal ou sensível.

Além disso, cada detentor de bitcoins poderá ter um ou mais endereços, sem que precise revelar sua titularidade, a não ser quando realize alguma transação. Frise-se: para movimentar o saldo de bitcoins constante em um determinado endereço, o detentor da chave privada correspondente – e, em consequência, do saldo de bitcoins – deverá solicitar a transação para a rede que, constatando a suficiência de saldo, validará a operação e a registrará em um bloco.

Os blocos das redes possuem capacidade de armazenamento limitada e, no caso da rede bitcoin, um bloco é minerado[14] a cada dez minutos[15], aproximadamente.

Com a mineração, os blocos são encadeados na rede e as transações neles constantes estarão permanentemente registradas.

4. Análise da pertinência tecnológica entre a blockchain e a Lei Geral de Proteção de Dados

Pode-se estabelecer, desde logo, que, em razão de sua arquitetura e características, a tecnologia blockchain não traz vantagens imediatamente perceptíveis para o armazenamento de dados pessoais ou sensíveis de forma pública e direta.

Entretanto, mediante a utilização de alguns recursos tecnológicos já existentes, é possível observar rigorosamente a legislação e, ainda, valer-se de todas as propriedades da blockchain.

Tomando-se a rede bitcoin como exemplo, rede pública, distribuída e não permissionada, a realização de transação depende da divulgação das chaves pública e privada.

Embora, em primeira análise, as chaves pública e privada não configurem dados pessoais, se for possível atrelá-las a uma pessoa física, haverá essa identificação. De outro lado, pela própria forma de funcionamento da criptografia assimétrica, elemento essencial para a realização da transação, se não forem fornecidas as chaves pública e privada, tal não será possível.

E, uma vez inseridas tais informações na rede, a transação será imutável.

Portanto, diante de uma rede distribuída, pública, não permissionada, na qual a transação seja feita diretamente pelo titular dos dados, caso haja rompimento da criptografia ou por outro modo o detentor das chaves pública e privada venha a ser conhecido, nada poderá ser feito.

Ademais, a correção do dado, quando envolver a correção da própria transação (se houver sido feita por engano, por exemplo), dependerá exclusivamente daquele que recebeu dito ativo, se este decidir realizar transação no sentido inverso, revertendo-a.

[14] A mineração é o ato de criação de um novo bloco na rede. Ela consiste em uma competição entre os nós da rede na solução de um problema matemático. Aquele que solucionar o problema matemático primeiro criará o bloco e receberá, em troca, bitcoins.

[15] Este tempo é o grau de dificuldade da rede do problema matemático a ser solucionado pelos mineradores no cumprimento da prova de trabalho, a fim de serem remunerados com créditos em bitcoin.

Acrescente-se, ademais, que se a transação for realizada com pessoa desconhecida, ou se forem remetidos ativos para um endereço equivocado, é possível que sequer se descubra quem os recebeu.

Esse cenário, entretanto, não impossibilita o uso das redes públicas, não permissionadas e distribuídas com a Lei Geral de Proteção de Dados.

Como os blocos da rede bitcoin possuem tamanho limitado, nem sempre é possível inserir, por exemplo, um arquivo de imagem. Todavia, nada impede que tal arquivo venha a ser convertido em uma *hash*[16] e que a própria *hash* conste no bloco. Uma vez que, a depender do padrão criptográfico utilizado, não é possível reverter a *hash* obtida no arquivo convertido, ao menos não de acordo com os recursos tecnológicos disponíveis na data da elaboração deste estudo, a anonimização da informação desta forma atenderia aos ditames legais.

Entretanto, tendo em vista a existência de redes que interagem com a rede distribuída ou, ainda, a possibilidade de anonimização desses dados (para que conste apenas a *hash* resultante na blockchain), as redes distribuídas não são de todo incompatíveis com a LGPD.

Além disso, como nas redes não permissionadas não há óbices à participação de quem quer que seja, nada impede que qualquer pessoa obtenha cópia integral de todas as transações realizadas e, a partir dela, realize mineração de dados, caso em que, a depender da natureza destes, poderá se submeter à legislação protetiva.

Todavia, reconhece-se desde já a dificuldade de monitoramento de tais condutas, já que não há nada, ao menos até o encerramento da elaboração do presente texto, que possa impedi-las.

Com relação às redes descentralizadas e às permissionadas, as soluções são distintas. Há claros pontos de centralização e, por consequência, de controle, inclusive de quem são os membros da rede. Estabelecidos tais núcleos, é possível delimitar quais informações são registradas ou, ao menos, por qual meio tal ocorreu.

Ainda que eventualmente isso não seja possível, diante do ponto de centralização vislumbra-se uma via para imposição da obrigação de informar o usuário final acerca do funcionamento da blockchain e das cautelas que devem por ele ser tomadas na realização de operações.

Dito isso, os registros realizados em blockchain são imutáveis, não importando exatamente a classificação da rede. Porém, quando há intermediação, há a possibilidade de maior controle do conteúdo que constará em um registro em blockchain.

A correção de dados na blockchain também não é imune a peculiaridades.

Nesse particular, o atendimento ao direito do titular de dados de correção ou atualização de informações a seu respeito ocorrerá somente a partir do momento em que tal correção ou atualização for inserida na cadeia de blocos, pois não é tecnicamente possível a alteração de informações já registradas na blockchain.

Entretanto, nesse ponto, destaca-se que pode ser, inclusive, forma de atender à seguinte recomendação:

[16] Nesse ponto, destaca-se que a função *hash* converte dados de comprimento variável, apresentando um resultado com comprimento fixo (WIKIPEDIA, 2019). Assim, quando o número de caracteres convertido em hash for maior que aquele do resultado da função, haverá economia de espaço.

> *Evidentemente, é de todo aconselhável o registro do histórico dos apontamentos, sem que necessariamente ocorra a deleção da informação desatualizada, a qual poderá vir a ter utilidade para variados fins, seja para o controlador, seja para o titular (MALDONADO; BLUM, 2019, posição 7037).*

Quanto ao direito ao apagamento, "o qual pressupõe a completa eliminação dos dados quando há o requerimento do titular e quando, de fato, inexista base legal para a subsistência do tratamento" (MALDONADO; BLUM, 2019, posição 7037), surgem as maiores arestas com a tecnologia blockchain.

Embora a LGPD tenha feito menção à eliminação do dado e respeitáveis autores salientem que ela deve ser realizada de forma completa, trata-se de medida que, tecnicamente, não é tão simples de ser tomada, a depender da forma como mantido o dado em questão.

Quando arquivos são excluídos da mídia de armazenamento do computador, na verdade há uma desindexação, de sorte que eles não são mais localizados e, após, eles são sobrescritos com informação nova (ZARAMELA, [20--?]). Isso significa que, na prática, os dados não serão completamente apagados, mas, sim, indisponibilizados.

Em outras palavras, em mídias de armazenamento, quando um dado é excluído, o espaço por ele ocupado é lido pela máquina como disponível para gravação de novos arquivos, que sobrescreverão os dados cuja deleção se pretendia.

Assim, ainda que o legislador tenha estabelecido que a exclusão dos dados é direito do titular, respeitadas as opiniões em contrário, parece ser possível considerar que a indisponibilidade dos dados ou sua corrupção — hábil a impedir o acesso ao seu conteúdo — atende ao quanto pretendido pela norma.

5. Sugestões para compatibilização tecnológica

Observadas as ressalvas feitas ao longo deste texto, no sentido de que não é recomendável a inserção do dado pessoal em rede blockchain, sem nenhuma cautela ou recurso para obscurecer seu acesso, apresentam-se algumas sugestões.

Assim, a primeira medida sugerida é a de anonimização de dados, prevista na própria LGPD, em seu art. 5º, XI, definida como a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

A utilização da anonimização de dados pode ser interessante por alguns motivos. O mais evidente, aquele que envolve a proteção dos dados do titular. Em um segundo momento, considerando a eficiência da rede que, como regra, possui recursos limitados de armazenamento, a anonimização de dados poderá redundar em economia de espaço[17].

A própria rede bitcoin se vale de pseudônimos (os endereços) e da possibilidade da criação de mais de um deles por pessoa, notadamente porque a identidade daqueles que realizam transações não interfere na regularidade delas.

[17] Uma das formas de promover a anonimização de dados é converter a informação em uma *hash*. Se a *hash* for menor que o arquivo convertido, haverá melhor aproveitamento do espaço no bloco.

Ademais, é possível a utilização de redes paralelas (*sidechains*) ou separadas (*off-chains*), objetivando o resguardo das informações. Por exemplo: a transação pode ser realizada em uma rede paralela e apenas seu resultado constar na rede principal. Ou, ainda, os dados pessoais ou sensíveis podem constar em meio independente e ser apenas indexado na rede prioritária.

Sem prejuízo do quanto já analisado, vale ressaltar que, até em virtude da limitação do tamanho dos blocos existentes nas diversas blockchains, não há motivos para não usar indexação da informação.

Se não houver necessidade de o dado constar, ele próprio, na rede blockchain – e, diga-se, em uma análise superficial e objetiva isso não se verifica –, é possível lançar mão de sua indexação, por meio do uso de criptografia.

Melhor explicando, bastará que o dado cuja existência se pretende aferir mediante o uso dos atributos da rede blockchain seja convertido em uma *hash* e a *hash* seja transposta para a rede.

Aquele que eventualmente alcançar a informação na rede blockchain estará diante de um código intransponível mas que, confrontado com o dado original, terá sua existência comprovada na data e horário de criação do bloco.

Caso o titular do dado não pretenda mais se valer de tal recurso, bastará que ele próprio não mais disponibilize a informação entregue para conversão em *hash*.

Haverá, nesse ponto, controle integral da informação pelo titular do dado, em pleno atendimento aos objetivos delineados na Lei Geral de Proteção de Dados.

6. Considerações finais

Conquanto blockchain seja uma ferramenta de inegável potencial para o exercício da liberdade de expressão (TAPSCOTT; TAPSCOTT, 2018, p. 245), tecnologias são meios, não fins em si mesmas, e seu uso deve ser avaliado de forma crítica e ponderada.

Ademais, para além de um óbice à incidência da LGPD, blockchains poderão se tornar forma de resguardar a privacidade do titular dos dados.

Nesse sentido, Mougayar:

> *Veja o blockchain e as aplicações descentralizadas baseadas nele. Seu advento traz possíveis soluções para a segurança de dados porque a criptografia se torna uma parte padrão de aplicações blockchain, especialmente as que pertencem às partes de dados. Por padrão, tudo é criptografado. Pelo mérito de descentralizar a arquitetura dos elementos da informação, cada usuário pode ser proprietário de seus dados privados, e repositórios centrais são menos vulneráveis a perdas de dados ou violações, porque eles apenas armazenam informações criptografadas e apontadores codificados para locais de armazenamento distribuídos que estão espalhados por redes de computadores também distribuídas. Assim, hackers não conseguem reconstruir ou entender quaisquer informações parciais que podem ter em mãos. Pelo menos, essa é a teoria por trás dessa visão, e há trabalho a ser realizado para trazer isso para a realidade (2017, p. 53).*

A sociedade da informação fomentou modelos de negócios construídos sobre a captação irrestrita de dados dos particulares e um estado de monitoramento permanente.

Tal situação nutriu um terreno fértil para abusos que, conforme vêm à tona, causam notória situação de desconforto naqueles que percebem a violação de sua privacidade. Em contrapartida, daí emergem instrumentos jurídicos e tecnológicas hábeis a limitar tais condutas e a permitir o exercício racional de direitos por todos os envolvidos.

Diante do exposto, percebe-se que, após análise acurada da natureza da blockchain e das informações nela envolvidas, não há óbices ao seu uso de forma plenamente compatível com a Lei Geral de Proteção de Dados, ao menos quanto aos direitos de apagamento e correção de dados.

Com pouca reflexão, qualquer meio, até mesmo um pedaço de papel, pode afrontar os termos da LGPD.

7. Referências bibliográficas

ALTER, Adam. *Irresistible*: the rise of addictive technology and the business of keeping us hooked. Nova Iorque: Penguin Books, 2018. *E-book*.

ANTONOPOULOS, Andreas. *Mastering bitcoin*: programming the open blockchain. 2. ed. California: O'Reilly, 2017.

BASHIR, Imran. *Mastering Blockchain*. 2. ed., Birmingham: Packt, 2018. *E-book*.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018. *E-book*.

BLOCO gênese do Bitcoin. Disponível em: https://bit.ly/2R68Kqi. Acesso em: 7 ago. 2019.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://bit.ly/2Tx6Ro4. Acesso em: 7 ago. 2019.

BRASIL. *Lei nº 13.853, de 8 de julho de 2019*. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: https://bit.ly/365Hc8s. Acesso em: 7 ago. 2019.

CAMPBELL-VERDUYN, Malcolm (ed.). *Bitcoin and beyond*: cryptocurrencies, blockchain and global governance. Nova Iorque: Routledge, 2018. *E-book*.

CASEY, Michael J.; VIGNA, Paul. *The truth machine*: the blockchain and the future of everything. New York: St. Martin's Press, 2018.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei geral de proteção de dados pessoais comentada*. São Paulo: Revista dos Tribunais, 2019.

DAVIS, Alison; LE MERLE, Matthew C. *Blockchain competitive advantage*. Tiburon: Fifth Era Media, 2019. *E-book*.

EHA, Brian Patrick. *How money got free*. Londres: Oneworld Book, 2017.

ETWARU, Richie. *Blockchain trust companies*: "Every company is at risk of being disrupted by a trusted version of itself". Indianapolis: Dog Ear Publishing, 2017.

FILIPPI, Primavera de; WRIGHT, Aaron. *Blockchain and the law*: the rule of code. Massachussets: Harvard University Press, 2018. *E-book*.FUNÇÃO Hash. *In*: WIKIPEDIA:

the free encyclopedia. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: https://bit.ly/3al5YEW. Acesso em: 16 ago. 2019.

JUN, Myungsan. *Blockchain government*: a next form of infrastructure for the twenty-first century. Scotts Valley: CreateSpace, 2018. *E-book*.

KRAMER, Adam D. I.; GUILLORY, Jamie E.; HANCOCK, Jeffrey T. Experimental evidence of massive scale emotional contagion through social networks. *In:* PNAS, 2014, [*s. l.*]. *Proceedings* […]. [*s. l.*]: National Academy of Sciences of the United States of America, 2014. p. 1-5. Disponível em: https://bit.ly/30vwUgR. Acesso em: 6 ago. 2019.

KRAVCHENKO, Pavel; SKRIABIN, Bohdan; DUBININA, Oksana. *Blockchain and decentralized systems*. v. 1. Kharkiv: Distributed Lab, 2018. *E-book*.

LAURENCE, Tiana. *Blockchain for dummies*. Hoboken: John Wiley & Sons, 2017.

MALEKAN, Omid. *The story of blockchain*: a begginer's guide to the technology that nobody understands. New York: Triple Smoke Stack, 2018. *E-book*. METADADOS. *In*: WIKIPEDIA: the free encyclopedia. [São Francisco, CA: Wikimedia Foundation, [s. d.]. Disponível em: https://bit.ly/3asqLGR. Acesso em: 25 ago. 2019.

MOUGAYAR, William. *Blockchain para negócios*: promessa, prática e aplicação da nova tecnologia da internet. Rio de Janeiro: Alta books, 2017.

NAKAMOTO, Satoshi. *Bitcoin*: a peer-to-peer electronic cash system. [*S. l.*: *s. n.*], 2008. Disponível em: https://bit.ly/374U53Z. Acesso em: 7 ago. 2019.

NORMAN, Allan T. *Blockchain technology explained*: the ultimate beginner's guide about blockchain wallet, mining, bitcoin, ethereum, litecoin, zcash, monero, ripple, dash, IOTA and smart contracts. Scotts Valley: CreateSpace, 2017.

OSMAN, Maddy. *Estatísticas e fatos surpreendentes do Youtube* (2º Site mais visitado). Kinsta, [*s. l.*], 20 jun. 2019. Disponível em: https://bit.ly/38eMWOM. Acesso em: 6 ago. 2019.

SWAN, Melanie. *Blockchain*: blueprint for a new economy. California: O'Reilly, 2015.

TALBOT, Michael. *A brief description of blockchain*: why it matters in the real world. [*S. l.*]: Veracity Tech Academy, 2018. *E-book*.

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution*: how the technology behind bitcoins is changing money, business, and the world. 2. ed. Toronto: Penguin Canada, 2018.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Estrasburgo, 4 maio 2016. Disponível em: https://bit.ly/2NDhNwJ. Acesso em: 19 ago. 2019.

WERBACH, Kevin. *The blockchain and the new architecture of trust*. Cambridge: MIT Press, 2018. *E-book*.

ZARAMELA, Luciana. *Apague definitivamente os dados de seu disco rígido*. Canaltech, [*s. l.*], [20--?]. Disponível em: https://bit.ly/2TI697q. Acesso em: 20 ago. 2019.