Instituto
de Tecnologia
& Sociedade
do Rio

Trabalho final do IV Grupo de Pesquisa ITS Rio

Identidade autossoberana para além do hype

Beatriz Souza Costa

Inovação

Introdução

Os atributos que caracterizam uma pessoa é o que define o termo "identidade". Esses caracteres podem ser aspectos biométricos, nomenclatura e, até mesmo, posicionamentos adotados durante a vida civil. Por ser inerente à pessoa humana, integra os direitos da personalidade. De acordo com a renomada civilista Maria Helena Diniz, "o direito da personalidade é o direito da pessoa defender o que lhe é próprio, como a vida, a identidade, a liberdade, a imagem, a privacidade, a honra, etc."[1]. Esse direito da personalidade se traduz, em uma de suas extensões, no mundo físico e digital através da identidade física e digital, sejam elas emitidas por órgãos governamentais ou não.

Os documentos de identidade fundacionais, como as certidões de nascimento e de casamento, são a identidade legal. A partir deles, é possível gerar os documentos de identidade funcionais, como a Carteira Nacional de Habilitação e o passaporte. Com a desmaterialização das informações, as interações passaram a ser executadas por meio de sistemas de informação interconectados e da internet, resultando no surgimento da identidade digital. Está é conceituada como "os elementos de *hardware* ou *software* que permitem que uma pessoa se identifique e seja autenticada, obtenha as permissões para acessar determinados recursos de informação ou físicos (por exemplo, o acesso a uma área) e realizar transações pela Internet ou redes privadas".[2]

Devido à própria estrutura da Internet, tema que abordaremos ao longo deste artigo, hodiernamente, o usuário fornece seus dados para obter acesso ao serviço a cada *site* acessado. Por conseguinte, diversos *players* do mercado possuem um vasto banco de dados que passam a estar automaticamente suscetíveis a ataques cibernéticos. A "gestão da identidade traz, por um lado, desafios em termos de privacidade, proteção de dados e novos riscos de fraude e, por outro lado, a necessidade de revisar e ajustar os esquemas de governança, os marcos legais e as tecnologias que podem estar se tornando obsoletas".[3]

É nesse cenário que a identidade autossoberana (também conhecida como self-sovereign identity ou SSI, ambos termos em inglês), que, assim como os outros sistemas identitários, se encaixa na discussão atemporal da extensão do direito à privacidade, à proteção de dados e da autodeterminação informativa. O modelo de identidade autossoberana prima permitir o gerenciamento da identidade pelos próprios usuários, sem depender de qualquer tipo tradicional de autoridade centralizada.

Do ponto de vista dos cidadãos, estes experimentarão benefícios econômicos e ganhos de eficiência de serviços, além da alteração do equilíbrio de poder, aumentando a propriedade e o controle sobre seus dados. Uma solução de identidade autossoberana reduz a necessidade de manter repositórios centralizados de informações

de identificação. Uma vez que a propriedade e o atestado de identidade são transferidos para os cidadãos, não há necessidade de hospedar servidores e bancos de dados com dados pessoais. Além disso, com o uso da tecnologia *blockchain*, serão experimentados benefícios econômicos, ganhos de eficiência e um menor risco de vazamentos de dados pessoais.[4]

Considerando a fase inicial da tecnologia *blockchain* no funcionamento da SSI, é notório alguns desafios que precisam ser superados. São eles: (i) interoperabilidade; (ii) proteção de dados, com foco no direito ao esquecimento quando falamos de *on-chain records*; (iii) adesão popular; e (iv) fator humano, principalmente quando falamos de *off-chain records*. Pensando nesses gargalos, elaboramos o presente artigo.

1. Premissa Constitucional

Para demonstrar a importância temática, é de suma importância fixarmos parâmetros sobre o direito à privacidade. A Constituição Federal assegura a privacidade (gênero) ao reconhecer o direito à indenização pelo dano material ou moral decorrente da violação à intimidade, à vida privada, à honra e à imagem das pessoas (espécies), conforme o inciso X do artigo 5º. Portanto, o direito à privacidade é um direito fundamental.

O direito à privacidade sofreu diversas mutações interpretativas ao longo dos anos, indo do *right to be left alone*[5] até o estado atual, onde o ordenamento resguarda a faculdade que cada indivíduo possui de obstar a intromissão de estranhos, assim como de impedir o acesso e a divulgação de informações privadas, sejam elas hábitos, convicções, relacionamentos afetivos, liberdade sexual, convicção política e afins.

Nas palavras de Celso Lafer em "A Reconstrução dos Direitos Humanos",

> *"[a] construção doutrinária e pretoriana em torno do direito à intimidade, que tem como ponto de partida o tema clássico da inviolabilidade de domicílio, passa pelo sigilo da correspondência, o segredo profissional, o direito à honra e à reputação, e acabou adquirindo projeção autônoma em relação aos demais direitos da personalidade, que têm como objeto a integridade moral do ser humano".*[6]

Neste diapasão, Gustavo Tepedino, Heloisa Helena Barboza e Maria Celina Bodin de Moraes recordam,

> *"Como leciona Stefano Rodotà, na atual sociedade de informação tendem a prevalecer definições mais funcionais do conceito, as quais, em diversos modo, fazem referência à possibilidade de um sujeito conhecer, controlar, direcionar ou mesmo interromper o fluxo de informações que lhe dizem respeito (Tecnologie e Diritti,*

> *p. 101, original não grifado). Na doutrina brasileira, Celso Lafer, procurou ampliar o conceito, tomando-o não apenas como "o direito do indivíduo estar só", mas ainda como a "possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só refere, e que diz respeito ao seu modo de ser no âmbito da vida privada" (A reconstrução dos Direitos Humanos, p. 239). (...).*
>
> *Sustenta-se na atualidade que o controle das informações pessoais leva também ao direito de determinar o modo de construção da própria esfera privada (Stefano Rodotà, Tecnologie e Diritti, p. 122) – conceito que se encontra em crescente expansão, incluindo cada vez maior número de setores da vida humana e compreendendo, assim, toda uma gama de escolhas existenciais relacionadas à política, ao sexo e à religião, à guisa de exemplo".* [7]

Nas palavras de Caio Mário Pereira da Silva, o direito à privacidade "oferece caráter dúplice: o direito de estar só, de não se comunicar; e simultaneamente de não ser molestado por outrem, como também pela autoridade pública, salvo quando um imperativo de ordem pública venha a determiná-lo".[8] Conclui-se que a finalidade do direito à privacidade é, a grosso modo, defender a esfera privada da pessoa de toda intromissão de terceiros.

Analisando este direito fundamental aplicado a dados, em 1983, o Tribunal Constitucional Alemão inaugurou uma nova linha doutrinária ao afirmar que "não existem mais dados insignificantes". Nas palavras de Marcus Vinicius Furtado Coêlho, ex-presidente da Ordem Brasileira de Advogados:

> *"O livre desenvolvimento da personalidade impõe o asseguramento de uma série de garantias fundamentais no plano constitucional, entre as quais destaca-se o* ***direito à autodeterminação de dados e informações pessoais****. Essas informações podem ser definidas, na compreensão de Schertel, como sinais utilizados na comunicação, que servem para identificar uma pessoa e, quando assumem a forma impressa, transformam-se em dados pessoais".*[9] *(grifos nossos)*

Ingo Sarlet identifica o direito à autodeterminação como a face subjetiva do direito à privacidade, isto porque, neste aspecto, a privacidade opera como "direito de defesa, portanto, como direito à não intervenção por parte do Estado e de terceiros no respectivo âmbito de proteção do direito e, como expressão também da liberdade pessoal, como direito a não ser impedido de levar sua vida privada conforme seu projeto existencial pessoal e de dispor livremente das informações sobre os aspectos que dizem respeito ao domínio da vida pessoal, e que não interferem em direitos de

terceiros".[10] Conclui-se que a autodeterminação informativa é a faculdade do titular dos dados determinar e controlar os seus próprios dados.

Recentemente, o Supremo Tribunal Federal, em decisão histórica, reconheceu a existência da autodeterminação informativa no julgamento da medida cautelar na Ação Direta de Inconstitucionalidade nº 6387[11] contra a Medida Provisória nº 954/2020.[12] A MP determinava que as empresas de telecomunicações compartilhassem os dados como nome, telefone e endereço, de todos os seus usuários com a Fundação Instituto Brasileiro de Geografia e Estatística — IBGE, para fins de pesquisas estatísticas, tendo em vista a situação de emergência de saúde pública decorrente do novo coronavírus.

A ministra Rosa Weber, ao fazer menção ao artigo de Warren e Brandeis, determinou que desde então reconhecia-se que "as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual é necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo". Em sua decisão, a ministra afirmou ainda que "decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais". Afastando a constitucionalidade da referida MP, o Tribunal Pleno do STF proferiu decisão histórica ao reconhecer expressamente que a Constituição Federal de 1988 assegura aos brasileiros o direito à autodeterminação informativa, devendo o uso dos dados e informações pessoais ser controlado pelo próprio indivíduo, salvo quando a legislação estritamente determinar.

Paralelamente, ainda temos o direito à proteção de dados que é a possibilidade de cada titular de dados determinar de forma autônoma a utilização que é feita de seus próprios dados pessoais, em conjunto com diversas garantias, para evitar que os dados sejam utilizados de forma prejudicial ao titular ou à coletividade. Tal direito já existia em nosso ordenamento jurídico, mas foi consolidado com a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018[13])

Inclusive, está em tramitação o Projeto de Emenda Constitucional nº 17/2019[14], cujo objetivo é incluir a proteção de dados pessoais no rol das cláusulas pétreas. Caso a PEC seja aprovada, com a alteração do 5º da Constituição Federal, qualquer outra proposta que tenta abolir a proteção de dados pessoais não será possível, proteção conferida graças à elevação de seu status à cláusula pétrea. Ademais, a proposta fixa competência privativa da União para legislar sobre a proteção e o tratamento de dados pessoais. Tendo o exposto como premissa, passamos a analisar a trajetória da identidade digital.

2. Breve histórico sobre a identidade digital

A internet foi criada em 1969, nos Estados Unidos. Inicialmente conhecida como Arpanet – rede de titularidade do Departamento de Defesa norte-americano -, sua função era interligar laboratórios de pesquisa. A partir de 1982, o uso da Arpanet tornou-se maior no âmbito acadêmico e, com a expansão, começou a ser utilizado o nome "internet". Por quase duas décadas, apenas os meios acadêmico e científico tiveram acesso à rede. Em 1987, pela primeira vez, foi liberado seu uso comercial nos EUA.

Kim Cameron, chefe de arquitetura de identidade e acesso da Microsoft, no artigo *The Laws of Identity*[15], publicado em 2005, afirma em sua introdução que "a internet foi criada sem uma forma para saber a quem ou a que você está se conectando" (tradução livre). Para ele, a internet foi criada sem uma camada de identificação, assim, o sistema de endereçamento da Internet é baseado na identificação de máquinas em uma rede e não de pessoas, e, portanto, não tem como identificar pessoas de forma única.

No mundo físico, os governos emitem e validam a identificação civil através da emissão de documentos físicos, como a carteira de identidade. Assim, o Estado se perpetua, através de suas instituições, como uma figura centralizada e historicamente considerada como confiável, que garante a identidade de cada cidadão. Por outro lado, no mundo digital, mesmo com os avanços obtidos desde 1987, ainda não existe uma forma fácil, segura e aceita pela maioria da população, capaz de provar quem são seus usuários.

O relatório *Picture perfect: A blueprint for digital identity*, publicado em 2016 pela Deloitte, atesta que os sistemas de identidade compartilham aspectos básicos, são eles: "(i) usuários – aqueles que obtêm uma identidade para conseguir realizar transações; (ii) fornecedores de identidade – aqueles que capturam e armazenam os atributos da identidade dos usuários, asseguram a veracidade e chegam a concluir as transações em nome deles; e (iii) os terceiros de confiança – aqueles que atendem aos usuários após a obtenção da identidade com os fornecedores" (tradução livre).

Ademais, a evolução da identidade digital tenta resolver três problemas centrais no âmbito da governança de dados. O primeiro é a segurança, uma vez que a informação precisa ser protegida contra divulgação não intencional. O segundo é o controle, onde objetiva-se que o proprietário da identidade tenha gerência de quem pode ver e acessar seus dados e para que fins. Por último, temos a portabilidade, que permitirá a utilização de dados onde o usuário quiser, sem vinculação a qualquer provedor.

O artigo "A gestão da identidade e seu impacto na economia digital", publicado em 2017 pelo Banco Interamericano de Desenvolvimento, afirma que a "gestão de sistemas de identidade requer um modelo de governança e um modelo de negócio;

um marco legal apropriado e atualizado; a simplificação e padronização de processos e sistemas; o estabelecimento de mecanismos de interoperabilidade que facilitem a coordenação entre os diferentes organismos, e a promoção e coordenação do ecossistema de uso da identidade".[16]

Cristopher Allen[17], em seu artigo *The path to self-sovereign identity*, divide a história da identificação digital em quatro momentos. O autor inicia sua dissertação no modelo centralizado, em que a identidade pertence e é controlada por uma única entidade. Dentro do domínio desta entidade, a identificação funciona perfeitamente, mas não pode ser utilizada em domínio distinto. Desta forma, o usuário deverá criar uma identidade para cada site ou aplicativo que utilizar. A principal característica desse modelo é que os dados de cada usuário são de propriedade da própria entidade. Como consequência, a remoção dos dados da sua base apaga por completo a identidade digital do usuário.

O segundo modelo explicitado por Allen é o federado, que confere um nível de portabilidade quando comparado com o centralizado. Nele, é possível usar a identificação criada em uma entidade em outra. Em um nível mais avançado, os sites e aplicativos poderiam até compartilhar a informação de usuários. Como exemplo, temos o Facebook Login, que permite que usuários utilizem o login e senha criados na rede Facebook para ingresso em outras redes. Por mais que esse modelo permita a portabilidade, os dados continuam sendo titularidade da entidade que o usuário se inscreveu. Com isso, ser desconectado desta entidade inicial acarretará a impossibilidade de uso da rede de terceiros.

Em seguida temos o modelo *user-centric*, onde o usuário controla os seus dados na rede, inclusive, para quem eles serão disponibilizados. O indivíduo cria o seu próprio "armazém de dados" com informações que ele poderá dar permissão de acesso a outras organizações, mantendo um registo à medida que o faz. A identidade centrada no usuário é mais frequentemente manifestada na forma de armazenamento, independente de dados pessoais em um extremo do espectro, e de grandes redes sociais, no outro extremo. No entanto, todo o espectro ainda depende da seleção de um provedor de identidade individual pelo usuário e da concordância com seus contratos de adesão, muitas vezes unilaterais.

Antes de adentrarmos no último modelo, objeto deste trabalho, importante frisar que a quantidade de relações travadas no âmbito digital e a complexidade das mesmas é exponencial. Inclusive, há diversas legislações setoriais que regulam tanto a identificação quanto a relação digital, com fim de conferir segurança da mesma maneira que o mercado confia nos documentos físicos emitidos pelas autoridades públicas. Enquanto na internet criamos uma identidade digital em cada site ou aplicativo que acessamos ou optamos por utilizar serviço de identificação de outros provedores, no mundo físico, a depender do órgão público que teremos

contato, diferentes documentos nacionais nos são solicitados. Assim, possuímos cada vez mais diferentes tipos de identidade e oferecemos os nossos dados a uma quantidade considerável de *players* do mercado.

Isto posto, apresentamos o último modelo: a identificação autossoberana. O surgimento de novas soluções criptográficas mais seguras desencadeou uma nova visão sobre o tema "identidade digital", que, em última análise, poderá solucionar problemas existentes nos ambientes digital e tradicional.

Neste modelo, assim como no *user-centric,* o usuário decide quando e como as informações são compartilhadas. Contudo, ele supera os três elementos acima mencionados, pois permite o controle individual, é seguro e permite total portabilidade. O indivíduo, a quem a identidade pertence por completo, controla e gerencia sua identidade. A existência digital do indivíduo é independente de qualquer organização individual.

A melhor maneira de pensar em identidade autossoberana, é como um registro digital ou recipiente de transações de identidade, que o próprio usuário controla. O fundamento central é o controle pessoal dos dados pelos seus titulares. Para a identidade digital ser realmente autossoberana, a infraestrutura precisa ser um ambiente confiável, e que não pertença ou seja controlada por qualquer organização, mesmo que seja um pequeno grupo de organizações. Por isso, esse modelo, ainda incipiente, encontrou guarida na tecnologia *blockchain*, embora, não necessariamente, limitado a ela. Para uma melhor compreensão do tema, cumpre estabelecer alguns parâmetros sobre a tecnologia *blockchain*.

3. Premissas básicas sobre a tecnologia *Blockchain*

O termo *blockchain* se refere a uma das hipóteses de "tecnologia de registro distribuído" (ou *Distributed Ledger Technology* - DLT, na expressão em inglês). Assim, existem diversas formas de DLT, entre elas a tecnologia *blockchain*. Contudo, é comum que se utilize o termo *"blockchain"* para toda e qualquer DLT, mesmo que ela não envolva, necessariamente, "blocos" *(block)* ou seu encadeamento *("chain").*

A forma mais simples de se entender *blockchain*[18] é imaginar um banco de dados organizado como um livro registro, em que os dados são agrupados em blocos e estes, por sua, vez são encadeados em uma sequência cronológica. Os dados são inseridos na *blockchain* através de técnicas de criptografia, como funções de *hashing*[19]. Tanto os blocos quanto seu encadeamento são construídos utilizando criptografia de dados, sendo que cada bloco contém, em geral: (i) o número do bloco; (ii) os dados armazenados no bloco; (iii) o *hash* do bloco anterior; (ii) o *hash* do próprio bloco.

Por conta deste conteúdo dos blocos, e tendo em vista o modo de funcionamento dos *hashes*, qualquer tentativa de alteração no *hash* de um bloco "b", teria impacto imediato no bloco "b+1", tendo em vista que este último traz nele a informação do

hash anterior e o seu próprio *hash*, o qual é gerado, tomando por base todas as informações nele contidas. Isto leva a concluir que, quanto mais antigo o bloco, mais difícil seria sua alteração, pois todos os blocos sequenciais teriam que ser alterados.

Assim, a estrutura de encadeamento dos blocos, em que cada um deles traz o *hash* do anterior, é um dos principais elementos que assegura a confiabilidade/imutabilidade dos dados, e que tornou a tecnologia tão difundida. Porém, tal segurança somente é possível graças a uma outra característica, esta considerada um dos marcos da tecnologia: a descentralização (ou distribuição, para ser mais abrangente conceitualmente) do processo de consenso/validação das transações registradas.

Todos os nodes[20] que rodam o *software* da *blockchain* mantém uma versão igual da *blockchain* entre si, e mesmo que não tenham "resolvido" o problema matemático e criado um bloco, funcionam como validadores das "soluções" encontradas por terceiros, confirmando, assim, que o novo bloco deve ser mantido na *blockchain*. Tal método de consenso, conhecido como mineração[21], gera uma dificuldade prática enorme para violação da *blockchain*, tendo em vista que seria necessário reunir, em tese, 50%+1 da capacidade computacional dos mineradores para "vencer" a batalha contra os remanescentes e acrescentar um bloco "violado". Isto para alterar apenas o último bloco.

Para alterar um bloco mais antigo, seria ainda mais complicado, pois, como visto, a alteração de um bloco mudaria seu *hash*, com consequências em todos os blocos seguintes. Como a *blockchain* cresce sempre a partir da sua maior ramificação e todas as menores são descartadas neste processo, uma tentativa de alteração, por exemplo, do antepenúltimo bloco, teria que construir um novo penúltimo e um novo último de forma mais "rápida" do que o acréscimo de um novo bloco na *blockchain* original. Este mecanismo previne, entre outros eventos, a ocorrência do *double-spending*[22], dando mais segurança às transações registradas na *blockchain*[23].

De forma didática, as características mais marcantes da *blockchain* são as seguintes: (i) descentralização – já mencionada acima; (ii) eliminação de intermediários –a confiança que antes era depositada no intermediário passa à tecnologia, "eliminando", assim, a sua necessidade; (iii) imutabilidade – informações inseridas na *blockchain* não podem ser modificadas; (iv) irreversibilidade – por ser imutável, uma vez gravada na *blockchain*, a informação é irreversível; (v) segurança – ainda devido à imutabilidade e à descentralização, temos um alto nível de segurança, pois toda informação é gravada de forma definitiva; (vi) transparência – qualquer pessoa pode fazer transações e consultar o histórico de transações da rede sem pedir autorização a ninguém; logo, é facilmente auditável.

Mencionado acima, as informações são inseridas na *blockchain* através da criptografia, de forma que qualquer documento pode ser convertido em um *hash* – longa sequência de letras e números – similar a uma impressão digital. A validação das

informações e a transformação em *hash* possibilitam que as informações ali inseridas sejam compartilhadas e autenticadas sem a revelação das mesmas. Portanto, embora tenha sido criada para dar apoio a um criptoativo, a utilização da tecnologia no setor da identificação permite a criação de uma impressão digital confiável e auditável do documento de identificação.

Para o presente artigo, cumpre ainda diferenciar o que seria o registro *on-chain* do *off-chain*. A *blockchain* usualmente possui um limite sobre o tamanho e quantidade de dados que podem ser armazenados em um único bloco. Além disso, o custo de cada transação na rede pode ser muito custoso. Por fim, existem diversos dados que são confidenciais e sigilosos; logo, registrá-los na *blockchain* pode gerar danos irreversíveis.

Considerando o exposto, há uma divisão entre os dados que são gravados na *blockchain (on-chain records)* e aqueles que são grandes demais para serem armazenados na *blockchain* de modo eficiente, ou que requer a capacidade de ser alterado ou excluído *(off-chain records)*. Portanto, para alguns dados identitários, pode ser interessante fazer o registro fora da rede, e nesta registrar, apenas, a tradução criptográfica do que foi registrado *off-chain*, garantindo a validade e confiabilidade na informação registrada fora da *blockchain*.

A tecnologia *blockchain* proporciona uma maneira transparente, imutável, confiável e auditável de lidar com a identificação de forma transparente e segura. A tecnologia garantirá fundamentos que a identidade autossoberana precisava para sair do mundo teórico, quais sejam: (i) descentralização, ou seja, não pertencer a qualquer organização, governo ou terceiro interessado; (ii) existência por maior tempo que os usuários; (iii) garantia do direito ao esquecimento; e (iv) inclusão.

4. Benefícios da identidade autossoberana

De pronto, cumpre ressaltar que existem ferramentas de identidade do mundo físico no mundo digital, como os certificados digitais emitidos pelas autoridades certificadoras, todavia, estas ainda dependem de um intermediário que atribui confiança ao certificado usado por um indivíduo. Ademais, o serviço não é gratuito e existem, somente, 80 organizações ao redor do mundo que controlam a emissão desses certificados.[24] No Brasil, por exemplo, temos a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, que é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão brasileiro através do credenciamento centralizado de autoridades certificadoras, conferido pela Autoridade Certificadora Raiz – AC-Raiz.

O caminho para um modelo de identificação digital sem a dependência de um terceiro intermediário, atualmente, traduz-se na construção de redes distribuídas de confiança, que possam validar as informações produzidas por indivíduos em meios

físicos e digitais. "O conceito de identidade autossoberana refere-se a um modelo em que cada usuário tem total controle sobre seus dados, que podem ser armazenados em carteiras pessoais (semelhantes a carteiras de criptomoedas). Neste contexto, pode-se decidir quando e como as informações são compartilhadas."[25]

Nas palavras de Emily Fry[26] e Elizabeth M. Renieris[27],

> *"a ideia básica por trás da identidade autossoberana é permitir um modelo de gerenciamento de identidade que coloque os indivíduos no centro de suas transações relacionadas à identidade, permitindo-lhes gerenciar uma série de identificadores e informações pessoais, sem depender de qualquer tipo tradicional de autoridade centralizada. Uma escola emergente de SSI se baseia na combinação da tecnologia de registro distribuído e uso de identificadores descentralizados, bem como outros padrões técnicos em desenvolvimento pelo World Wide Web Consortium (WC3), e às vezes, também, é conhecida como "identidade descentralizada". [28]*

A identidade digital possui cinco fragilidades centrais: (i) o problema da proximidade – relações a distância possuem um alto risco de fraude identitária; (ii) escalabilidade – sistemas de identificação digitais são baseados em relações comerciais e integrações técnicas para enraizar as autoridades de confiança; (iii) flexibilidade - os sistemas de identidade atuais são rígidos, com esquemas e casos de uso fixos; (iv) privacidade - identificadores compartilhados, como *cookies*, permitem que informações pessoais sejam acumuladas e correlacionadas sem o consentimento qualificado do usuário; (v) consentimento - os sistemas de identidade dependem de identificadores universais, como endereços de e-mail, números de telefone que tornam fácil para terceiros correlacionar o comportamento e manter o controle das pessoas sem sua permissão.[29]

Em teoria, a descentralização e a criptografia resolveriam esses problemas. Ao oferecer mais segurança contra ataques *hackers*, visto a dificuldade para quebrar a criptografia da *blockchain*, supera-se o problema da privacidade e da proximidade. Por sua vez, o usuário, ao ter controle dos seus dados, aplicativos e serviços, somente terão acesso aos dados mínimos e necessários[30], resolvendo o problema do consentimento. Caso o sistema seja adotado por diversas instituições, soluciona-se os problemas da flexibilidade e da escalabilidade.

Ademais, como a tecnologia torna a informação nela gravada imutável, inquestionável e segura, por meio de assinaturas digitais baseadas em criptografia de chave pública. Outra vantagem é a redução dos custos envolvidos no modelo centralizado tradicional de identificação, uma vez que o registro de uma informação só precisará ser feito uma única vez e será válido em todas as instituições. Em adendo, a

identidade digital única, baseada em *blockchain*, também possibilita que os dados sejam sempre atualizados com as informações mais recentes do usuário.

Somente a título de exemplificação, podem ser citados alguns casos que declaram ser uma identidade autossoberana, como a Sovrin, rede de identidade de código aberto pública e permissionada, em que a fundação sem fins lucrativos Sovrin Foundation supervisiona o consenso das transações. Outro exemplo é a uPort, sistema de identidade de código aberto desenvolvido pela ConsenSys, o qual permite o gerenciamento de dados pelos usuários através da plataforma de *blockchain* Ethereum.

Ainda temos a Veres One, *blockchain* pública otimizada para fins de identidade digital, em que o sistema da rede foi projetado para ser autossuficiente com a finalidade de evitar ataques contra a rede e recompensar financeiramente os usuários para garantir sua segurança. No Brasil temos o BlockIoT, é o projeto CPqD (Centro de Pesquisa e Desenvolvimento em Telecomunicações)[32] que tem como objetivo a criação de identificação digital de pessoas e coisas com o uso da *blockchain*[33].

Outro projeto do CPqD, em conjunto com o LIFT — Laboratório de Inovações Financeiras e Tecnológicas, é o FinID — Sistema de Identidade Digital Descentralizada. Além desses, está em curso alguns projetos feitos pela Microsoft, IBM e Deloitte, em conjunto com o governo brasileiro.

Para alguns pesquisadores, "a identidade digital única já é realidade em alguns países como Estônia, Cazaquistão e Índia. Na Estônia, por exemplo, esta identidade unifica o acesso a diversos serviços, como transações bancárias, solicitação de benefícios estatais, declaração de impostos, registros escolares, etc. (Thompson e Yu, 2017)". Importante mencionar que os sistemas desses países não são, necessariamente, baseados em *blockchain* e/ou utilizam tecnologias descentralizadas. Contudo, o uso da tecnologia será viável ao controle pessoal de dados e servirá como prova oficial identitária.

5. Atuais desafios da identidade autossoberana

Por mais que a identidade autossoberana traga inúmeros benefícios, existem gargalos que precisam ser superados. Discutiremos aqui os quatro principais desafios a serem superados, iniciando pela interoperabilidade. A interoperabilidade é "a capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente".[34] Enquanto a integração é o processo de conectar dois ou mais sistemas através do uso de uma tecnologia, a interoperabilidade é a comunicação de diferentes redes sem a necessidade de outra tecnologia.

Quando acessamos uma rede utilizando os dados do Facebook, por exemplo, não estamos tratando de uma interoperabilidade e sim de uma integração. Para que a

identidade seja autossoberana é necessário que haja a interoperabilidade entre os sistemas, caso contrário, permanecerá o cenário em que o usuário fornece os mesmos dados múltiplas vezes para diferentes *players*.

Vimos acima que existem diversos projetos em *blockchain* para viabilizar a identidade autossoberana. Para que a interoperabilidade aconteça, é necessário que todos estejam de acordo sobre como a mesma ocorrerá. Dever-se-á ter uma padronização tecnológica ampla, para que o menor esforço seja demandado no momento da elaboração de interfaces, culminando em uma comunicação mais rápida e ágil. Defende-se aqui a adoção de "padrões abertos, ou seja, aqueles que estão publicamente disponíveis e não são controlados por nenhum governo ou corporação, que tornam possível que quaisquer empresas, cidadãos e países se conectem e troquem informações com autonomia".[35]

O segundo aspecto a ser superado é a adesão popular. A tecnologia *blockchain* existe desde 2008; logo, a mesma é nova se comparada com as tradicionais. Mesmo com 12 anos em circulação, é ínfima a parcela da população mundial que possui acesso à tecnologia. Afinal, ainda 46,4% (quarenta e seis vírgula quatro por cento)[36] da população mundial não possui acesso à internet. Portanto, o caminho ainda é longo para a disseminação dessa tecnologia.

Tornar a identidade autossoberana, significa dar ao público o controle de suas informações, porém, ao mesmo tempo, é aumentar a responsabilidade pessoal dos titulares para a atualização e pertinência de seus dados. Para que uma tecnologia seja aceita e utilizada, esta tem que provar para o usuário que o seu uso melhorará a sua performance em uma função específica, e a sua interface precisa ser fácil. Além disso, fatores externos, como a adesão em massa, gera um efeito comportamental positivo para a consolidação de uma tecnologia. Assim, por mais que o sistema seja interessante, esses fatores poderão afastar a sua real aplicabilidade.

Neste sentido, Adrian Doerk, no texto *The growth factors of self-sovereign identity*, afirma que um dos aspectos críticos a serem considerados é que "se não houver uma educação massiva e prestadores de serviços disponíveis para sanar dúvidas, educar e assegurar a identidade digital, não veremos nenhum grau significativo de adoção por parte do usuário".[37] Outro ponto levantado pelo autor é a obtenção de confiança do público na tecnologia, afinal, como toda tecnologia, é possível que a identidade seja abusada para fins de vigilância.

Pode levar muitos anos para que ocorra a adoção da identidade autossoberana e, quando a população passar a confiar e a usá-la, poderá ter surgido uma nova tecnologia que deixará a SSI baseada em *blockchain* defasada.[38] Por fim, a tecnologia deverá assegurar que pessoas com deficiência consigam utilizá-la, afinal, o direito à identidade é um direito constitucional de todo cidadão, tanto no Brasil quanto em outros países.

Em seguida, temos a portabilidade, desafio que emerge da proteção de dados. Nos termos do artigo 18, inciso V, da LGPD, o titular de dados tem o direito a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa. Por mais que os defensores da SSI indiquem a possibilidade técnica da portabilidade, ainda é incipiente o debate sobre a mitigação de riscos, alocação de responsabilidade ou mecanismos de aplicação ou reparação.

Outro aspecto da proteção de dados é o direito ao esquecimento, direito de eliminação de dados e direito de retificação. Acima, vimos a diferença do registro *on-chain* e *off-chain*. Quando as informações identitárias são registradas diretamente na *blockchain*, devido a sua característica de imutabilidade, o titular dos dados não conseguirá retificar ou eliminar os dados registrados.

Por mais que existam plataformas *blockchain* que aleguem ser possível a modificação, isso sugere um afastamento da plataforma do ideal criado acerca da própria tecnologia, em que o mecanismo de encadeamento de blocos garantiria imutabilidade e, por consequência, confiabilidade. O que é possível tecnicamente é o registro da informação atualizada no bloco posterior, informando que o registro do bloco "X" foi de um dado errado. O problema poderá ser superado, caso exista um sistema de governança *on-chain* que permita a modificação segura do bloco questionado.

Note que a responsabilidade da veracidade e do registro dos dados é transferido ao titular, portanto, a cobertura conferida pelas leis de proteção de dados existentes poderá ser questionada. Afinal, quem será o responsável pela plataforma ou pela demora da retificação ou remoção? Questões ainda em aberto neste modelo.

Por fim, também há problemas quando o registro das informações é feito *off-chain*. Isto porque, por mais que os problemas de eliminação e modificação sejam superados com mais facilidade, voltamos ao fator humano. Portanto, os problemas atuais da identificação no mundo físico transportar-se-ão para o digital. Os grandes bancos de dados *off-chain* continuarão suscetíveis a ataques cibernéticos, fraudes e todos os problemas que a própria teoria de identidade digital tenta superar.

Conclusão

É notório que a evolução do debate sobre o modelo identitário ideal é necessário e atemporal, visto que as inovações tecnológicas tendem a modificar a visão que a sociedade constrói acerca de um conceito. Com a atualização do conceito de privacidade e a sobressalência da autodeterminação informativa, o debate sobre a identidade autossoberana não poderia ser mais pertinente.

As características inerentes da tecnologia *blockchain* – descentralização, eliminação de intermediários, imutabilidade, irreversibilidade, segurança e transparência – retiram da teoria a SSI, na medida em que, ao eliminar o intermediário de modo seguro e auditável, transfere ao titular dos dados a capacidade de autodeterminar-se.

Vimos, ao longo do presente artigo, que as cinco fragilidades centrais da identidade digital – proximidade, escalabilidade, flexibilidade, privacidade e consentimento – podem ser superadas com a adesão da SSI.

Contudo, é necessário solucionar aspectos pendentes, quais sejam: interoperabilidade; proteção de dados, com foco no direito ao esquecimento quando falamos de *on-chain records*; fator humano, e, principalmente, a adesão popular para que o modelo funcione. O debate acerca da identidade autossoberana não podia ser mais contemporâneo e necessário no contexto brasileiro, principalmente com a promulgação de atos normativos que permeiam o assunto - como a Lei Geral de Proteção de Dados e o Decreto nº 10.278, de 18 de março de 2020. Contudo, precisamos ultrapassar a exposição dos benefícios e adentrar na discussão sobre os pontos em aberto para melhorar a construção do sistema.

Notas

1. DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro*. São Paulo: Saraiva, 2007, p. 119-120.

2. PAREJA, Alejandro; PEDAK, Mari; GÓMEZ, Carlos; BARROS, Alejandro. *A gestão da identidade e seu impacto na economia digital*. Banco Interamericano de Desenvolvimento. 2017. Disponível em: <https://publications.iadb.org/publications/portuguese/document/A-gest%C3%A3o-da-identidade-e-seu-impacto-na-economia-digital.pdf> Último acesso em: 26.06.2020.

3. PAREJA, Alejandro; PEDAK, Mari; GÓMEZ, Carlos; BARROS, Alejandro. *A gestão da identidade e seu impacto na economia digital*. Banco Interamericano de Desenvolvimento. 2017. Disponível em: <https://publications.iadb.org/publications/portuguese/document/A-gest%C3%A3o-da-identidade-e-seu-impacto-na-economia-digital.pdf> Último acesso em: 26.06.2020.

4. Para os fins deste artigo, consideramos que ainda não há tecnologia que viole a criptografia da *blockchain*.

5. WARREN, Samuel D.; BRANDEIS, L. D., "The Right to Privacy". Harvard Law Review ,vol. IV, 15 de dezembro de 1890.

6. LAFER, Celso. *A reconstrução dos direitos humanos*. São Paulo: Companhia das Letras, 2003, p. 240.

7. TEPEDINO, Gustavo; BARBOZA, Heloisa Helena; MORAES, Maria Celina Bodin de. *Código Civil Interpretado: Conforme a Constituição da República*. Rio de Janeiro: Renovar, 2014, 3.ed. p. 60-61.

8. PEREIRA, Caio Mario da Silva. *Instituições de Direito Civil - Volume I*. 30ª Edição. Rio de Janeiro: Forense, 2017. p. 216.

9. COÊLHO, Marcus Vinicius Furtado. *O direito à proteção de dados e a tutela da autodeterminação informativa*. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-28/constituicao-direito-protecao-dados-tutela-autodeterminacao-informativa#_ftnref3>. Acesso em: 03.07.2020.

10. SARLET, Info Wolfgang; MARINONI, Luis Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. 8ª Edição. São Paulo: Saraiva Educação, 2019, p. 576.

11. BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6.387/DF – Distrito Federal. Relatora: Ministra Rosa Weber. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf> Acesso em: 15.07.2020.

12. BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. Diário Oficial da União, Atos do Poder Executivo, Brasília, DF, 17.04.2020. Seção 1 - Extra, p. 1.Disponível em: <http://www.in.gov.br/web/dou/-/medida-provisoria-n-954-de-17-de-abril-de-2020-253004955> Acesso em: 15.07.2020.

13. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Atos do Poder Legislativo, Brasília, DF, 15.08.2018. Seção 1, p. 59.Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/KujrwoTZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337> Acesso em: 15.07.2020.

14. BRASIL. Proposta de Emenda à Constituição nº 17, de 2019. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757> Acesso em: 15.07.2020.

15. CAMERON, Kim. *The Laws of Identity*. 2005. Disponível em: <https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>. Último acesso em: 03.06.2020.

16. PAREJA, Alejandro; PEDAK, Mari; GÓMEZ, Carlos; BARROS, Alejandro. *A gestão da identidade e seu impacto na economia digital*. Banco Interamericano de Desenvolvimento. 2017. Disponível em: <https://publications.iadb.org/publications/portuguese/document/A-gest%C3%A3o-da-identidade-e-seu-impacto-na-economia-digital.pdf> Último acesso em: 26.06.2020

17. Christopher Allen é um desenvolvedor em *blockchain* e de identidade digital, pioneiro na criptografia da internet e co-autor do "TLS Security Standard".

18. Para esta explicação, consideramos a *blockchain* do Bitcoin.

19. A função Hash (Resumo) é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções Hash são conhecidas por resumirem o dado.

20. Na infraestrutura da *blockchain*, os nodes (ou nós) são os computadores responsáveis pelo consenso sobre uma transação em tempo real, contendo cópias dos registros autenticados distribuídos entre eles.

21. A depender a *blockchain* utilizada a forma de validação pode ser diferente.

22. O *double-spending* refere-se a um cenário em que alguém consegue utilizar os mesmos fundos mais de uma vez.

23. Consideramos a *blockchain* pública.

24. KONOPACKI, Marco. *Blockchain e identidades digitais: caminhos para uma nova democracia*. ITS Rio. 2018. Disponível em: <https://feed.itsrio.org/blockchain-e-identidades-digitais-caminhos-para-uma-nova-democracia-7719b8ae5doe> Último acesso em: 01.07.2020.

25. Binance Academy. *Casos de Uso Blockchain:* Identidade Digital. 2020. Disponível em: <https://academy.binance.com/pt/blockchain/blockchain-use-cases-digital-identity> Último acesso em: 01.07.2020.

26. CEO da Digital Trust na MATTR, empresa sediada na Nova Zelândia que desenvolve padrões abertos, infra-estrutura técnica e software voltado a identificação digital.

27. Fundadora e CEO da HACKYLAWYER, especializada em direito e engenharia de políticas. Advogada especialista em privacidade (CIPP/E, CIPP/US), em identidade e pesquisadora do Berkman Klein Center for Internet & Society da Universidade de Harvard, onde pesquisa estruturas de governança de dados para a era digital.

28. FRY, REINIERIS. *SSI? What we really need is full data portability*. 2020. Disponível em: <https://womeninidentity.org/2020/03/31/data-portability/> Último acesso em: 07.07.2020.

29. WINDLEY, Philip. *How blockchain makes self-sovereign identities possible*. Computer World. 2018. Disponível em: <https://www.computerworld.com/article/3244128/how-blockchain-makes-self-sovereign-identities-possible.html> Último acesso em: 07.07.2020.

30. LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

31. Na criptografia de chave pública ou criptografia assimétrica é formada por uma chave pública utilizada para cifrar o conteúdo e por uma chave privada utilizada para decifrar o texto cifrado. Nas assinaturas digitais, a criptografia assimétrica ocorre quando a chave privada é utilizada para codificar o conteúdo e a respectiva chave pública para decifrar a mensagem criptografada, obtendo, assim, a autenticidade.

32. Centro de pesquisa brasileiro focado na inovação em tecnologias da informação e comunicação. Ele atua na pesquisa, desenvolvimento e suporte de diversos setores, como o da administração pública e financeiro

33. AUGUSTO, Thaís. *CPqD quer utilizar o blockchain para dar mais segurança à identidade digital.* Canal Tech. 2019. Disponível em: <https://canaltech.com.br/blockchain/cpqd-quer-utilizar-o-blockchain-para-dar-mais-seguranca-a-identidade-digital-136101/I> Último acesso em: 08.07.2020.

34. MELLO, Ana Paula Pessoa; MESQUITA, Hudson; VIEIRA, Carlos Eduardo. *Introdução à Interoperabilidade.* Escola Nacional de Administração Pública. 2015. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/2399/1/M%C3%B3dulo_1_EPING.pdf> Último acesso em: 15.07.2020.

35. MELLO, Ana Paula Pessoa; MESQUITA, Hudson; VIEIRA, Carlos Eduardo. Introdução à Interoperabilidade. Escola Nacional de Administração Pública. 2015. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/2399/1/M%C3%B3dulo_1_EPING.pdf> Último acesso em: 15.07.2020.

36. *Estudo da ONU revela que mundo tem abismo digital de gênero.* ONU News. 2019. Disponível em: <https://news.un.org/pt/story/2019/11/1693711#:~:text=O%20uso%20da%20Internet%20continua,popula%C3%A7%C3%A3o%20de%20todos%200%20mundo.> Último acesso em: 15.07.2020.

37. DOERK, Adrian. *The growth factors of self-sovereign identity*. Medium. 2020. Disponível em: <https://medium.com/@SSI_Ambassador/the-growth-factors-of-self-sovereign-identity-33aa3cc17ce7> Último acesso em: 15.07.2020.

38. WILSON, Chuck. *O papel do blockchain em um ecossistema de identificação em franca evolução.* Valid. 2018. Disponível em: <https://valid.com/pt-br/blockchainid_por/> Último acesso em: 15.07.2020.

Bibiografia

ALLEN, Christopher. *The path to self-sovereign identity*. Publicado em 25.04.2016. Disponível em: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.> Último acesso em: 04.02.2020.

ALLESSIE, David; SOBOLEWSKI, Maciej; VACCARI, Lorenzino. *Blockchain for digital government.* 2019. Disponível em: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government. Último acesso em: 10.03.2020.

AUGUSTO, Thaís. *CPqD quer utilizar o blockchain para dar mais segurança à identidade digital.* Canal Tech. 2019. Disponível em: <https://canaltech.com.br/blockchain/cpqd-quer-utilizar-o-blockchain-para-dar-mais-seguranca-a-identidade-digital-136101/I> Último acesso em: 08.07.2020.

Berryhill, J., T. Bourgery and A. Hanson (2018), *"Blockchains Unchained: Blockchain Technology and its Use in the Public Sector"*, OECD Working Papers on Public Governance, No. 28, OECD Publishing, Paris. Disponível em: <https://doi.org/10.1787/3c32c429-en.>

Binance Academy. *Casos de Uso Blockchain: Identidade Digital.* 2020. Disponível em: <https://academy.binance.com/pt/blockchain/blockchain-use-cases-digital-identity> Último acesso em: 01.07.2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Atos do Poder Legislativo, Brasília, DF, 15.08.2018. Seção 1, p. 59. Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/KujrwoTZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337> Último acesso em: 15.07.2020.

BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. Diário Oficial da União, Atos do Poder Executivo, Brasília, DF, 17.04.2020. Seção 1 - Extra, p. 1.Disponível em: <http://www.in.gov.br/web/dou/-/medida-provisoria-n-954-de-17-de-abril-de-2020-253004955> Último acesso em: 15.07.2020.

BRASIL. Proposta de Emenda à Constituição nº 17, de 2019. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757> Último acesso em: 15.07.2020.

BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6.387/DF – Distrito Federal. Relatora: Ministra Rosa Weber. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf> Último acesso em: 15.07.2020.

CAMERON, Kim. *The Laws of Identity*. 2005. Disponível em: <https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>. Último acesso em: 03.06.2020.

COÊLHO, Marcus Vinicius Furtado. *O direito à proteção de dados e a tutela da autodeterminação informativa*. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-28/constituicao-direito-protecao-dados-tutela-autodeterminacao-informativa#_ftnref3>. Último acesso em: 03.07.2020.

DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro*. São Paulo: Saraiva, 2007, p. 119-120.

DOERK, Adrian. *The growth factors of self-sovereign identity*. Medium. 2020. Disponível em: <https://medium.com/@SSI_Ambassador/the-growth-factors-of-self-sovereign-identity-33aa3cc17ce7> Último acesso em: 15.07.2020.

DONEDA, Danilo; KANASHIRO Marta. *O novo sistema brasileiro de identificação - traços exclusivos de uma transformação geral.* Politics. Setembro 2012. Disponível em: <https://politics.org.br/edicoes/o-novo-sistema-brasileiro-de-identifica%C3%A7%C3%A3o-tra%C3%A7os-exclusivos-de-uma-transforma%C3%A7%C3%A3o-geral>. Acesso em 15 out. 2019.

Estudo da ONU revela que mundo tem abismo digital de gênero. ONU News. 2019. Disponível em: <https://news.un.org/pt/story/2019/11/1693711#:~:text=O%20uso%20da%20Internet%20continua,popula%C3%A7%C3%A3o%20de%20todos%200%20mundo.> Último acesso em: 15.07.2020.

FAFT, *Public consultation on FATF draft guidance on digital identity.* 2019. Disponível em: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html.>

FRY, REINIERIS. *SSI? What we really need is full data portability.* 2020. Disponível em: <https://womeninidentity.org/2020/03/31/data-portability/> Último acesso em: 07.07.2020.

KANG, Margareth; DOS SANTOS, Maike Wille; DONEDA, Danilo. *Políticas de Identidade na era digital e o registro civil nacional.* 2016. Disponível em <http://opiniaopublica.ufmg.br/site/files/artigo/4-Margareth-Kang.pdf>. Último acesso em 15.10.2019.

KONOPACKI, Marco. *Blockchain e identidades digitais: caminhos para uma nova democracia.* ITS Rio. 2018. Disponível em: <https://feed.itsrio.org/blockchain-e-identidades-digitais-caminhos-para-uma-nova-democracia-7719b8ae5d0e> Último acesso em: 01.07.2020.

LAFER, Celso. *A reconstrução dos direitos humanos.* São Paulo: Companhia das Letras, 2003, p. 240.

Learning Machine. *Digital Identity.* Disponível em: <https://www.learningmachine.com/digital-identity/> Último acesso em 15.10.2019.

MELEIRO, Juan. *Identidade Auto-Soberana.* 2018. Disponível em: <https://medium.com/mosaicouniversity/identidade-auto-soberana-parte-1-35f3013da8e7> Último acesso em 15.10.2019.

MELLO, Ana Paula Pessoa; MESQUITA, Hudson; VIEIRA, Carlos Eduardo. *Introdução à Interoperabilidade.* Escola Nacional de Administração Pública. 2015. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/2399/1/M%C3%B3dulo_1_EPING.pdf> Último acesso em: 15.07.2020.

PAREJA, Alejandro; PEDAK, Mari; GÓMEZ, Carlos; BARROS, Alejandro. *A gestão da identidade e seu impacto na economia digital.* Banco Interamericano de Desenvolvimento. 2017. Disponível em: <https://publications.iadb.org/publications/portuguese/document/A-gest%C3%A3o-da-identidade-e-seu-impacto-na-economia-digital.pdf> Último acesso em: 26.06.2020.

PEREIRA, Caio Mario da Silva. *Instituições de Direito Civil - Volume I.* 30ª Edição. Rio de Janeiro: Forense, 2017. p. 216.

SARLET, Info Wolfgang; MARINONI, Luis Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional. 8ª Edição.* São Paulo: Saraiva Educação, 2019, p. 576.

SOVRIN FOUNDATION (2017). *The inevitable Rise of Self-Sovereign Identity.* Disponível em: <https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.> Acesso em: 10.04.2020.

SOVRIN FOUNDATION (2018). *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trus.* Disponível em: <https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf>. Acesso em: 1.04.2020

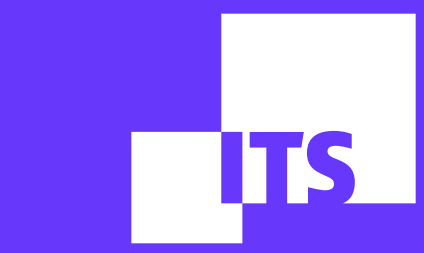
TEPEDINO, Gustavo; BARBOZA, Heloisa Helena; MORAES, Maria Celina Bodin de. *Código Civil Interpretado: Conforme a Constituição da República.* Rio de Janeiro: Renovar, 2014, 3.ed. p. 60-61.

Wang F and De Filippi P (2020). *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion.* Disponível em <https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full> Último acesso em: 15.07.2020.

WARREN, Samuel D.; BRANDEIS, L. D., *"The Right to Privacy".* Harvard Law Review ,vol. IV, 15 de dezembro de 1890.

WILSON, Chuck. *O papel do blockchain em um ecossistema de identificação em franca evolução.* Valid. 2018. Disponível em: <https://valid.com/pt-br/blockchainid_por/> Último acesso em: 15.07.2020.

WINDLEY, Philip. *How blockchain makes self-sovereign identities possible.* Computer World. 2018. Disponível em: <https://www.computerworld.com/article/3244128/how-blockchain-makes-self-sovereign-identities-possible.html> Último acesso em: 07.07.2020.



Acesse nossas redes

itsrio.org