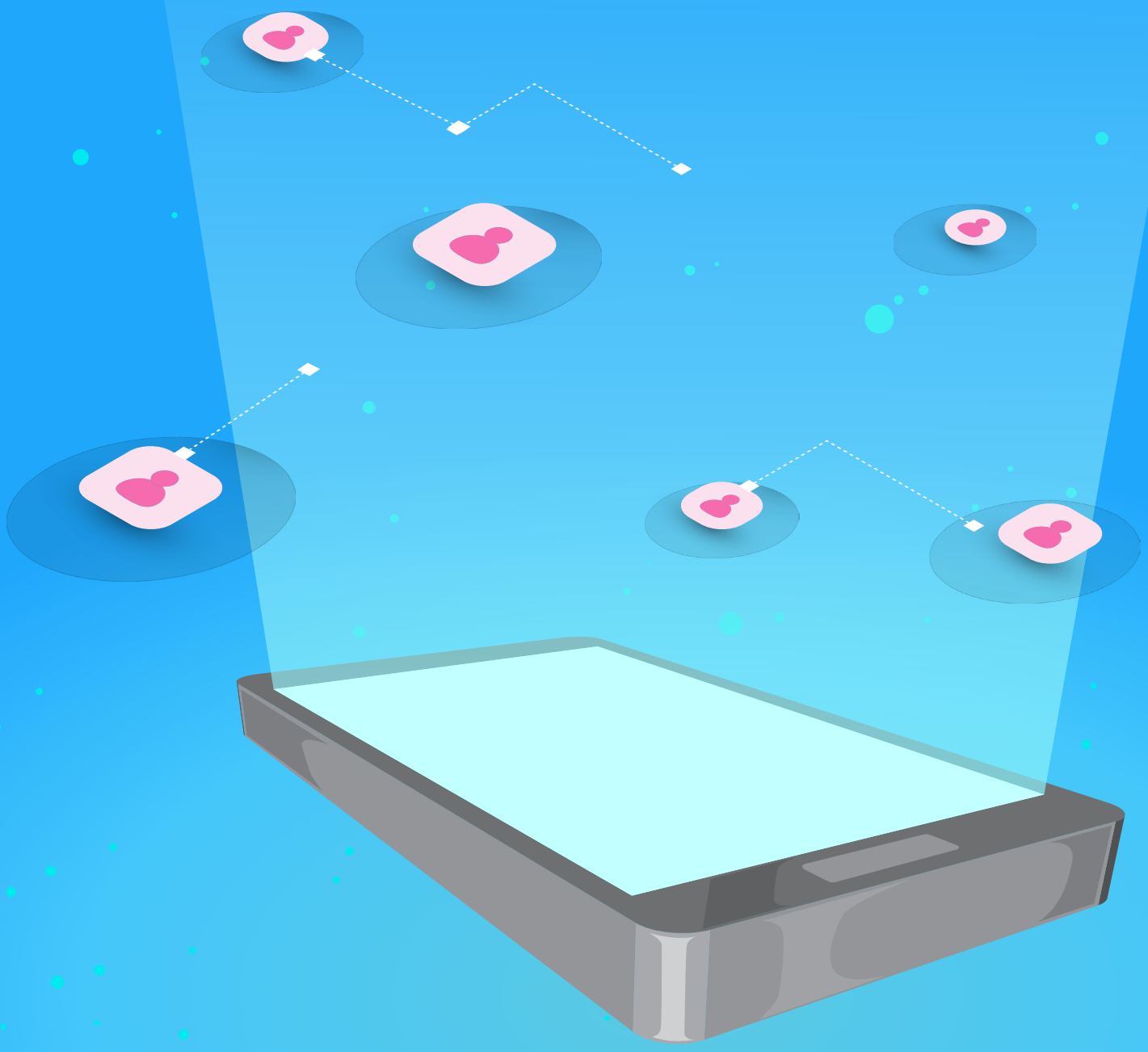
CARTILHA

Quem somos on-line?



REALIZAÇÃO

UNICO

LTS

sumário interarivo, clique para ser redirecionado.

Da identificação à autodeterminação: Entendendo a identidade digital

Inúmeras são as possibilidades de nos identificarmos e nos apresentarmos ao mundo. Para confirmarmos que nós somos realmente nós mesmos, existe um processo destinado a verificar essa informação, também conhecido como **identificação**.

Nossos **documentos oficiais**, como RGs, CPFs e passaportes, sem dúvida, nos auxiliam em tais procedimentos, mas, na maioria dos casos, eles precisam ser apresentados fisicamente e separadamente: um para cada ocasião. E qual o real custo disso? Aproximadamente **R$ 174,2 bilhões** são gastos anualmente em processos analógicos de identificação no Brasil, **o equivalente a 2% do PIB nacional.**

Vale dizer que, para além desse custo nacional, cada brasileiro gasta **entre R$ 487 a R$ 830 por ano** nos processos de identificação. Isso inclui despesas que exigem nossa presença física para identificação, incluindo a apresentação e assinatura de documentos.

Confira alguns desses gastos:

Processos de contratação de Recursos Humanos para cada brasileiro economicamente ativo	R$ 150,00
Fazer matrícula ou solicitar documentos em instituições de ensino para cada brasileiro com menos de 30 anos de idade	R$ 30,00
Gasto por adulto para realizar assinaturas ou efetivar registros de contratos de financiamento	R$ 61,00
Realizar a emissão de documentos e exercer direitos enquanto cidadão (como votar e fazer prova de vida) para cada brasileiro adulto	R$ 26,40
Deixar de retirar mercadoria por estar se documento	R$ 1,80
Ir ao branco para assinar documentos ou liberar cartões de credito ou debito por titular de conta	R$ 18,00
Deixar de fazer exame ou consulta médica por estar sem documento	R$ 4,00

Para agravar essa situação, existem pessoas que sequer têm prova de suas identidades, ou seja: não têm documentos oficiais. No Brasil, **cerca de 3 milhões de cidadãos** não possuem registro civil. Ao redor do mundo, **quase 1 bilhão de pessoas** vivem nessas condições de ausência de identificação formal.

A tecnologia, no entanto, tem avançado no sentido de servir como suporte para uma significativa melhora no cenário da identificação oficial no mundo todo. Não só para a identidade digital emitida pelo governo, mas para um ecossistema onde a identidade digital seja a base da confiança. No Brasil, **já há mais smartphones do que pessoas:** são **242 milhões de celulares inteligentes para 214 milhões de habitantes.** E, no mundo, estima-se que **3/4 da população mundial acima de 10 anos têm acesso a aparelhos celulares.** Por que celulares podem ajudar no problema da identificação?

Porque são dispositivos geralmente individuais, que oferecem conforto e potencial controle da identificação biométrica, além de permitirem que o usuário faça o input de mais informações que podem também ajudar na identificação.

Por isso, usar a tecnologia como suporte a favor da emissão de documentos de identificação pode levar a algo verdadeiramente transformador no acesso à cidadania e no aumento da eficiência. A progressiva e intensa digitalização da vida pode deixar no passado a realidade de processos analógicos tradicionais de identificação.

Assim, a chamada **identidade digital,** que é um conjunto de dados que identificam uma pessoa para fins de acesso ou transações, abre novos horizontes aos processos de validação de informações on-line, permitindo que as pessoas confirmem suas identidades de maneira mais simples e segura possível.

É biscoito ou bolacha? Diferenças entre identidade digital, credencial e outros elementos de identificação

A definição de **identidade digital** não é objetiva e depende de contextos e propósitos concretos. De forma ampla, seu conceito está atrelado a um conjunto de atributos capturados e armazenados eletronicamente.

A exemplo de **dados biográficos** (como nome, data de nascimento, endereço e filiação), **dados biométricos** (como varredura de íris, impressões digitais, face etc.) ou mesmo **credenciais** (informações sobre fatos relacionados à pessoa identificada, como certificados de cursos, licença para dirigir, etc.), muitos dados pessoais, ou conjuntos de dados pessoais, podem fazer parte da identidade. Para isso, o controle precisa estar na mão dos usuários.

Assim, a identidade digital é um mecanismo técnico voltado à identificação das pessoas. Além de ser mais conveniente e confiável, dispensa a necessidade de contato físico para a captura de informações.

E por que importa?

Há um padrão engessado nos processos de identificação tradicionais, ou seja, nos meios analógicos, a exemplo de solicitações frequentes de dados pessoais e a realização constante de cadastramento prévio para obter serviços, além da apresentação de documentos físicos. A cadeia de identificação de pessoas ainda é muito complexa, e os atores que participam dela muitas vezes não seguem padrões e normas que permitam a interoperabilidade, obrigando usuários a repetidamente ter que fornecer seus dados de novo.

Em razão disso, pessoas são obrigadas a entrar em sistemas que não se conversam para fazer algo que deveria ser extremamente simples, criando uma confusa rede de informações pessoais forjada com o único intuito de promover a identificação de alguém.

A ausência de **interoperabilidade** sistêmica impulsiona exigências cada vez maiores para atribuir confiabilidade nos processos de identificação. Além disso, cria inúmeras cópias dos dados, que ficam em "pontos cegos" dos usuários, que não tem como controlar os vários cadastros que fizeram para o acesso aos serviços.

Este cenário enfraquece valores caros como a **autodeterminação informativa** das pessoas, que é o direito de poder ter autonomia sobre suas informações e quem pode acessá-las. Isso porque a interoperabilidade entre sistemas é uma condição indispensável à concretização de direitos importantes ao titular de dados, como a portabilidade, possibilitando a transmissão e reutilização das informações pessoais.

Exemplo: Para entrar em uma boate, o estabelecimento precisa saber que aquela pessoa é maior de 18 anos. Quando a boate precisa confirmar esta idade, acaba obtendo acesso a diversos outros dados constantes de documentos de identificação, sendo que a única informação relevante é apenas a informação de que a pessoa está apta a consumir álcool, pois tem mais de 18 anos.

O que significa ter a soberania de nossa própria identidade?

A emissão de documentos feita digitalmente pode acontecer de acordo com a situação. Assim, no exemplo anterior, quando a pessoa estiver de posse de sua identidade digital, pode emitir uma credencial em seu celular confirmando que ela está apta para consumir álcool. A boate então só precisaria dessa informação, sem precisar coletar dados como data de nascimento, nome, número de cidadão, registro nacional etc.

A autogestão dos dados está no cerne das chamada **identidades autossoberanas**. Muitas vezes são instrumentalizadas por tecnologias emergentes, como a *blockchain*, ou por outras tecnologias já consolidadas. O importante é diminuir a manipulação desnecessária de dados ou informações pessoais, colocando o controle dos dados nas mãos das pessoas.

Se a identidade digital diz respeito a nós, a segurança deve estar em nossas mãos.

Caminhos que estão sendo trilhados

Nesse contexto desafiador, vale mencionar outra qualidade associada à identidade digital, que é chave para o seu uso em larga escala. Trata-se da Identidade Digital Descentralizada (DID), que é uma forma de identidade autossuficiente, ou seja, a pessoa ou entidade tem controle total sobre sua identidade sem depender de uma autoridade central.

A identidade digital descentralizada pode ser reutilizável, pois possibilita que a pessoa utilize sua identidade nos mais diversos ambientes, analógicos e digitais, para diversos contextos, de forma global, segura e confiável.

A identificação descentralizada (DID) e a identificação reutilizável são conceitos diferentes no contexto de identidade digital, mas podem ser complementares. As DIDs têm como base tecnologias de *blockchain* e utilizam técnicas criptográficas para garantir e gerenciar informações de identidade. Elas também proporcionam às pessoas a capacidade de criar, possuir e gerenciar suas informações de identidade digital.

Já a identificação reutilizável é quando uma única identificação digital, pode ser usada em várias situ-

ações ou serviços online sem a necessidade de criar identificações separadas para cada um.

Há duas abordagens para que estas técnicas sejam aplicadas:

1) um ecossistema integrado e descentralizado, que seria composto por três elementos:

i) **Identificadores descentralizados**, ou DIDs, são um tipo de identificador globalmente exclusivo que permite que uma entidade seja identificada de maneira verificável, persistente e que não requer o uso de um registro centralizado. Ao contrário de processos tradicionais de identificação, os DIDs podem ser dissociados de servidores centralizados e se tornarem independentes entre si. Seu design permite que o controlador de um DID prove seu controle sobre ele sem exigir permissão de qualquer outra parte.

ii) **Uma credencial verificável** é um documento com afirmações sobre o recurso de alguém, suas capacidades ou realizações (certificado, licença para dirigir etc.).

iii) ***Blockchain* ou registro descentralizado.**

2) protegido por PETs.

As PETs são tecnologias voltadas a tornar a privacidade **mais tangível para usuários de produtos e serviços.** Diversas são as técnicas e tecnologias que promovem essas adaptações, em respeito ao conceito princípio caro à sistemática de proteção de dados pessoais, **conhecido como *Privacy by Design*.**

Algumas metodologias PETs podem ser adotadas como formas de proteção de dados de identidades digitais:

Prova de conhecimento zero	Privacidade diferencial	Aprendizado de máquina federado
Método que permite uma parte provar a outra que uma determinada informação é verdadeira sem transmitir qualquer informação, além do fato de que a informação é realmente verdadeira.	Sistema que permite compartilhar publicamente bancos de dados, descrevendo padrões sobre os grupos existentes dentro dos conjuntos de dados, mas retendo informações sobre os indivíduos ao acrescentar "ruído" ao conjunto de dados.	Modelo que permite a análise e processamento de dados dentro dos próprios dispositivos finais, protegendo os dados granulares e permitindo processamento de dados extremamente sensíveis.

Voltando aos itens de uma identidade descentralizada: cada participante do ecossistema pode criar quantas credenciais verificáveis quiser, e a tecnologia permite usos separados para diferentes formas de relacionamento e contexto. Os dados são **totalmente controlados pelo proprietário da identidade.**

Atualmente, já existem desenvolvedores que utilizam as DIDs como uma técnica voltada à identificação pessoal, suportados por experimentos que empregam *blockchain* como suas fundações:

Decentralized Identity Foundation	***Hyperledger Foundation***	***IRMA***	***Sovrin***
Organização orientada por práticas de engenharia e focada no desenvolvimento dos elementos fundamentais para estabelecimento de um ecossistema aberto para identidade descentralizada, além de garantir a interoperabilidade entre todos os participantes.	Fornece ferramentas, bibliotecas e componentes reutilizáveis para identidades digitais enraizadas em *blockchains* ou outros registros distribuídos, garantindo, assim, sua interoperabilidade em domínios administrativos, aplicativos e qualquer outro sítio.	Significa *I Reveal My Attributes*. A IRMA permite que você divulgue on-line, por meio de seu celular, certos atributos pessoais (como ser maior de 18 anos), mas ao mesmo tempo oculte outros (como seu nome ou número de telefone). É, assim, uma ferramenta voltada para a privacidade.	Organização sem fins lucrativos fundada para administrar a Estrutura de Governança que rege a Rede Sovrin, um serviço público que permite identidades digitais auto-soberanas na Internet.

Considerações finais

As potencialidades das identidades digitais são imensas. Quando implementadas corretamente, podem levar a uma verdadeira explosão de oportunidades de conexão, trazendo ganhos em diversas interfaces do desenvolvimento socioeconômico global. Por exemplo, o potencial econômico de identidades digitais pode promover um **aumento de 13% do PIB do Brasil até 2030.** Segundo relatório realizado pela consultoria norte-americana Liminal, esse mercado deve crescer até 91% nos quatro próximos anos, impulsionado pelos setores de entretenimento, mídias sociais, turismo, economia compartilhada e saúde.

Entretanto, muitos também são os riscos atrelados. Sem uma política regulatória de proteção de dados adequada e funcional, o desvirtuamento do uso massivo de informações pessoais pode levar a desvios de finalidade e abusos de poder, tanto no setor público quanto no privado.

Pensando nisso, o Banco Mundial, juntamente com com o Centro para o Desenvolvimento Global **criaram 10 princípios para a identificação e o desenvolvimento sustentável**, pautados em três vertentes: inclusão, design e governança:

legenda: *inclusão* *design* *governança*

1.	Assegurar **cobertura universal** aos indivíduos, do nascimento à morte, livre de discriminações;
2.	Remover barreiras quanto ao acesso, uso e disparidades na **disponibilidade da informação e da tecnologia**;
3.	Estabelecer uma **identidade robusta**, única, segura e acurada;
4.	Criar uma plataforma que seja **interoperável** e responsável com as necessárias dos diversos usuários;
5.	Usar **padrões abertos**, garantindo a **neutralidade** da tecnologia e de seu fornecedor;
6.	Proteger a **privacidade** e os controles sob o design sistêmico;
7.	Planejar a **sustentabilidade** financeira e operacional sem comprometer a **acessibilidade**;
8.	Salvaguardar a privacidade dos dados, segurança e os riscos aos usuários por meio de uma **estrutura legal e regulatória compreensiva**;
9.	Estabelecer mandatos institucionais com ***accountability***;
10.	Reforçar a estrutura legal e a confiança por meio de uma **supervisão independente** com julgamento de reclamações.

A segurança, privacidade e inclusão devem estar no centro das iniciativas e transações que utilizam a identidade digital. É essencial adotar medidas rigorosas de proteção de dados para garantir que as informações pessoais dos usuários sejam armazenadas e transmitidas de forma segura. Além disso, a transparência na coleta e no uso dos dados é fundamental, pois viabiliza aos cidadãos o controle sobre suas informações e garante que elas sejam utilizadas apenas para os fins autorizados.

A identidade digital avançou muito nos últimos anos, mas essa jornada está apenas começando. À medida que a sociedade avança para uma economia cada vez mais digital, surgem novas demandas que, por sua vez, exigirão identificações mais eficientes e seguras. Na prática, a identidade digital é uma forma democrática de provar quem somos, gerando oportunidades de realizar interações de modo simples e seguro.

Este é o momento de construirmos programas que tenham impacto positivo nas próximas décadas para alcançarmos todo o potencial da identificação digital para a sociedade, os negócios e indivíduos. Tanto governos quanto empresas e demais instituições precisam incorporar desde já em seus programas os princípios da identidade digital que garantam privacidade, inclusão, valor, controle e segurança para as pessoas.

REALIZAÇÃO

UNICO

LTS