Junho, 2020

Good ID na América Latina

Fortalecendo usos apropriados da identidade digital na região

Autores
Alexandre Barbosa
Celina Carvalho
Cláudio Machado
Janaina Costa

Sumário

Agradecimentos

Gostaríamos de agradecer à Omidyar Network por financiar e apoiar esta pesquisa e nos conectar com a rede de colegas do Sul Global envolvidos no debate da identidade digital. Agradecemos também aos colegas do Centro de Internet e Sociedade (CIS) da Índia e do Centro de Propriedade Intelectual e Direito de Tecnologia da Informação (CIPIT) pelas discussões e cooperação. Estamos a caminho de fortalecer o movimento Good ID.

Especialistas

O seguintes especialistas contribuíram para esse relatório:

Fabro Steibel • Diretor Executivo, ITS Rio

Alejandro Barros • Consultor Internacional de Políticas Públicas de Desenvolvimento Digital

Edgar Vásquez Cruz • Provedor de soluções de TI

Evelyn Téllez Carvajal • Pesquisadora, INFOTEC México

Fernanda da Escóssia • Jornalista e professora universitária, IBMEC Rio

José Villalba • CEO, eID

Juan Carlos Lara • Diretor de Pesquisa e Políticas Públicas, Derechos Digitales

Miguel Arce • Gerente Comercial, Pagos Digitales Peruanos

Miguel Morachimo • Diretor Executivo, Hiperderecho

Raquel Chrispino • - Juíza de Direito, Tribunal de Justiça do Estado do Rio de Janeiro

Ricardo Saavedra • Gerente de Registro e Certificação Digital, RENIEC

Edição

Celina Bottino • Diretora de Projetos, ITS Rio

Clara Langevin • Consultora licenciada, Universidade de Columbia

Projeto de design

Ana Luisa Figueiredo • ITS Rio

Fotos

Tales Duarte • ITS Rio

Agência Brasil

Financiado por

OMIDYAR NETWORK

ITS Instituto de Tecnologia & Sociedade do Rio

Abreviações

AFIS	Sistema de Identificação Automatizada de Impressões Digitais
CadÚnico	Cadastro Único para Programas Sociais do Governo Federal
CEDN	Coordenação da Estratégia Digital Nacional
CEN	Certidão Eletrônica de Nascimento
CEV	Cartão Eletrônico de Vacinação
CR	Registro Civil
CRVS	Registro Civil e Estatísticas Vitais
CURP	Chave Única de Registro de População
CDD	Customer Due Diligence
DNI	Documento Nacional de Identidade
ID4D	Identidade para o Desenvolvimento
TIC	Tecnologias de Informação e de Comunicação
INFOTEC	Centro de Pesquisa e Inovação em TIC no México
KYC	Conheça Seu Cliente
MIS	Sistema de Gestão de Informação
NHDID	Identificador Digital de Saúde Nacional
OEA	Organização dos Estados Americanos
OECD	Organização para Cooperação e Desenvolvimento Econômico
OMS	Organização Mundial da Saúde
OPAS	Organização Pan-Americana da Saúde
PBF	Programa Bolsa Família
RENIEC	Programas de Protección Social
RCEV	Registro Civil y Estadísticas Vitales
RENIEC	Registro Nacional de Identificação e Estado Civil
ODS	Objetivos do Desenvolvimento Sustentável
SID	Sistema de Identidad Digital
SPP	Programas de Proteção Social
ONU	Organização das Nações Unidas
UNAIDS	Programa Conjunto das Nações Unidas sobre HIV/AIDS
UNESCO	Organização das Nações Unidas para a Educação, a Ciência e a Cultura
UNSD	Divisão de Estatística das Nações Unidas
UDHR	Declaração Universal dos Direitos Humanos

Resumo Executivo

Foto: Agência Brasil

Resumo Executivo

A transformação digital da economia e da sociedade é uma realidade. Assim, a identidade digital se destaca como um elemento essencial do futuro. Sob a mesma analogia, é preciso poder facilmente provar (ou demonstrar) digitalmente quem se é ou correr o risco de ser apagado oficialmente no futuro.

Embora traga muitas oportunidades, a transformação digital não é a panacéia para os problemas latino-americanos. Tecnologias disruptivas, abordagens inovadoras e principalmente as expectativas dos novos usuários entram no cenário em que os velhos problemas permanecem. Em relação à identificação, a população pobre e vulnerável continua enfrentando barreiras de acesso à documentação pessoal básica, práticas de proteção da privacidade e de dados fracas, sistemas de identificação altamente centralizados e pouca utilização da identificação como meio de melhorar a prestação de serviços.

Concomitantemente, o desafio de como identificar indivíduos e garantir seus direitos, deveres e controle sobre os dados aumenta. Além disso, a identificação pode variar consideravelmente em conceito, arranjos legais e organizacionais, infraestrutura operacional e tecnológica. Então, a identidade digital está se tornando um chavão, usada de maneira diferente de acordo com as agendas políticas.

Além disso, questões importantes como exclusão, discriminação e vigilância não podem ser negligenciadas. Estes foram usados como base para este relatório, adaptados à perspectiva latino-americana. O princípio norteador deste estudo é a inclusão, sendo a lente para nossa análise.

Com o aumento da adoção e promoção dos sistemas nacionais de identidade digital em todo o mundo, surgem preocupações particulares sobre como garantir seu uso apropriado. Tanto as abordagens setoriais como regionais precisam endereçar os desafios tradicionais e emergentes de inclusão e privacidade. Com financiamento e apoio da Omidyar Network, a equipe de Inovação da ITS, por meio de um projeto de pesquisa durante um ano, elaborou um quadro analítico para identificar sistemas regionais de “boas identidades”, do inglês Good ID, e promover estrategicamente práticas adequadas nos usos setoriais da identificação digital. Para tanto, esta pesquisa traça três objetivos principais:

- Investigar os usos apropriados da identidade digital em setores específicos, como as práticas atuais de identificação e as circunstâncias em que a identificação digital pode ser uma ameaça aos direitos dos indivíduos.
- Mapear princípios e determinar diretrizes para a concepção, ajuste e implementação da identificação digital para o desenvolvimento sustentável na América Latina. Portanto, colocando inclusão, sistemas seguros e boa governança no centro da agenda.
- Apoiar os formuladores de políticas e profissionais da América Latina na implementação dos princípios de um bom sistema de identificação, portanto inclusivo. Assim, fortalecer e consolidar o movimento Good ID no continente.

Para fundamentar nossos objetivos, realizamos uma vasta revisão da literatura para entender a identificação digital como um fenômeno e as partes interessadas envolvidas. Posteriormente, avaliamos os diferentes impactos e relações da identificação digital em casos de uso setoriais. Por fim, entrevistamos especialistas com uma abordagem multissetorial do México, Chile, Peru e Brasil para respaldar os estudos de casos específicos.

Nossos resultados são estruturados em casos de usos setoriais para melhor compreensão do funcionamento dos sistemas de identificação nesses contextos específicos e os respectivos impactos da identificação digital. Os setores selecionados foram serviços de governo digital, inclusão financeira, acesso à saúde e proteção social. Essa abordagem foi necessária devido à complexidade do problema. Estabelecer uma resposta única para todos os casos de usos setoriais seria uma abordagem frívola. Como principais sugestões para os usos apropriados nos setores, destacamos:

Serviços de Governo Digital

Agendas nacionais e regionais de governo digital vêm sendo desenvolvidas e implementadas por diversos países em todo mundo. A maneira como as pessoas “acessam” essas plataformas e o valor real dos mecanismos participativos é determinado por uma identificação digital. Assim, a identificação digital pode diminuir ou aumentar a distância entre Estado e sociedade, aumentar ou diminuir a confiança no setor público. Principais conclusões:

1. **Os Serviços de Governo Digital devem abranger, desde o primeiro passo, um sistema de identificação amplamente acessível que agregue valor ao usuário, simplificando procedimentos, reduzindo custos diretos e indiretos e possibilitando serviços de transação.**
2. **Estruturas de autenticação federada ou integrada que usam dados compartilhados de diferentes sistemas devem seguir e incorporar**

práticas robustas de transparência e informar os usuários sobre o tratamento de seus dados pessoais, de acordo com a lei nacional de proteção de dados ou, na ausência deles, seguindo as melhores práticas internacionais.

3. **Serviços digitais do governo devem alcançar os grupos mais vulneráveis; portanto, deve haver uma opção de identificação digital gratuita para esses usuários. Independentemente do nível de garantia exigido por um determinado serviço governamental digital, as credenciais digitais devem ser iguais e inclusivas para os usuários. Idealmente por meio de credenciais digitais gratuitas.**

Inclusão Financeira

A identificação é essencial para determinar a confiabilidade do cliente e reduzir fraudes. A identificação digital pode ser um facilitador de procedimentos eficientes e mais simples do *Know Your Customer* (KYC) - Conheça Seu Cliente - permitindo, assim, a inclusão financeira. Pode também apoiar políticas e sistemas de combate à lavagem de dinheiro e antiterrorismo. A temática ganhou mais atenção com a expansão do *open banking* (isto é, compartilhamento de dados financeiros e pessoais entre instituições financeiras) em todo o mundo. Principais conclusões:

1. **Os requisitos básicos de KYC devem idealmente ser gratuitos para a inclusão financeira da população alvo e fáceis de executar. É importante separar claramente quais são os dados básicos usados para identificar alguém das informações complementares necessárias para o acesso a serviços específicos e a devida diligência sobre o cliente.**
2. **Como o setor líder em identificação do ponto de vista tecnológico, as empresas de tecnologia financeira e os grandes bancos devem apoiar e ser os principais impulsionadores das tecnologias de aprimoramento da privacidade. Além disso, a inexistência de mecanismos de reparação, reclamação, e de acesso ao histórico dos dados são um importante indicador de práticas inadequadas, dada a maturidade tecnológica do setor.**
3. **Reguladores financeiros devem trabalhar em estreita colaboração com as autoridades de identificação e proteção de dados, garantindo a interoperabilidade com o sistema nacional de identificação.**

Acesso à saúde

A identificação envolve várias questões importantes, como o direito universal aos cuidados de saúde à segurança do paciente e à eficiência na prestação de serviços públicos. A identificação correta ajuda a impedir o tratamento inadequado de um paciente, por exemplo, atribuir ao paciente um medicamento no qual ele é alérgico. A identidade digital também pode facilitar a emissão de prontuários eletrônicos agregados e a geração de dados para apoiar políticas de saúde. Principais conclusões:

1. **Caso uma identificação nacional (digital) exclusiva para serviços de saúde seja estabelecida, esta poderá estar vinculada à identidade fundacional. A integração, no entanto, não deve permitir o acesso a dados médicos confidenciais por terceiros. Quando necessários para informações de saúde pública, os dados devem ser anonimizados, impedindo que o paciente seja reidentificado.**
2. **O acesso a serviços médicos de urgência, e não apenas emergências, nunca deve ser condicionado à identificação. O mesmo vale para identidade digital.**
3. **Métodos de identificação alternativos podem ser desenvolvidos para garantir a integridade do cadastro para políticas nacionais que dependem da identificação da população alvo (como programas de vacinação). A identidade digital poderia apoiar isso.**

Proteção Social

Muitas vezes, a identificação é necessária para provar a elegibilidade em programas sociais, como transferência de renda, pensões, cartões de alimentação, seguro social e outros. Todavia, aqueles que mais necessitam da assistência estão também entre os que não possuem um documento de identidade, incluindo camponeses, pessoas carentes e marginalizadas. A identidade digital é, portanto, reputada como forma de superar o problema para sistemas de identificação deficientes, com potencial para facilitar inscrição de beneficiários e transações de governo para pessoas. No entanto, especialmente nos países em desenvolvimento, isso pode levar à negligência do papel fundamental desempenhado pela documentação básica.

1. **Os governos devem criar um cadastro único para a proteção social, adotando uma perspectiva inclusiva da população vulnerável. É crucial simplificar e tornar os serviços de identificação mais acessíveis para a população não documentada, equilibrando os requisitos e as condições dos beneficiários.**

2. A integração de sistemas de gestão de informação e esquemas de identificação digital deve considerar o risco de excluir a população mais vulnerável e, ao mesmo tempo, atingir a efetividade das políticas públicas.
3. A adoção da tecnologia biométrica na proteção social precisa ser precedida de uma avaliação holística do sistema nacional de identificação, no qual os marcos institucionais e legais devem ser avaliados através das lentes da inclusão e da promoção de direitos, garantindo que os pobres e os mais vulneráveis não sejam excluídos.

Seção 1

América Latina e identificação na era digital

Foto: Agência Brasil

1. América Latina e identificação na era digital

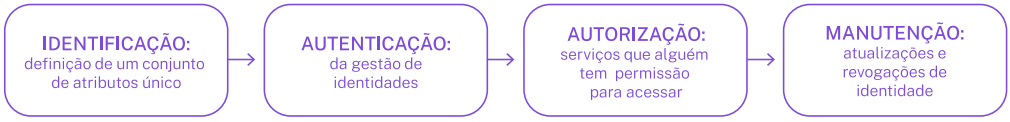
1.1. Um panorama da Identidade digital

Nas últimas décadas, duas perspectivas sobre a identificação de indivíduos na era digital se destacaram na literatura sobre o tema. Uma entende identidades digitais, combinadas com tecnologias emergentes, como uma ferramenta para vigilância em massa e, portanto, é vista com desconfiança. A outra, entende a digitalização dos sistemas de identidade como um meio de fortalecer os direitos e melhorar o acesso aos serviços.

O ponto é que identidade digital pode ter significados diferentes. Sua definição pode ser estabelecida como um conjunto de atributos armazenados e capturados eletronicamente (por exemplo: nome, sexo, data de nascimento e dados biométricos, como varredura de íris, impressões digitais, face, entre outros) e/ou credenciais (por exemplo: PINs, cartões de identificação, aplicativos móveis) que identificam exclusivamente uma pessoa. No entanto, apoiamos uma visão mais sistêmica de identidade digital. Para além da autenticação digital ou do login em um site, ou uma identidade legal digitalizada em um aplicativo móvel, certificados digitais ou registros de nascimento eletrônicos isolados.

Entendemos a ID digital como um mecanismo técnico para a identificação digital e segura de indivíduos, em que não há contato pessoal. Em um sistema de identidade fundacional (Banco Mundial, 2018d)[1], a identidade digital deve ser fundada em uma instituição responsável, uma legislação consistente e meios técnicos que permitam sua interoperabilidade com diferentes sistemas de informação. Em outras palavras, supõe-se que a identidade digital herda as mesmas características desejáveis da identificação civil, ou seja: inclusiva, acessível, portátil e persistente.

Fgura 1: Ciclo de vida do gerenciamento de identidades



Fonte: elaboração própria

A gestão tradicional de identidades geralmente é dividida em quatro etapas: (i) registro ou identificação, (ii) autenticação, (iii) autorização e (iv) manutenção. Cada uma tem estágios específicos. Por exemplo, a primeira abrange a emissão, o uso e o gerenciamento de identidades pessoais (incluindo a coleta de dados de identidade; validação por meio de prova e desduplicação de identidade; e emissão de credenciais). A identificação está relacionada ao processo de alguém declarar ou afirmar quem reivindica ser. A autenticação e autorização, por sua vez, são etapas distintas. Autenticação é a validação de identidade e deve garantir que uma pessoa seja real (ser-humano) e singular (única). Embora a identificação possa ser pública, a autenticação deve ser uma informação privada. A autenticação geralmente é associada a algo que se tem (por exemplo, um token físico), a algo que se sabe (por exemplo, uma senha) e a algo que se é (por exemplo, impressões digitais). O elemento "algo que se é" está se tornando cada vez mais relevante com a maturidade da tecnologia biométrica, como a identificação facial.

Ao verificar e autenticar um indivíduo em uma transação, é importante determinar a quais serviços específicos se pode ter acesso. O processo de determinação dessa elegibilidade é chamado de autorização. Cada um desses estágios se torna mais desafiador em sistemas totalmente digitais, ou mesmo híbridos. Por fim, a etapa de manutenção, associada à possibilidade de atualizar ou revogar identidades e credenciais.

Riscos e equilíbrio

Os esquemas de identidade digital estão submetidos a riscos de consequências adversas e subversão do seu propósito (Bhadra, 2019). Primeiramente, o próprio sistema pode ser distorcido e excluir parte da população, tal como violar direitos fundamentais, como acesso a serviços básicos e a privacidade. Portanto, há riscos de exclusão legal, cultural, econômica e tecnológica (Banco Mundial, 2019b).

Além disso, o fosso digital continua sendo uma barreira para muitos nos países em desenvolvimento e os baixos índices de educação digital geram riscos ainda maiores de exclusão das populações pobres e vulneráveis. Muitos projetos de identidade digital dependem de aplicativos móveis e, portanto, exigem níveis significativos de conectividade e acesso a dispositivos tecnológicos. Nesse sentido, se não forem cuidadosamente implementados e disseminados, esses programas tendem a aumentar o fosso digital e a desigualdade social (Ratcliffe, 2019).

Por fim, a sensibilidade dos dados pessoais deve ser destacada, especialmente ao tratar usos setoriais, em que pode ser agravada, como no setor de

saúde. O risco de uso indevido dessas informações aumenta com a digitalização. O acesso não autorizado ou uso indevido de informações pessoais pode reduzir a confiança, minar o direito à privacidade, discriminar e, em alguns casos, colocar grupos vulneráveis em risco (Banco Mundial, 2019b). De tal forma, deve-se buscar uma abordagem equilibrada, em que os riscos decorrentes da adoção de sistemas de identidade digital sejam mitigados.

Princípios

O Objetivo de Desenvolvimento Sustentável 16.9 da Agenda 2030 da ONU estabelece como meta fornecer identidade legal para todos, mas não há um modelo de sistema de identificação que sirva a todos, não existe 'receita de bolo'. É impraticável advogar por um padrão único de sistema de identidade digital, mas é crucial informar as partes interessadas sobre certos princípios orientadores, opções técnicas e boas práticas, para que o sistema possa ser mais adaptado às necessidades, os objetivos e o contexto.[2]

Os governos, órgãos internacionais multilaterais, setor privado e organizações da sociedade civil têm abordado os sistemas de identificação digital, seus potenciais riscos e oportunidades. Como resultado, alguns princípios foram estabelecidos para mitigar os riscos mencionados, bem como aprimorar os benefícios e oportunidades ao implementar um sistema de identificação digital.

Nesse sentido, destacamos o trabalho realizado pelo grupo de organizações internacionais coordenado pelo Banco Mundial e pelo Centro para Desenvolvimento Global, que contribuíram ao debate com os Princípios de Identificação para o Desenvolvimento Sustentável (Banco Mundial, 2016). Com objetivo de alcançar profundos resultados, os princípios orientadores foram sistematizados em três pilares: i) promover a inclusão, por meio da cobertura e acessibilidade universal da identidade; ii) estabelecer um design preciso, seguro, responsivo e sustentável; e iii) garantir boa governança e criar confiança, protegendo a privacidade e os direitos do usuário.

Para mais, o movimento Good ID, uma coalizão multissetorial, auxilia políticas, projetos de tecnologia e práticas sobre o assunto mundialmente[3], advogando por sistemas que garantam privacidade, inclusão, valor, controle e segurança para o usuário.

Essa pesquisa busca justamente contribuir para a compreensão e promoção desses princípios nos usos setoriais da identidade digital no contexto latino-americano.

Usos setoriais de identidade digital

Há uma distinção entre sistemas de identidade "funcionais" e "fundacionais". Os sistemas funcionais emitem identificações com objetivo de servir a uma função específica, em determinado setor. Estes sistemas autorizam ou outorgam acesso a um serviço específico, podendo ou não se vincularem à sistemas de identificação com outras finalidades. Qualquer pessoa pode ter várias identidades funcionais (por exemplo, carteira de motorista, cartão de saúde, título de eleitor). Os sistemas fundacionais, diversamente, têm como objetivo principal proporcionar a identidade como um bem público, sem conectá-la a um serviço específico.[4] A identidade fundacional é uma abordagem integrada da certidão de nascimento e a identificação civil.

Os sistemas de identidade digital têm características, funcionalidades e riscos diferentes de acordo com o seu uso. Neste relatório, apresentaremos alguns exemplos, abordando seus usos no contexto do governo digital, serviços financeiros, acesso à saúde e proteção social.

Apesar de existirem outros casos de uso setoriais para identificação digital, não serão aprofundados neste estudo. Por exemplo, muitos países associam sua identificação civil à agenda eleitoral. Um caso pragmático é o sistema de votação eletrônica da Estônia. Quanto aos sistemas tributários, a identificação digital tem potencial para facilitar a cobrança e o pagamento de impostos em transações entre pessoas e governo (*People to Government*, P2G) e impedir a evasão fiscal. Portanto, tem o condão de catalisar a capacidade estatal (Gelb, A. *et. al.*, 2020). Esses são apenas alguns dos muitos usos práticos para identidades digitais.

1.2. Inclusão como elemento central

A identidade é um direito que deve ser estendido a todos. Todavia, isso não significa que a identificação deva ser obrigatória; mas quem deseja ser identificado pelo sistema, deve ter meios para tanto.

O direito à identidade não é apenas um "passaporte" para outros direitos, como também é um direito em si. A identidade está intrinsecamente ligada ao direito à nacionalidade e ao reconhecimento em todo lugar do indivíduo perante a lei. Estes são reconhecidos como direitos humanos pela comunidade internacional (Declaração Universal dos Direitos Humanos, 1948) e devem ser protegidos por estruturas legais e institucionais robustas.

Registro Civil e Estatísticas Vitais

De acordo com a Divisão Estatística das Nações Unidas (United Nations Statistics Division, UNSD), o registro civil e as estatísticas vitais (Civil Registration and Vital Statistics, CRVS) são registros contínuos, permanentes, obrigatórios e universais da ocorrência e características dos eventos vitais da população, de acordo com a lei.

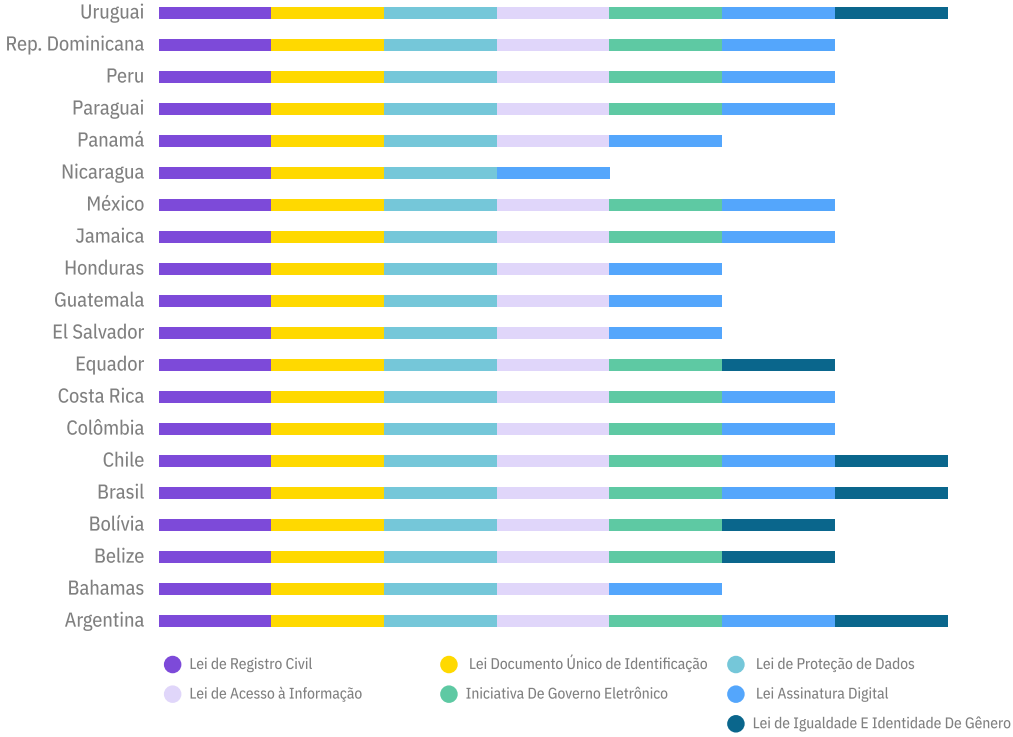
Vincular CRVS e ID é uma recomendação do Grupo de Especialistas em Identidade Legal da ONU, por desempenhar um papel crucial em uma estrutura legal. Registro civil se trata do meio oficial para provar as informações biográficas necessárias para assegurar muitos direitos humanos, como o direito a um nome e à filiação. Além disso, ao integrar o registro civil e a identificação civil, é possível uma obter visão holística (do começo ao fim) dos indivíduos, mostrando como um vínculo orgânico entre os sistemas poderia melhorar os serviços de gerenciamento de identidades e impulsionar a prestação de serviços aos cidadãos.

No entanto, em alguns contextos, esta integração pode ser complicada.

Os países da América Latina possuem legislações bastante avançadas e abrangentes em identificação e proteção de dados. Em uma visão geral do quadro legislativo, a tabela a seguir mostra quais países regulam i) o registro civil; ii) a emissão de um único documento de identificação; iii) a proteção de dados pessoais; iv) acesso à informação; v) governo eletrônico; vi) assinatura digital; vii) igualdade e identidade de gênero. Os sistemas de identificação digital oferecem novas possibilidades, mas também sujeitam os indivíduos a mais riscos. (fig. 2)

Embora o reconhecimento institucional da identidade como direito e a legislação de proteção de dados sejam essenciais, podem ser necessárias salvaguardas complementares para garantir a conformidade e um sistema inclusivo de identificação digital. Por exemplo, é fundamental ter uma abordagem centrada no usuário, colocando os indivíduos no cerne da identidade digital e garantindo o controle para quando, como e se eles desejam afirmar suas identidades no meio digital (GSMA, 2016). Essas salvaguardas devem ser enraizadas em uma estrutura institucional e legal mais ampla que as soluções tecnológicas isoladas, mas da perspectiva da proteção de direitos e da inclusão socioeconômica.

Figura 2: Marcos legais por país



Fonte: Adaptado de Registro Civil e órgão de identificação: análises e fichas de países, Banco Interamericano de Desenvolvimento (BID), Estefania Calderón, 2019, <*Registros civiles y oficinas de identificación: análisis y fichas de país*>

Vale ressaltar que, em alguns contextos e em muitos exemplos históricos a identificação pode colocar um indivíduo em risco de violência ou exclusão. Intencionalmente ou não, os esquemas de identificação podem facilitar a perseguição de grupos pertencentes a uma determinada religião, etnia, sexo ou ideologia política, bem como contribuir para a estigmatização dos indivíduos (por exemplo, exposição de estados de saúde e de doença ou situação de vulnerabilidade econômica, na intenção de provar elegibilidade em um benefício social).

A digitalização não elimina os riscos acima mencionados e pode adicionar outros. Os esquemas de identificação digital podem adicionar riscos perceptíveis de exclusão a populações pobres e vulneráveis. O acesso e a educação digitais são fundamentais. No entanto, a lacuna digital continua sendo um desafio em todo o mundo, especialmente nos países em desenvolvimento. É por isso que é fundamental ter um design claro da identificação digital para promover a inclusão em todas as suas dimensões e fortalecer as

salvaguardas de todos os indivíduos. Um sistema não pode ser classificado como de "boa identificação" sem endereçar esses pontos.

Cobertura universal

Os Objetivos Globais das Nações Unidas para o Desenvolvimento Sustentável exigem que todos os indivíduos tenham uma prova legal de sua identidade até 2030 (alvo 16.9). Ao estabelecer esse objetivo, as Nações Unidas não tornaram obrigatórios os esquemas de identidade para todos, mas reconheceram o direito à identidade de todos os indivíduos. A diferença entre cobertura universal e identidade obrigatória não é um jogo de palavras. Uma implementação de Good ID significa um esquema de identidade digital que permite que todos os indivíduos participem plenamente da sociedade e economia em que vivem. No entanto, é notório que o processo enfrenta muitos desafios importantes para ser inclusivo ao invés de excludente.

Além disso, a tecnologia da informação e comunicação (TIC) e a infraestrutura de dados do país são elementos críticos. Um nível mínimo de infraestrutura de TIC para o fornecimento de identidade digital deve ser considerado de uma maneira que permita incluir todos os residentes de um país. As políticas também devem considerar populações remotas que têm baixas taxas de acesso à infraestrutura e sofrem com o fosso digital.

Multicanal e prioridades

Identidades digitais e mecanismos tradicionais de identificação podem coexistir. A substituição completa de documentos pessoais físicos por um esquema digital pode não ser possível em muitos países. Ao mesmo tempo, os indivíduos também devem ter acesso a meios alternativos de identificação e escolhas na forma como se identificam. Portanto, uma abordagem multicanal deve ser considerada em países onde não há garantia de um nível mínimo de infraestrutura de TIC em todo o território nacional.

Um ponto de atenção para esse sistema híbrido é que ele pode iniciar um processo de diferenciação entre aqueles que têm acesso aos serviços habilitados para ID digital e aqueles que são mantidos no sistema físico. Por exemplo, se os serviços digitais fossem mais eficientes do que os serviços presenciais, isso aumentaria a desigualdade gerada pelo divisor digital.

Equilíbrio de gênero

A prova de idade e identidade pode ser crucial para garantir a independência e a inclusão financeira das mulheres, além de ser uma ferramenta para proteger meninas do casamento[5] e do trânsito infantil. No entanto, a desigualdade de gênero está muito presente nas estatísticas de inclusão,

registro civil e registros vitais. De acordo com o Centro de Excelência para Sistemas de Registro Civil e Estatísticas Vitais, as mulheres são negativamente mais afetadas pelos registros de óbito e sujeitas a maiores dificuldades em registrar seus filhos do que os homens (Centro de Excelência para Sistemas CRVS, 2020).

Isso significa que eles enfrentam maiores barreiras e são sub-representados em estatísticas vitais, como as utilizadas nas políticas públicas para reduzir a mortalidade feminina, por exemplo. Além disso, são necessários registros de casamento, divórcio e óbito para que as mulheres obtenham benefícios de pensão e reivindiquem direitos de herança. A digitalização da identidade deve abordar essas preocupações.

Acessibilidade

Um bom sistema de identificação é projetado para o seu contexto e garante o acesso adequado aos usuários e o funcionamento decente do sistema. Quando esses aspectos falham, grande parte da sociedade pode ser excluída do acesso a serviços vitais. Portanto, é importante considerar qual deve ser o padrão mínimo para infraestrutura e como o sistema abordará especialmente as minorias e os indivíduos vulneráveis. Ou seja, não deve excluir por defeito as pessoas que têm um nível mais baixo de educação digital[6] ou aquelas com dificuldades socioeconômicas no acesso à mídia digital, como comunidades rurais, ribeirinhas, indígenas e quilombolas.

1.3. Identificação digital na América Latina

A América Latina desempenhou um papel importante no desenvolvimento de tecnologias modernas de identificação, especialmente no aprimoramento da datiloscopia (impressões digitais) (Ferrari, 2015). Juan Vucetich e seus colaboradores em La Plata, Argentina, aprimoraram o método e projetaram uma nova perspectiva sobre o uso de impressões digitais em um contexto não-criminal.[7] A datiloscopia foi mais simples de usar e mais eficaz que a Bertillonage, criada por Alphonse Bertillon na França, resultando em sua adoção no século XX como o método oficial de identificação criminal e civil em quase todos os países da América Latina. A abordagem de Vucetich foi a referência hegemônica antes que a identificação começasse a ser automatizada usando o Sistema Automatizado de Identificação de Impressões Digitais (*Automated Fingerprint Identification System*, AFIS) durante a década de 1970. Isso mostra que a América Latina sempre esteve aberta a inovações em tecnologia de identificação; portanto, logicamente, os atores da região estão atualmente procurando desenvolver e aplicar IDs digitais em muitos setores.

Dito isto, o sucesso de qualquer programa nacional, digital ou não, depende muito do processo e do contexto, e não da tecnologia. A situação política do país e a capacidade do governo de implementar um determinado sistema não podem ser negligenciadas. Além disso, outros fatores a serem considerados são também meio ambiente, cultura, histórico de conflitos e níveis de pobreza. Assim, nesta seção, apresentamos uma visão geral da inter-relação desses fatores e identidade na região.

Aspectos regionais e culturais da identificação

A identificação das pessoas pode ser percebida como um direito *per se* ou, inversamente, como base do direito à privacidade. Os países latino-americanos, em seu próprio contexto histórico, também atravessaram essa dicotomia no desenvolvimento de seus sistemas de identificação. Ao contrário de outros países do Sul Global, a América Latina tem uma cultura, religião e herança colonial muito semelhantes. Esse terreno comum se reflete na maneira como a identificação é percebida na região.

Quarenta anos antes da Declaração Universal dos Direitos Humanos das Nações Unidas, Vucetich (1916) mencionou"o direito a um nome". Seja um anacronismo histórico ou não, e independentemente de uma definição precisa de "direito à identidade", é inegável que a argumentação de Vucetich foi muito inovadora em comparação com os pioneiros de outras formas e sistemas de identificação. Argumentou durante a elaboração do Registro da Lei de Identidade Popular, na Argentina, que a identificação de todos os habitantes, sem distinção, seria um passo importante para garantir o cumprimento do direito de nomear e garantir o funcionamento eficaz das instituições do Estado e, consequentemente, para o bem da sociedade. O momento pode ser percebido como o marco do direito à identidade na região.[8]

Além disso, a antropóloga Mariza Peirano questionou os significados sociais e culturais dos documentos pessoais no Brasil (Peirano, 2009). Sua pesquisa adotou uma abordagem inovadora e destacou que os documentos não se limitavam ao uso formal e burocrático, mas tinham um grande significado simbólico para as pessoas. O Cartão de Registro de Emprego e Segurança Social é muito mais do que um livro de registro de emprego, divide a população em pessoas honestas e "vagabundos" (vagabundos). Ela conclui que "documentos criam o cidadão", na percepção subjetiva das pessoas.

Nesse sentido, o trabalho de Fernanda da Escóssia é muito relevante para o tema na América Latina (Escóssia, 2019a). Sua pesquisa de doutorado foi sobre a vida de pessoas não registradas na cidade do Rio de Janeiro. Ela investiga a percepção de um indivíduo quando não possui uma prova legal de identidade, demonstrando que ele não se vê como ser humano.

"(...) eu descobri que essas pessoas se sentiam muito privadas da noção de 'eu sou uma pessoa', 'eu tenho direitos'. Muitos deles costumavam me dizer que se sentiam 'como um cachorro'... 'eu não sou ninguém'. Ela enfatizou que o registro civil é uma pré-condição para um 'senso de melhor existência'" (Escóssia, 2019b).

Prova de identidade, nesse sentido, não é apenas possuir um pedaço de papel ou um aplicativo móvel. É a possibilidade real de ter sua existência oficialmente reconhecida pelo Estado. Como demonstra sua pesquisa, para muitos dos que não possuem registro civil, obtê-lo é um passo no caminho da dignidade.

No entanto, é importante destacar que a governança de identidades na região geralmente é realizada por uma autoridade central de identificação para registro e emissão de credenciais. Infelizmente, como a maioria dos países latino-americanos era governada por ditaduras na segunda metade do século passado, os sistemas de identificação eram frequentemente apropriados para vigilância e perseguição (por exemplo, a identificação biométrica facilitava a identificação de opositores ao regime). Assim, a história paradoxal da identificação nos países latino-americanos mostra como a identificação pode ser usada para bons e maus propósitos.

A digitalização da identificação na região

Como indicado anteriormente, a primeira etapa de um sistema de identidade legal é o registro civil do indivíduo. Nesse sentido, dados da UNICEF mostram que a América Latina ainda enfrenta um grande desafio para alcançar o registro universal de nascimentos (UNICEF, 2016). (fig. 3)

Na América Latina, existe um número significativo de grupos minoritários étnicos. Um estudo realizado pela Organização dos Estados Americanos (OEA) concluiu que o principal fator que afeta o sub-registro foi a existência de barreiras legais para o cadastro usando nomes étnicos (OEA, 2008). No mesmo tom, o relatório da UNICEF também destaca como certos grupos podem enfrentar barreiras adicionais a serem incluídas no registro civil (UNICEF, 2016). Vale ressaltar que as crianças rurais da região amazônica representaram aproximadamente 10% das crianças sem identificação em 2015 (Center for Global Development, 2017b). Isso mostra como o próprio processo de registro geralmente não tem sensibilidade para fornecer a inclusão de populações indígenas e ribeirinhas. As diferenças urbano-rurais também mascaram disparidades subjacentes mais profundas, principalmente relacionadas à pobreza. Além disso, populações excluídas, como migrantes sem documentos, geralmente desconhecem seus direitos em relação ao registro de nascimento ou podem relutar em registrar seus filhos

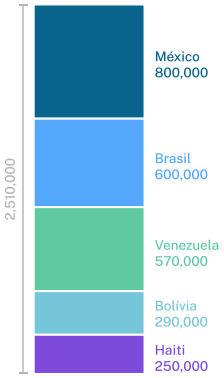
Figura 3: Estatísticas de registro de nascimento na América Latina

Os nascimentos de cerca de 3 milhões de crianças com menos de 5 anos de idade na América Latina e no Caribe nunca foram registrados.

Percentual de crianças menores de cinco anos cujos nascimentos estão registrados e número de crianças menores de cinco anos cujos nascimentos não estão registrados.

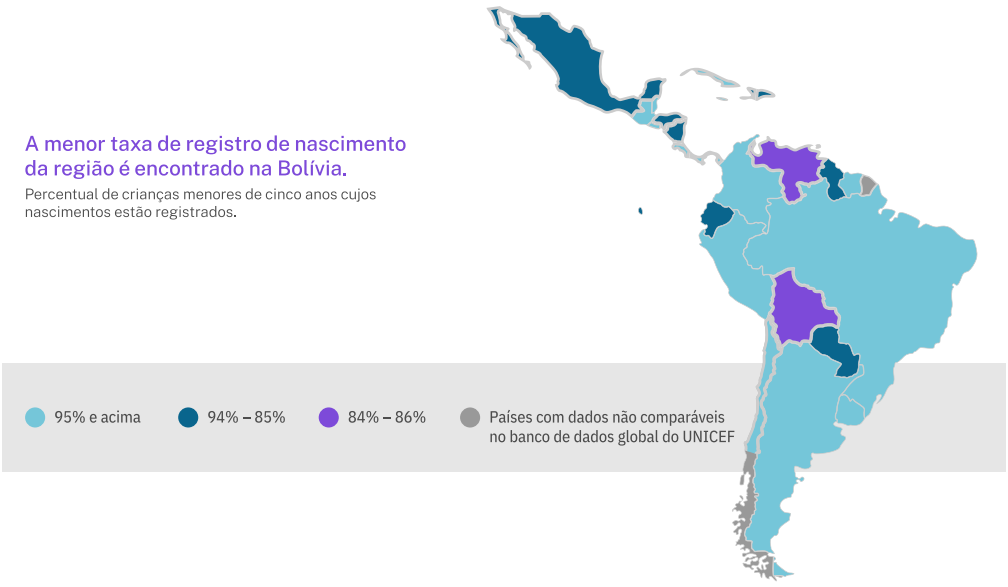
1 em cada 4 crianças sem registro de nascimento na região vive no México

Número de crianças menores de cinco anos cujos nascimentos não estão registrados, nos cinco países com o maior número de crianças não registradas na região.



A menor taxa de registro de nascimento da região é encontrado na Bolívia.

Percentual de crianças menores de cinco anos cujos nascimentos estão registrados.



Fonte: Reproduzido de Registro de nascimento na América Latina e no Caribe: fechando as lacunas, UNICEF, 2016, <Birth Registration in Latin America and the Caribbean: Closing The Gaps>

por medo de deportação para seu país de origem (UNICEF, 2016). Essas barreiras de acesso geralmente permanecem ou aumentam com a identificação digital, sendo que esta ganhou importância como chave para acessar direitos e serviços no mundo digital.

Além disso, a necessidade de melhorar a gestão pública e responder às necessidades dos cidadãos também está impulsionando a promoção da identidade digital como uma ferramenta essencial para a inclusão e redução dos custos de transação em toda a economia, contribuindo para a melhoria da qualidade dos serviços, tanto no setor público quanto no setor privado (BID, 2019; BID, 2017).

Figura 4: Nos países com níveis gerais mais baixos, o registro de nascimento é mais comum nas áreas urbanas do que nas rurais; onde os níveis são mais altos, as disparidades devido ao local de residência diminuem

Porcentagem de crianças abaixo de cinco anos com registro de nascimento por área de residência.

Fonte: Reproduzido do Birth Registration in Latin America and the Caribbean: Closing The Gaps, UNICEF, 2016, <Birth Registration in Latin America and the Caribbean: Closing The Gaps>

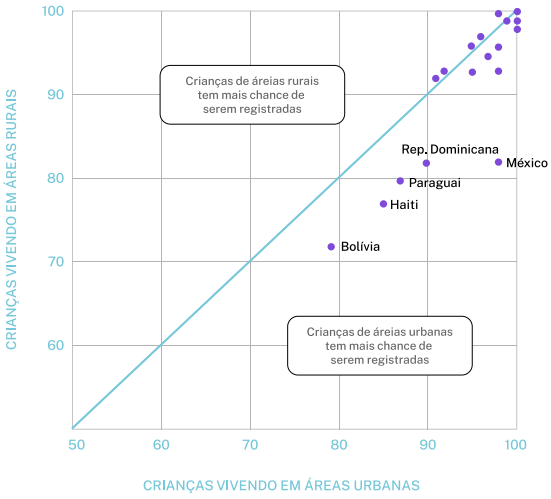
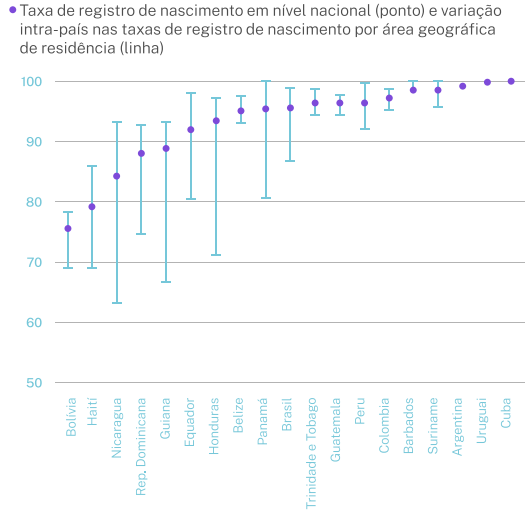


Figura 5: A prevalência nacional de registro de nascimentos pode ocultar importantes disparidades geográficas

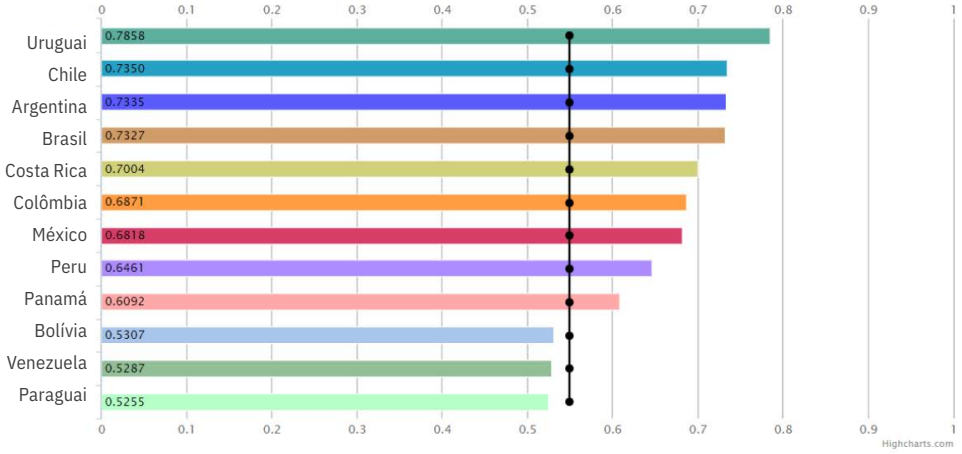
Percentual de crianças menores de cinco anos cujos nascimentos estão registrados e a área geográfica com os níveis mais alto e mais baixo de registro de nascimento.

Fonte: Reproduzido do Birth Registration in Latin America and the Caribbean: Closing The Gaps, UNICEF, 2016, <Birth Registration in Latin America and the Caribbean: Closing The Gaps>



Dito isto, a transformação digital está em todos os lugares, inclusive nos países da América Latina. Apesar das semelhanças regionais, o ritmo e o impacto da digitalização na sociedade e no setor público são proporcionais aos índices de desenvolvimento humano. Por exemplo, o índice de desenvolvimento do governo eletrônico das Nações Unidas[9] demonstra que países como Uruguai (que possui um índice muito alto), Chile, Argentina, Brasil e Costa Rica pontuam mais de 0,7 em 1; em outros, é realmente baixo, como Haiti (0,34) e Nicarágua (0,42)[10]

Figura 6: Índice de Desenvolvimento do Governo Eletrônico da ONU



Fonte: Reproduzido do Latin America at the United Nations Electronic Government Index (2018). <https://www.un.org/development/desa/publications/2018-un-e-government-survey.html>

Em relação ao registro e identificação civil, o desenvolvimento de novas soluções e serviços que facilitem a verificação e autenticação dos dados de identidade não apenas permitiria aos cidadãos acessarem facilmente os serviços, mas também facilitaria a coleta de informações usadas para melhorar o planejamento governamental e o gerenciamento de mais programas e serviços específicos (BID, 2019).[11]

Um número significativo de órgãos de identificação e registro pode funcionar de forma digital em muitos países da América Latina, mas o uso de livros de registro ainda não foi eliminado. Inclusive, em algumas regiões, o arcabouço jurídico exige que o registro de eventos vitais seja mantido em livros físicos.[12] (fig. 7)

Na Argentina, o documento de identidade nacional foi fortalecido pelo sistema de identidade digital (SID). O Uruguai melhorou consideravelmente o desempenho do seu governo digital, tornando-se um dos países líderes

Figura 7: Tipo de respaldo documental nos registros civis por país

Fonte: Adaptado do Civil Registries and Identification Offices: Analysis and Country Records, Inter American Development Bank (IADB), Estefania Calderón, 2019, <Registros civiles y oficinas de identificación: análisis y fichas de país>

da América Latina nesse campo. Desde 2007, o país possui um plano de digitalização do governo e, como resultado, oferece uma identidade digital gratuita para todos os seus cidadãos. Além disso, espera-se que até o final do ano de 2020 100% dos uruguaios tenham uma identidade digital. O governo peruano desenvolveu recentemente um documento eletrônico de identidade nacional (DNI-e), um cartão contendo um chip com chaves criptográficas de autenticação incorporadas.

Apesar do lado oposto do uso da identificação biométrica em regimes autoritários, a população latino-americana tende a preferir a autenticação biométrica devido à percepção de facilidade de uso pelos usuários (Mastercard, 2019b). De fato, o relatório foi conduzido por uma empresa externa com fins comerciais, mas ainda fornece informações úteis sobre o desenvolvimento futuro da identificação digital na região.

No entanto, vale enfatizar, uma parte significativa da população da América Latina ainda não tem acesso à infraestrutura básica, o que é condição prévia para a implementação adequada dos sistemas de identidade digital.[13] A precariedade de infraestruturas de eletricidade, telecomunicações e de dados aumentam o fosso digital entre o campo e as áreas urbanas (Domínguez, 2018), bem como as altas taxas de analfabetismo (UNESCO, 2009) são desafios fundamentais. O relatório da UNESCO (2017)[14] indica que mais de 200 milhões de latino-americanos permanecem offline. Por outro lado, os países da região adotaram medidas significativas em direção à digitalização (OCDE, 2019a).

1.4. Abordagem

Desde o início de nossa pesquisa procuramos entender as situações em que a identidade digital deve ser requerida, de que maneira e por quais atores. Após várias rodadas de discussões e workshops, a necessidade de aprofundar o estudo sobre sistemas de identificação tradicionais para tratar a temática de identidade digital ficou evidente. Isto considerando as maneiras pelas quais a identificação diverge entre setores, bem como a identidade digital afeta e é impactada em cada uso setorial. De tal forma, usamos uma lente de risco e direitos humanos nesse processo e focamos em desenhar recomendações para salvaguardar transformações digitais sustentáveis da identificação.

As perguntas gerais da pesquisa foram:

- Quais são os usos apropriados da identificação digital no setor?
- Como a identificação digital pode ser usada para promover o desenvolvimento sustentável da América Latina?

Para respondê-las, questionamos durante o processo de análise setorial de casos de uso:

- Qual o papel da identificação no setor?
- Como ocorre a identificação no setor e qual a sua relação com a identidade legal?
- Qual é o diagnóstico do setor na América Latina?
- Quais são os riscos da identificação digital no setor e como mitigá-los?
- Em quais circunstâncias a identificação digital deve ser solicitada no setor?

Para responder a essas perguntas, dividimos nossa abordagem em três etapas: (1) revisão da literatura; (2) análise setorial de casos de uso; (3) estudos de caso (ver detalhes do Anexo I). Além disso, a análise de cada estudo de caso identifica os paradigmas de uso e riscos apropriados associados e as formas de avançar em direção a um esquema de boa identificação.

Seção 2

Usos Setoriais no Contexto Latino-Americano

Foto: Tales Duarte

2. Usos Setoriais no Contexto Latino-Americano

2.1. Serviços de Governo Digital

Os Serviços de Governo Digital se referem ao uso de tecnologias digitais, como parte integrante das estratégias de modernização do governo.[15] A digitalização de serviços públicos (por exemplo, declaração de impostos, renovação de credenciais, agendamento de compromissos, atualização de informações pessoais, obtenção de autorizações e certificações, entre outros) não é uma novidade. Ela acompanha o desenvolvimento e a maturidade da Internet principalmente desde a virada do milênio. Inicialmente, era conhecida como governo eletrônico e foi recentemente renomeada para governo digital (OCDE, 2019d).

Para permitir a digitalização dos serviços públicos, os governos investem há muito tempo em métodos de identidade e autenticação digital que garantam acesso fácil, seguro e legítimo aos seus cidadãos.

O Papel da ID nos Serviços de Governo Digital

Tradicionalmente, os serviços governamentais são prestados pessoalmente e sujeitos a identificação para a prática de certos atos, como declaração de impostos, renovação da carteira de motorista, agendamento de vacinas, por exemplo. Devido à transformação digital, a identidade digital é um facilitador essencial dos serviços de governo digital. Um sistema de identificação digital bem implementado, que ofereça um alto nível de garantia e adote recursos e protocolos avançados de segurança para proteger dados de identificação e pessoas é fundamental para ususfruir dos possíveis benefícios para o setor. Isso inclui economizar dinheiro e tempo na execução de procedimentos burocráticos, mas também aproximar as pessoas das decisões políticas, adicionando segurança e confiança para ampliar o processo participativo (OCDE, 2019c).

A identidade digital contribui para facilitar o exercício da cidadania e do envolvimento político possibilitando, por exemplo, canais de consulta digital. Um sistema de identificação digital confiável e seguro é essencial para garantir a legitimidade do processo de consulta. O mesmo pode ser aplicado para facilitar mecanismos de participação direta, como referendo, plebiscito ou propostas legislativas, como no caso do aplicativo Mudamos.[16]

Métodos de Identificação e Possibilidades para Serviços de Governo Digital

A identificação em serviços de governo digital pode variar consideravelmente de país para país. Em um determinado sistema, um simples procedimento de autenticação de único fator (ou seja, login e senha) permite que os usuários naveguem por uma plataforma governamental. Em outros, os usuários terão que comprar ou receber um token baseado em uma infraestrutura de chave pública (*Public Key Infrastructure*, PKI), com o qual vários procedimentos são permitidos, inclusive votar on-line.[17] Por outro lado, esses sistemas de identificação digitais podem ser centralizados ou federados. Em alguns países, vários fornecedores de autenticação privados estão disponíveis para o usuário.[18]

Uma variedade de credenciais podem ser usadas para obter um alto nível de garantia para autenticação e verificação, incluindo biometria, senhas, certificados digitais, códigos QR e telefones celulares com informações de identidade embutidas nos dispositivos.

Contexto dos Serviços de Governo Digital na América Latina

A prestação de serviços na América Latina geralmente é concebida, como uma iniciativa isolada da entidade governamental responsável pela prestação do mesmo, que se concentra em suas próprias prioridades internas.[19] Essa desintegração se reflete na interface digital, e não é necessariamente contornada. Isso afeta negativamente o valor potencial de economia em termos de tempo e facilidade para os usuários e, consequentemente, dificulta a sua adoção.

73%
DOS PAÍSES NA REGIÃO JÁ DESENVOLVIAM ESTRATÉGIAS NACIONAIS DE DESENVOLVIMENTO DIGITAL.

60%
ESTABELECERAM TAMBÉM CANAIS DIGITAIS PARA CERTOS SERVIÇOS GOVERNAMENTAIS, INCLUINDO COLÔMBIA, MÉXICO, URUGUAI, BRASIL E ARGENTINA.

- Em parte, graças a essas iniciativas, a conectividade à internet na região se acelerou (OECD, 2019b).
- Vários países anunciaram estratégias governamentais digitais estimuladas por organizações internacionais e empresas de consultoria, que levantaram sérias preocupações, apesar do potencial.

Riscos para Identidade Digital no Setor

A lógica guiando os serviços de governo digital deve ser voltada para atender aos usuários e não serem um fim em si mesmo.[20]

- Se cada entidade governamental implementa sua própria identidade digital, surge um problema de interoperabilidade e grande parte da eficiência e do potencial de valor para o usuário se perde.
- Os serviços digitais podem representar sérios riscos à privacidade do indivíduo, mediante vazamentos e uso indevido de dados de identificação e outras informações sensíveis vinculadas ao perfil do usuário (por exemplo, em uma declaração de imposto de renda).
- A identificação facial, em particular, tornou-se uma tendência na autenticação do governo. Mas também pode implicar em violações de privacidade e discriminação.[21]
- O governo deveria primeiro a endereçar a regulação da proteção de dados, mas esse nem sempre é o caso. A abordagem "digital em primeiro lugar" para a prestação de serviços governamentais pode resultar em uma ruptura da acessibilidade aos serviços públicos, em que aqueles que não conseguem acessar ou usar canais digitais tão facilmente são excluídos ou encontram maior dificuldade para se relacionar com o Estado.
- A identificação digital, como chave de acesso a esses serviços digitais, significa que um sistema nacional de identificação digital mal projetado pode resultar em exclusão de uma grande parte da população do acesso aos serviços.

- Para mitigar esses riscos, é essencial uma abordagem multicanal de prestação de serviços governamentais. Eles não devem ser restritos ao acesso digital. Além disso, as identidades digitais devem ser acessíveis, idealmente gratuitas para o usuário. É preciso possibilitar acesso a qualquer serviço, independentemente do nível de garantia - de que a pessoa seja quem ela afirma ser - necessário. Isso não significa que os certificados digitais baseados em PKI devam ser usados para todas as transações e serviços, mas os usuários poderem escolher diferentes credenciais conforme o grau de sigilo e segurança exigido.
- O sistema não deve ser implementado apenas para o hype, sem considerar qual será o ganho efetivo para o usuário.

Usos Apropriados de Identidade Digital no Setor

Os serviços de governo digital vão além da oferta de serviços digitalmente. Eles permitem por meio de um canal digital o estabelecimento de um relacionamento mais próximo entre o governo e seus cidadãos. Por um lado, é legítimo exigir identificação para a outorga de determinados serviços personalizados (digitalmente ou não), quando um determinado nível de garantia é necessário para confirmar o status do cidadão, como emitir certificados, obter licenças, pagar impostos, etc.[22]

Por outro lado, a prestação de certos serviços, ligados ao exercício da cidadania, por exemplo acesso a informações úteis, transparência de atos governamentais, promoção da democracia e engajamento do cidadão, não devem ser condicionados à identificação, pois não há sentido em tal exigência. O que é importante, portanto, é avaliar criticamente a quantidade de dados pessoais necessária para determinar a identidade, o método de autenticação[23] usado para serviços governamentais digitais e se o processo é ou não proporcional e inclusivo.

Conclusões para um uso apropriado da ID digital no setor

- Os Serviços Digitais do Governo devem abranger, desde o primeiro passo, um sistema de identificação amplamente acessível que agregue valor ao usuário, simplificando procedimentos, reduzindo custos diretos e indiretos e possibilitando serviços de transação.
- Estruturas de autenticação federada ou integrada que usam dados compartilhados de diferentes sistemas devem seguir e incorporar práticas robustas de transparência e informar os usuários sobre o tratamento de seus dados pessoais, de acordo com a lei nacional de proteção de dados ou, na ausência deles, seguindo as melhores práticas internacionais.
- Os Serviços Digitais do Governo devem alcançar os grupos mais vulneráveis; portanto, deve haver uma opção de identificação digital gratuita para esses usuários. Independentemente do nível de garantia exigido por um determinado serviço governamental digital, as credenciais digitais devem ser iguais e inclusivas para os usuários. Idealmente por meio de credenciais digitais gratuitas.

Estudo de caso: **Governo Digital e Identificador Único do Chile**

Desde 1943, o sistema de identificação chileno busca identificar todos os residentes, além de apenas criminosos (Laval, 2018). Posteriormente, em 1973, o número único de identidade (*Rol Único Nacional*, RUN) foi criado e coincide com o RUT (*Rol Único Tributário*), que funciona tanto como identificação civil quanto um identificador do contribuinte. A partir de 1982, o RUT começou a ser emitido no momento do registro de nascimento, que já era informatizado.

A identificação faz parte do cotidiano de todos os chilenos, pois é obrigatória para quase todas as interações formais. Conforme relatado pela organização Privacy International com relação ao acesso à serviços e direitos, **"se você não tiver o RUT (*Rol Único Tributario*), não poderá fazê-lo"**. (Privacy International, 2018). Portanto, para quase todos os serviços governamentais, é necessário ter uma RUT.

Isso significa não apenas fornecer identificação para interagir com o estado, mas condicionar essa interação à presença de um identificador. Isso pode levar à exclusão legal e abuso de privacidade. Por exemplo, conhecendo o RUT de uma pessoa, por meio dessas informações publicamente disponíveis, também é possível determinar seu domicílio, estado civil, alguns dados eleitorais e verificar seu nome completo e de seus pais. Todas essas informações podem ser coletadas de maneira legal.

Em 2001, o registro on-line de nascimento e óbito tornou-se disponível. Posteriormente, em 2009, foi lançada uma solução para autenticação digital denominada "ClaveÚnica", emitida presencialmente pelo sistema de Registro Civil. Há um esforço contínuo para impulsionar a ClaveÚnica como a única maneira de autenticar para serviços digitais governamentais.

O RUT é necessário para obter a ClaveÚnica[24]. Inclusive, na recente Estratégia do Governo Digital do Chile, a identidade digital foi colocada entre os seis principais pilares (Gobierno Digital Chile, 2018). Como exemplos dessas políticas de serviços governamentais digitais, estão o *Cero Filas* (Zero Filas), que evita a necessidade de prova de identidade fragmentada em instituições públicas e a *Empresa en un día* (Empresa em um dia), que simplifica o processo de abertura de uma empresas no páis. No entanto, aproximadamente metade dos serviços públicos pode ser realizada on-line, dos quais menos de 15% utiliza a ClaveÚnica (OCDE, 2019e).

Tendo isso em vista, o Presidente Sebastián Piñera afirmou que *"... os serviços públicos em suas plataformas digitais de procedimentos ou serviços só podem usar a ClaveÚnica como um instrumento de identificação digital, para pessoas físicas, substituindo qualquer outro sistema de autenticação apropriado ao respectivo órgão da Administração."*[25]

Vale pontuar que o Chile possui há duas décadas um marco legal de proteção de dados(Lei 19.628/1999), como princípio geral, a lei estipula que os dados pessoais só podem ser processados com base no consentimento prévio e por escrito do titular dos dados, com apenas algumas poucas exceções (por exemplo, em certos dados acessíveis ao público ou no processamento puramente interno de dados para fins determinados). A lei também regula os direitos dos titulares de dados de acesso, retificação, exclusão ou bloqueio e objeção em certos casos.

No entanto, como apontado pelo diretor da Derechos Digitales, o problema no Chile está onde a identificação digital e a proteção de dados se coincidem: *"existe uma sensação geral de desproteção. Como a RUT de uma pessoa não é um dado privado, é possível obter o número de identificação de uma pessoa legalmente"*.

Ele adiciona que como ***"é possível criar um banco de dados com as informações de alguém com tanta facilidade, e considerando que também é simples transferir esse banco de dados entre particulares, há uma percepção de que não faz sentido armazenar essas informações, pois é muito fácil saber. Portanto, dificilmente há oposição a outra pessoa que as coleta"*** (Lara, J. 2019).

A integração de registro civil, identificação civil e identidade digital é um aspecto positivo do caso chileno. No entanto, deve haver estratégias claras para acessar serviços digitais básicos para aqueles sem ClaveÚnica, caso contrário, isso se traduzirá digitalmente no aspecto de alta centralização do RUT. Além disso, o modelo da ClaveÚnica pode e deve ser aprimorado para alcançar padrões de privacidade e segurança. Uma possibilidade é tornar privado o número de registro e implementar uma plataforma de supervisão de dados pessoais junto à chave pública de autenticação.

2.2. Serviços financeiros (Inclusão Financeira)

Considerando nossa abordagem de pesquisa com o objetivo de entender como a identidade digital pode contribuir para promover o desenvolvimento sustentável da América Latina, a análise setorial de casos de uso de serviços financeiros se concentra na agenda de **inclusão financeira**[27].

A inclusão financeira é mais do que possuir uma conta bancária. Em última análise, significa ter acesso a produtos e serviços financeiros úteis e acessíveis, que atendam às necessidades de indivíduos e empresas - transações, pagamentos, poupança, crédito e seguro - entregues de maneira responsável e sustentável.[28]

Os serviços financeiros digitais aumentaram e têm um papel de destaque como ferramenta de inclusão financeira, principalmente por meio de aplicativos de dinheiro móvel implementados em países em desenvolvimento como uma maneira de ultrapassar os procedimentos bancários convencionais e simplificar o acesso (Appaya & Varghese, 2019). Isso é importante para a agenda de desenvolvimento, pois facilita a vida cotidiana e ajuda as famílias e as empresas a se planejarem, levando em consideração desde objetivos de longo prazo até emergências. Inclusão financeira também está posicionada de forma destacada como facilitadora de outraos do Desenvolvimento Sustentável da Agena 2030.[29]

O Papel da ID para Inclusão Financeira

Para um terço dos adultos em aproximadamente 50 países com os mais baixos índices de desenvolvimento humano, a falta de documentação é o principal motivo para não ter uma conta bancária (Banco Mundial, 2018b). Um dos principais motivos alegados pelas instituições financeiras para condicionar o acesso aos seus serviços à documentação é sua obrigação em relação ao cumprimento de certos procedimentos padronizados em escala internacional, além de outros regulamentos dentro de suas jurisdições, que exigem a identificação do cliente. Por exemplo, Conheça Seu Cliente (*Know-Your-Customer*, KYC) e *Customer Due Diligence* (CDD)[30] são procedimentos obrigatórios e fundamentais para garantir a conformidade da instituição com as regras de combate à lavagem de dinheiro (*Anti Money Laundering*, AML) e ao financiamento do terrorismo (*Financing Terrorism*, FT).

A identificação digital no setor financeiro pode catalisar esforços multidimensionais de órgãos reguladores financeiros e autoridades governamentais para simplificar os pré-requisitos de CDD e KYC. Além disso, uma identidade digital confiável pode aumentar a capacidade das instituições financeiras de cumprir tais diretrizes de AML e combater o FT (GSMA, 2016).

O setor financeiro tem sido o principal impulsionador da inovação em esquemas de identificação, autenticação e autorização em todo o mundo. Isso provavelmente se deve ao fato de que a falha em identificar alguém em uma determinada transação pode levar a perdas financeiras diretas. O gerenciamento moderno de identificação no setor vai das arquiteturas de identidade de cartão de crédito federadas em meados do século passado ao open banking nos dias de hoje, por exemplo.

Além do mais, muitas partes interessadas internacionais (Mastercard, 2019a; McKinsey Global Institute, 2019) têm tentado quantificar previsões muito otimistas sobre os impactos econômicos que um sistema de identificação digital poderia trazer para o desenvolvimento do país implementador (Center for Global Development, 2017a) e pela inclusão financeira e seus benefícios para os mais vulneráveis (Banco Mundial, 2019a). No entanto, organizações da sociedade civil como Access Now[31] e Privacy International alertam que ainda não há evidências suficientes para confirmar os benefícios prometidos.

Métodos de Identificação e Possibilidades para Inclusão Financeira

Usando o registro da conta no contexto brasileiro como exemplo, as informações necessárias são (i) o número do documento de identificação e sua natureza; sua entidade emissora e data de emissão; os nomes do cliente e de sua mãe; data de nascimento; cidadania; nacionalidade; o número do registro do pagamento de impostos e informações se a pessoa é "politicamente exposta". Muitas entidades estão migrando para o uso da verificação de identidade legal por meio de um Conheça Seu Cliente eletrônico. Várias empresas de tecnologia financeira estão usando uma versão apenas móvel do sistema de prova de identidade.

A identificação está cada vez mais sendo feita através da verificação de identidade legal (por exemplo, identificação civil, passaportes, carteira de motorista) que são carregadas em uma plataforma digital que pode checar em bancos de dados oficiais do governo sua validade via interfaces programáveis de aplicações (*Application Programmable Interface*, API). As empresas de tecnologia financeira também contam com algoritmos de documentoscopia para evitar fraudes. Para CDD, o procedimento é semelhante: técnicas automatizadas podem determinar rapidamente a capacidade de alguém de cumprir regras específicas.

Além disso, desde M-Pesa[32] no Quênia (agora utilizado em vários países africanos), o dinheiro móvel foi identificado como muito atraente para novos clientes, incluindo a população desbancarizada (Ramada-Sarasola, 2012).

Nesse sentido, vale ressaltar que em alguns contextos, como no Peru, os números de celular são persistentes durante toda vida útil dos usuários. Nesse caso, o KYC também conta com a verificação de identidade de um identificador único emitido pelo estado, mas é muito mais simples para definir uma conta para serviços financeiros básicos, como armazenar dinheiro, efetuar pagamentos e transferências.

Finalmente, há uma gama de tecnologias emergentes sendo exploradas para registro e autenticação. Essas estão no centro da agenda de tendências da autenticação desprovida da necessidade de senha, combinando autenticação multifatorial e biometria (World Economic Forum, 2020)[33]. Com formas alternativas de estabelecer a unicidade de uma pessoa, a inovação no setor financeiro pode facilitar transferências de dinheiro, remessas e pagamentos digitais, garantindo o monitoramento financeiro e, assim, contribuindo para a inclusão financeira.[34] Além disso, no setor financeiro, as tecnologias de registros distribuídas (por exemplo, blockchain) estão mais maduras do que em qualquer outro setor.

Contexto de Inclusão Financeira na América Latina

Vários países latino-americanos estão implementando estratégias nacionais de inclusão financeira (Villarreal, 2017). **Colômbia, Peru e Uruguai estão entre os países com o melhor acesso financeiro em todo o mundo**.

13 países da região prepararam políticas e ações integradas relacionadas à distribuição, regulamentação e educação em serviços financeiros.

Além disso, alguns países (por exemplo, Brasil, Chile, México) lançaram suas estratégias de inclusão financeira há mais de uma década (Banco Central do Brasil, 2009).

A região é vista como muito proeminente para o desenvolvimento da indústria de tecnologia financeira (fintech) e um mercado importante devido à demanda populacional desbancarizada. Logo, os bancos digitais estão se tornando cada vez mais populares. Na América Latina, há um debate em evolução sobre estruturas regulatórias, a resistência de bancos tradicionais e questões de cibersegurança (Clavijo, S., *et. al*. 2019). De qualquer forma, a falta de prova de identidade ainda é uma barreira fundamental para a eficácia de tais políticas e pouca atenção pragmática foi dada a esse tópico (FATF, 2019).[35]

Os Riscos da Identidade Digital no Setor

A identidade digital por si só não é suficiente para remediar a exclusão financeira.

- Devido ao perfil de risco do setor financeiro, os processos de KYC podem acabar exigindo dados biográficos, biométricos e históricos adicionais dos clientes.[36]
- Além da identificação mínima necessária, as devidas diligências sobre o cliente exigem a obtenção de informações para, a respeito de situações de alto risco, determinar a natureza das atividades financeiras (FAFT, 2014).
- Os dados financeiros e de identificação combinados apresentam grandes riscos para os usuários em caso de violações (por exemplo, serem excluídos socioeconomicamente de programas específicos ou ter uma solicitação de crédito negada) e para a integridade do sistema financeiro (por exemplo, aumento da apropriação indevida de recursos públicos).
- Compartilhar dados de identificação entre instituições financeiras sem o consentimento claro, informado e expresso dos usuários também pode ser um fator de exclusão e discriminação, perpetuando a pobreza em vez de reduzi-la.[37]
- Cobrar taxas de serviços de verificação de identidade de usuário pode resultar em exclusão socioeconômica.

- O processo de verificação deve ser transparente e o mais barato possível.
- Para serviços financeiros básicos, deve haver processos KYC simplificados, digital e fisicamente, e com privacidade por padrão e desde a concepção.

Os Usos Apropriados da ID Digital no Setor

Como mencionado, o KYC é um procedimento obrigatório e a verificação da identidade do usuário é um elemento essencial para abrir contas bancárias ou para identificação do cliente em uma determinada transação financeira. Dito isto, é esperado que as entidades financeiras solicitem comprovantes de pagamento para avaliar a capacidade do cliente em pagar empréstimos, por exemplo. No entanto, não é razoável exigir e usar informações financeiras para determinar a unicidade de uma pessoa.

Além disso, é fundamental o consentimento do usuário para a coleta e o compartilhamento de dados pessoais. Para um uso apropriado da identificação digital no setor financeiro, o acesso não autorizado a dados de identidade de terceiros deve ser endereçado e comunicado publicamente.

Conclusões para um uso apropriado da ID digital no setor

- Os requisitos básicos de KYC devem idealmente ser gratuitos para a inclusão financeira da população alvo e fáceis de executar. É importante separar claramente quais são os dados básicos usados para identificar alguém das informações complementares necessárias para o acesso a serviços específicos e a devida diligência sobre o cliente.
- Como o setor líder em identificação do ponto de vista tecnológico, as empresas de tecnologia financeira e os grandes bancos devem apoiar e ser os principais impulsionadores das tecnologias de aprimoramento da privacidade. Além disso, a inexistência de mecanismos de reparação, reclamação e de acesso ao histórico dos dados são um importante indicador de práticas inadequadas, dada a maturidade tecnológica do setor.
- Reguladores financeiros devem trabalhar em estreita colaboração com as autoridades de identificação e proteção de dados, garantindo a interoperabilidade com o sistema nacional de identificação.

Estudo de caso: Peru e Inclusão Financeira

O Peru é um caso de identidade muito particular. Em 1995, o governo peruano iniciou uma extensa campanha de identificação estabelecendo constitucionalmente o Registro Nacional de Identificação e Estado Civil (*Registro Nacional de Identificación y Estado Civil*, RENIEC). Como autoridade de identificação independente, a RENIEC é responsável pela emissão do Documento de Identidade Nacional (DNI).

O RENIEC foi criado logo após um período de guerra civil, autoritarismo e perseguição que deixou milhões de peruanos sem prova de identidade legal. A autonomia do RENIEC é garantida pelas receitas obtidas com o fornecimento de serviços de verificação e autenticação de identidade a entidades privadas. Isso representou aproximadamente um terço de sua receita em 2015 e é provável que aumente, uma vez que quase toda a população já tem um DNI, mas não necessariamente registro civil.

Desde 2015, o Peru tem uma Estratégia Nacional para Inclusão Financeira, que identifica a falta de identidade como uma barreira fundamental de acesso (Comisión Multisectorial de Inclusión Financiera, 2015). Pagos Digitales Peruanos, um consórcio de bancos e empresas financeiras, lançou um sistema de pagamento móvel chamado BIM, que é frequentemente referido como um caso de inclusão financeira viabilizado pela identidade digital (Caruso, 2016)[38]. O sistema é uma réplica dos sistemas de dinheiro móvel na África.

A carteira digital BIM é uma iniciativa sem fins lucrativos lançada em 2011 visando principalmente os desbancarizados, mas apenas aqueles com telefone celular. Infelizmente, exclui-se a maioria da população que, além de não ter conta no banco, não tem acesso a um número de celular (Center for Financial Inclusion, 2019). Mesmo com a alta demanda, os entrevistados da RENIEC e da sociedade civil concordaram com a falha da BIM em termos de obter uma massa crítica de usuários até os dias de hoje.

O DNI não é apenas necessário para abrir uma conta. Na verdade, *"para obter um número de celular, você precisa usar seu número DNI"* (Miguel Arce, gerente de vendas da Pagos Digitales Peruanos).

O KYC da plataforma é garantido pelo código identificador exclusivo fornecido pela RENIEC e pela verificação cruzada em um banco de dados de fotos como parte de seu modelo econômico mencionado.[39] A BIM conecta ao RENIEC e obtém os dados complementares associados ao DNI inserido pelo cliente durante o registro do aplicativo. Se os dados não corresponderem, a conta é bloqueada no dia seguinte. Esta verificação cruzada também se aplica para desautorizar o acesso à menores de idade ou falecidos. Segundo

um executivo responsável pela BIM, os únicos dados fornecidos neste caso pela RENIEC são o nome completo e a prova da idade legal. Ao instalar a BIM, o usuário pode escolher qual provedor de serviços financeiros deseja usar.

No entanto, conforme argumentado pelos defensores dos direitos digitais, o perfil centralizado e poderoso da RENIEC apresenta sérios riscos à privacidade. Diferentemente da RENIEC, a Autoridade Peruana de Proteção de Dados,[40] não é independente. Além disso, não há uma compatibilidade clara entre a identidade digital e os regulamentos de proteção de dados.

Quanto à RENIEC, **"a partir de uma perspectiva da sociedade civil,[41] não gosto dessa autonomia. Uma autonomia sem controle, seria quase um poder absoluto "** (Morachimo, 2019).

Em relação à legislação de identidade digital, não houve revisão ou consulta para a concepção de normas, regulamentos, programas ou aplicativos, seja pelo Congresso, pela Autoridade de Proteção de Dados, pelo Ministério da Justiça ou pela sociedade civil.

Em termos de inclusão financeira, embora ainda exista uma enorme população sem conta no banco, o BIM não promoveu um impacto significativo. No entanto, a integração do BIM e do RENIEC é razoável na perspectiva da usabilidade, conveniência dos provedores de serviços financeiros e receita para a instituição pública. Ao mesmo tempo, a partir de uma perspectiva de governança de dados, a integração é preocupante devido ao desequilíbrio de poder da autoridade de identificação sobre a de proteção de dados. Ao permitir a supervisão multissetorial, a RENIEC atuaria proativamente para fortalecer o sistema de identificação digital.

2.3. Acesso à Saúde

O acesso à saúde é estabelecido como um direito humano, inscrito na Declaração Universal dos Direitos Humanos de 1948 como parte do direito a um padrão de vida adequado (art. 25). O direito à saúde é novamente reconhecido como um direito humano no Pacto Internacional dos Direitos Civis e Políticos de 1966. Além disso, o alvo dos ODS 3.9 estabelece o objetivo de alcançar a cobertura universal de saúde *"incluindo a proteção do risco financeiro, o acesso a serviços de saúde essenciais de qualidade e o acesso a medicamentos e vacinas essenciais seguros, eficazes, de qualidade e a preços acessíveis para todos"*.

A identificação de indivíduos pode ser uma ferramenta para atingir esses fins ou, inversamente, pode gerar discriminaçào negativa, negando acesso aos cuidados de saúde para aqueles que não são identificados. Essas potencialidades, boas e ruins, são ampliadas em um sistema de identificação digital.

O Papel da ID no acesso à saúde

A identificação no setor de saúde pode ser valiosa para a segurança do paciente (OMS, 2007), eficiência na prestação de serviços e gestão da saúde pública (Banco Mundial, 2018c). Mecanismos de identificação de pacientes podem ser importantes para integrar registros, gerar estatísticas e organizar dados para melhor planejar as políticas de saúde.

A partir da perspectiva dos prestadores de serviços, uma vez que a identidade do paciente é conhecida, é possível acessar o devido tratamento e o histórico médico a fim de garantir a prestação de um atendimento consistente e apropriado. Da perspectiva do paciente, a documentação é importante para comprovar a inscrição em programas de seguros ou outras redes que cobram despesas médicas. Em relação à "segurança do paciente", a identificação é um dos elementos mais relevantes apresentados pelas organizações internacionais de saúde.[42]

Métodos de identificação e possibilidades na área da saúde

O surgimento da identificação digital no setor da saúde está ligado à proliferação de políticas de tecnologia da informação em saúde a fim de implementar serviços on-line, incluindo prontuários médicos eletrônicos, registros clínicos pessoais e prescrições eletrônicas - em paralelo com a expansão de iniciativas em telemedicina (OMS e UIT, 2012).[43]

Os métodos atuais para identificação do paciente geralmente envolvem o uso de um número de registro médico emitido e mantido pelo provedor

do tratamento, que nem sempre possui um sistema interoperável. Assim, os pacientes podem ser vinculados a vários números de prontuários, cada um emitido pela clínica ou hospital que os atendeu. O relatório da ONUSIDA chama a atenção para o fato de que, se usado em um contexto mais amplo, é praticamente impossível, com base apenas no número determinar com acurácia a unicidade dos pacientes entre organizações ou regiões (ONUSIDA, 2014). Logo, isso restringiria os benefícios descritos anteriormente. Além disso, vale ressaltar que o método probabilístico de correspondência de prontuários médicos pode ser outra maneira de identificar pacientes (ONUSIDA).[44]

Para eliminar os múltiplos mecanismos paralelos e desconectados de registro de pacientes, a implementação de um Identificador Digital Nacional de Saúde (IDNS) é frequentemente considerada. Trata-se de um número exclusivo vinculado às informações de identificação pela autoridade confiável. O IDNS geralmente se integra à emissão de uma credencial, um cartão de identificação de saúde. O cartão pode ser usado pelo paciente para comunicar seu IDNS a terceiros a fim de autorizar o acesso às suas informações pessoais. Esse processo geralmente é acompanhado pela solicitação de documentação adicional e/ou coleta de dados biométricos.

Contexto dos serviços de saúde na América Latina

O modelo de identificação e prestação de serviços de saúde de maneira centralizada na América Latina foi construído gradualmente na década de 1990. Antes, os sistemas de saúde eram atrelados à seguridade social e quem não estava vinculado a esse sistema era direcionado para um serviço de 'uso geral'. Numa segunda etapa, esses serviços foram unificados na maioria dos países da América Latina.

No modelo anterior de prestação de serviços, nenhuma informação sobre o paciente era mantida, apenas os procedimentos realizados. Assim, o foco foi documentar e garantir a cobrança correta dos serviços, principalmente para evitar fraudes por parte do provedor descentralizado. Já no modelo centralizado os pacientes e seu histórico médico são monitorados para garantir a continuidade do tratamento. A mudança de paradigma exigiu um sistema de identificação mais sofisticado, o que permitiria focar na segurança do paciente.

Os progressos realizados pelos países latino-americanos no campo dos serviços eletrônicos de saúde (e-health) são múltiplos. Dados dos Estados Membros da Organização Mundial da Saúde (OMS)- disponibilizados por meio de seu escritório regional, a Organização Pan-Americana da Saúde (OPAS, 2016) - mostram uma visão geral mista das práticas relacionadas à saúde eletrônica.

77,8%
POSSUEM POLÍTICA OU ESTRATÉGIA NACIONAL DE TRANSFORMAÇÃO DIGITAL NA SAÚDE.

84.2%
RELATARAM TER PELO MENOS UM SISTEMA DE INFORMAÇÃO DE SAÚDE.

Embora de maneira heterogênea, políticas e tecnologias de saúde eletrônica penetraram nos estados latino-americanos. Um IDNS provavelmente será a chave pela qual os cidadãos terão acesso a essas novas maneiras de fornecer serviços de saúde.

Riscos para Identidade Digital no Setor

- Somente uma identidade digital nacional para o acesso à saúde não protegerá a privacidade e a confidencialidade das informações de atendimento do paciente, nem garantirá sua identificação precisa.[45]
- A digitalização dos registros e serviços de saúde e o surgimento de novas tecnologias levantam preocupações sobre a privacidade, proteção de dados de saúde, sobretudo dados biométricos, e sobre a relação de confiança entre pacientes e prestadores de serviços em outro patamar. Assim, a integridade dos dados de saúde começa a se transformar em um problema de segurança cibernética.
- O acesso não autorizado ou o uso indevido de informações pessoais pode reduzir a confiança, minar os direitos à privacidade e, em alguns casos, colocar grupos vulneráveis em sérios riscos de danos (Banco Mundial, 2018c).[46]
- Os sistemas de saúde eletrônica podem se tornar o maior conjunto de informações sobre os cidadãos de um país, tornando-se um registro civil de fato. Os registros médicos podem revelar origem étnica ou afiliação religiosa de maneira sistemática, o que não é apropriado para um sistema nacional de identificação fundacional.
- Possível compartilhamento e a venda de dados pessoais para diversos fins duvidosos, incluindo discriminação antiética por parte dos provedores de seguro de saúde.

- Grupos de risco e aqueles com estigmas sociais são extremamente dependentes do contexto e da cultura de cada região e, por esse motivo, políticas específicas devem ser projetadas para incluí-las. Para isso, é essencial o envolvimento da populações alvo para que possíveis preocupações possam ser identificadas e endereçadas.
- Métodos de identificação alternativos podem ser desenvolvidos para garantir a integridade do processo de solicitação de sistemas nacionais de saúde que exigem identificação, como programas de vacinação. Para isso, o objetivo da identificação pode ser alcançado por meio da reunião com um ancião da aldeia ou tribo, profissional de saúde da comunidade, líder religioso ou outra fonte confiável.
- A responsabilidade pela privacidade também pode ser endereçada por meio da aplicação de leis e regulamentos de privacidade e proteção de dados que se baseiam nos direitos individuais, garantindo um acesso adequado aos dados a fim de atender às necessidades de informações de saúde pública (Banco Mundial, 2018c).[47]

- Existem grupos de pessoas que podem ser excluídos do próprio programa de assistência médica ou de identificação, se isso não for planejado com cuidado. Algumas pessoas, como imigrantes, profissionais do sexo, indivíduos LGBTQ+, usuários de drogas ou pessoas com doenças estigmatizadas, podem relutar em se identificar, e essa decisão deve ser totalmente respeitada.
- Solicitar documentação adicional pode levar à exclusão. Dependendo do país e das diferentes condições locais das comunidades rurais e autóctones, pode haver documentação formal mínima para ajudar a verificar a identidade de uma pessoa. Além disso, situações específicas podem impedir que parte da população apresente documentos, como desastres naturais, guerras ou outras calamidades.

Os Usos Apropriados de Identidade Digital no Setor

Como mencionado anteriormente, o acesso aos serviços de saúde é um direito humano reconhecido internacionalmente. Nesse sentido, é necessário analisar em detalhes se e quando a identificação do paciente é um passo em direção à fruição desses direitos ou, pelo contrário, se está excluindo grupos ainda mais vulneráveis do acesso à saúde. Por fim, todos têm direito a cuidados médicos urgentes para salvar suas vidas ou evitar danos irreparáveis à sua saúde, e isso deve ser fornecido independentemente de qualquer documento de identidade, digital ou não, que seja apresentado.[48]

Conclusões para os usos apropriados de ID digital no setor

- Caso uma identificação nacional (digital) exclusiva para serviços de saúde seja estabelecida, esta poderá estar vinculada à identidade fundacional. A integração, no entanto, não deve permitir o acesso a dados médicos confidenciais por terceiros. Quando necessários para informações de saúde pública, os dados devem ser anonimizados, impedindo que o paciente seja reidentificado.
- O acesso a serviços médicos de urgência, e não apenas emergências, nunca deve ser condicionado à identificação. O mesmo vale para identidade digital.
- Métodos de identificação alternativos podem ser desenvolvidos para garantir a integridade do cadastro para políticas nacionais que dependem da identificação da população alvo (como programas de vacinação). A identidade digital poderia apoiar isso.

Estudo de caso: **Certidão de nascimento eletrônica e cartão de vacinação eletrônico do México**

Atualmente, vários documentos identificam oficialmente os cidadãos no México. Entre os principais, está o Código Exclusivo de Registro de População (CURP). Esse registro é uma combinação de letras e números atribuídos pelo Conselho Nacional de População a cada pessoa nascida no México ou a um estrangeiro em posse de uma autorização de residência; no entanto, o CURP ainda não se transformou em um ID nacional universal. As certidões de nascimento e o CURP servem como identidade fundacional e possibilitam que os indivíduos obtenham identificações funcionais, usadas para votar, para acessar programas de seguridade social, bem como serviços públicos de saúde. Embora a Coordenação da Estratégia Nacional Digital (CEDN), lançada no final de 2013, tenha implementado recentemente importantes ações de saúde eletrônica, o país atualmente não possui uma política ou estratégia nacional abrangente em vigor.

A identificação é necessária para receber assistência médica no México. Isso requer atenção, pois pode potencialmente excluir pessoas que não têm meios de identificação ou que não desejam se identificar para acessar serviços de saúde, sejam eles públicos ou privados. No entanto, de acordo com os especialistas entrevistados para o escopo deste trabalho, pessoas que não têm meios de identificação podem receber tratamento em caráter emergencial, por padrão da legislação.

Cada sistema de saúde ainda coleta, armazena e processa os dados de seus beneficiários. No entanto, o governo implementou, como parte da Estratégia Digital Nacional, a Certidão de Nascimento Eletrônica (CEN) e o Cartão de Vacinação Eletrônica (CEV), duas novas formas de documentação eletrônica usadas no sistema de saúde.

O CEN é uma versão eletrônica da certidão de nascimento em um formato nacional único estabelecido pelo Ministério da Saúde. Este documento é emitido aos recém-nascidos pela instituição de saúde afiliada do local de nascimento.[49] O CEN pode ainda ter uma versão impressa e tende a ser o primeiro passo para uma identidade digital exclusiva na área da saúde.[50]

A versão eletrônica da certidão de nascimento não é um requisito para obter uma cópia impressa da certidão de nascimento ou do CURP, e a versão em papel ainda está em uso. Embora a Lei Geral de Saúde estabeleça que seja obrigatória desde 2015, nem todas as instituições já implementaram a certidão de nascimento eletrônica (Mexico Digital, 2014). Segundo o governo mexicano, o sistema já está em vigor em 21 dos 31 estados e, em 2017, mais de 200.000 certificados eletrônicos foram emitidos (Mexico Digital, 2018).

Além disso, em alguns casos, o prontuário eletrônico já foi implementado (Comissão Nacional de Arbitraje Médico, 2018).

O CEV, criado em 2014, possui a mesma funcionalidade do Cartão Nacional de Saúde atualmente em uso, mas ainda há trabalho a ser feito para alcançar a plena operacionalidade. Apenas algumas cidades o implementaram, e a certidão eletrônica é obrigatória apenas nos estados que já implantaram o sistema. O projeto também inclui um aplicativo móvel, um painel de controle, um administrador da web e um cartão de vacinação contendo um chip. Os dados da certidão de nascimento e o CURP são inseridos neste chip e os dados de vacinação de cada pessoa são incluídos e armazenados eletronicamente com cópias manuscritas de segurança no mesmo cartão.

A combinação de CEV, CEN e prontuários eletrônicos pode representar um ganho para o governo, pois não precisaria realizar diagnósticos clínicos de forma repetitiva, uma vez que eles já são armazenados eletronicamente. No entanto, o banco de dados mexicano agrega dados sensíveis e biométricos do paciente e de suas famílias, aumentando os danos em caso de uso indevido ou vazamento. Isso é preocupante porque há pessoas interessadas em ter acesso a esse banco de dados, como as companhias de seguros.[51]

A lei mexicana de proteção de dados determina que deve haver um interesse legítimo na coleta de dados. No entanto, a lei não fornece nenhuma definição de "interesse legítimo". Assim, na prática, a lei atual permite uma coleta de dados que alguns diriam ser excessiva.

"O cumprimento da legislação sobre a proteção de dados pessoais mantidos por empresas de serviços estabelecidas no México é mínimo, como resultado do desconhecimento da lei." (Enríquez, O. 2018).

Além disso, a lei não define o padrão correto de armazenamento de dados ou as consequências por não conformidade.[52] É apropriado dizer que hoje o México possui legislação consistente em relação à proteção de dados pessoais, mas ainda é pouco conhecida e pouco aplicada.

Evelyn Tellez, pesquisadora do INFOTEC, o centro público de pesquisa do governo do México especializado no desenvolvimento de tecnologias de informação e comunicação, também reforçou certas questões delicadas relacionadas ao armazenamento e processamento de dados pessoais pelo governo. Por exemplo, os dados de mais de 80 milhões de mexicanos foram clonados recentemente.

Além disso, o registro clínico é o segundo registro mais importante no México no tocante à identificação (o primeiro sendo o instituto nacional eleitoral, INE). Uma explicação para esse fenômeno é que, para obter uma consulta médica, os usuários devem apresentar comprovante de endereço,

título de eleitor e uma certidão de nascimento como requisitos básicos. Além disso, também é solicitado que se forneça todas as impressões digitais do usuário e de sua família (pais e/ou filhos).

Existem lacunas na legislação que afetam diretamente a proteção de dados de cidadãos mexicanos (OCDE, 2018), ou se tornam evidentes nas análises de casos de vazamentos de dados maciços, conforme indicado por Evelyn. Portanto, existe uma desconfiança real sobre a segurança dos dados mantidos pelo estado mexicano,[53] e ter sua identidade roubada tem sido uma preocupação frequente para os mexicanos nos últimos anos[54]. De fato, de acordo com um especialista em segurança da informação no México, embora seja difícil falsificar credenciais como o INE, o sistema de identificação mexicano ainda é deficiente em segurança de dados e proteção contra a falsificação de identidade.

Além disso, como o cartão eletrônico de vacinação e os registros médicos eletrônicos estão sendo solicitados para acesso aos serviços de saúde, isso se torna um importante ponto de atenção. Se os canais de acesso não estiverem disponíveis para todos, isso sem dúvida seria uma prática equivocada do sistema de identificação.

2.4. Proteção Social

Apesar das diferentes abordagens e definições, a Proteção Social é o sistema de programas, atores, políticas e ações para proteger populações vulneráveis, erradicar a pobreza e promover o bem-estar e o trabalho decente (UNRISD, 2010). Entre os Programas de Proteção Social (*Social Protection Programs*, SPPs), existem esquemas contributivos e não contributivos (por exemplo, transferências de renda condicionais e incondicionais), que são endereçados neste estudo.

Considerando a abordagem holística dos Objetivos de Desenvolvimento Sustentável da ONU, a necessidade de uma melhor coordenação entre os programas de proteção social está em destaque.

O Papel da ID para Proteção Social

Sem prova legal de identidade, uma pessoa não pode ser incluída em quase nenhum programa de proteção social. Esse é um fator que estimula a demanda por documentação de identidade entre a população de baixa renda. Estudos mostram que a inclusão social impulsionou a demanda por registro e identificação civil na América Latina (Hunter, W. & Bril, R, 2016; Hunter, 2019).[55] Além disso, os governos criaram políticas para simplificar os serviços de identificação (Muzzi, 2010) e torná-los mais acessíveis à população vulnerável não documentada.[56]

A adoção e integração de tecnologias de identificação digital é uma tendência emergente e de crescimento acelerado nos programas de proteção social.

Nesse sentido, uma maneira eficiente de identificar indivíduos é essencial para garantir a interoperabilidade (vinculando informações entre programas sociais) promover a participação social e melhorar a prestação de serviços.

Métodos de identificação e possibilidades para proteção social

Os esquemas de proteção social exigem mais informações sobre a população do que os esquemas de identificação comuns. É necessário caracterizar indivíduos em vários aspectos de suas condições (por exemplo, idade, renda, número de dependentes do ou da chefe de família). Assim, os SPPs adotam uma ampla gama de métodos de identificação que variam de acordo com as capacidades do governo, a infraestrutura de tecnologia de informação e comunicação do país, os recursos financeiros disponíveis e a população alvo. Na maioria dos países, a inscrição de beneficiários é feita usando os IDs tradicionais em papel.

Quando o país possui um sistema de identificação fundacional, esta é usada como fonte primária para identificar os beneficiários dos esquemas de proteção social. No entanto, quando a cobertura do ID da identidade fundacional não é suficiente ou não existe, é necessário estabelecer uma maneira alternativa de identificar a população alvo. Assim, muitos países realizam um processo de registro específico para a população alvo do SPP e emitem um cartão para identificar os beneficiários.

Um típico Sistema de Gestão de Informação (Management Information System, MIS), como a espinha dorsal do gerenciamento de programas de proteção social, possui pelo menos três pilares funcionais:

Inscrição e identificação	Direcionamento e definição elegibilidade	Habilitação de transações e entrega de serviços

A interoperabilidade dos registros é combinada com o uso de um identificador exclusivo de forma a viabilizar uma visão holística dos beneficiários, vinculando-os a vários programas. Além disso, os países em desenvolvimento têm adotado a identificação biométrica devido ao seu potencial benefício para garantir uma identificação precisa.

Contexto da Proteção Social na América Latina

Os SPPs tradicionais na América Latina costumam estar vinculados às políticas trabalhistas. Ademais, como a principal inovação na redução da pobreza, por mais de duas décadas, o uso de transferências de renda não contributivas foi o foco de políticas sociais na região. Alguns exemplos são *Chile Solidario*, *Prospera* (México), *Mas Familias en Acción* (Colômbia), e a *Juntos* (Peru). Estes programas têm diversos pontos em comum, mas diferem em seus critérios de elegibilidade para determinar situações de pobreza.

Em 2014:

20
PAÍSES DA REGIÃO TINHAM UMA POLÍTICA DE TRANSFERÊNCIA CONDICIONADA DE RENDA,

25%
DA POPULAÇÃO DA AMÉRICA LATINA E DO CARIBE ESTAVAM INSCRITOS EM UMA POLÍTICA DE TRANSFERÊNCIA DE RENDA (CEPAL, 2015).[57]

Altos níveis de desigualdade caracterizam as sociedades latino-americanas (Ibarra & Byanyima, 2016). Uma parcela significativa da população não é apenas pobre, mas também social, cultural e legalmente excluída.

Freqüentemente, os mais vulneráveis, portanto, necessitando de assistência, também são invisíveis para o Estado. Eles são desconhecidos porque não possuem documentação pessoal formal e, consequentemente, não são auferidos por programas de proteção social.

Os Riscos para Identidade Digital no Setor

No âmbito de proteção social, assegurar a inclusão é fundamental, mas é também complexo. O objetivo envolve a identificação de indivíduos vulneráveis e socialmente excluídos, não apenas economicamente, mas frequentemente em outros aspectos de suas vidas.

- Sem condições materiais mínimas e acesso à informação, uma pessoa não pode transpassar todos procedimentos burocráticos para possuir um documento de identidade, tampouco uma identidade digital.
- O aspecto da vulnerabilidade implica que os beneficiários em potencial possam residir em habitações precárias, pouco resistentes às intempéries ou não possuir habitações, sendo, portanto, frequentemente incapazes de manter seus documentos. O uso da biometria tem sido amplamente incentivado a endereçar esse desafio.
- Independentemente da crescente adoção da identificação biométrica (Carmona, 2019), estudos conduzidos no contexto indiano[58] mostram que o risco de excluir grupos vulneráveis é preocupante (Drèze et al., 2017; Muralidharan, 2020).[59]
- A identificação nos SPPs coleta uma ampla variedade de dados pessoais. Isso significa que muitos dados sensíveis estão expostos aos riscos comuns a qualquer esquema de identificação digital, como vazamentos de dados, mas que especificamente no contexto da proteção social pode significar estigmatização e constrangimento.
- O fosso digital (incluindo níveis de educação e acesso digital tecnológico) é frequentemente intrínseco à situação de vulnerabilidade daqueles que dependem de assistência social, com alto risco de exclusão.

- Essa situação complicada foi enfrentada pela criação de programas de proteção social que abordam simultaneamente os dois lados da equação: proporcionar renda mínima e acesso a serviços básicos e simplificar os procedimentos para obter documentação pessoal básica.
- Nesse sentido, a proteção de dados deve ser percebida como um elemento de proteção social (Sepúlveda, 2019).
- Nesse sentido, os identificadores da proteção social não devem estar vinculados a bancos de dados biométricos.

» Qualquer falha no sistema apresenta grandes riscos de exclusão e pode ter severas conseqüências. Por exemplo, se uma pessoa não tem a identidade digital exigida por agências governamentais ou se sua identidade digital está "incompleta" pois suas impressões digitais não foram carregadas no banco de dados nacional devido ao baixo acesso à internet (Access Now, 2018).

Os Usos Apropriados de ID Digital no Setor

No contexto da proteção social, a identificação dos beneficiários é um componente essencial e integrado do esquema. Tornar os indivíduos elegíveis para proteção social é uma maneira de incluí-los. No entanto, existem preocupações sobre os meios utilizados para identificação.

Na América Latina, a adoção da identificação biométrica obrigatória ainda não está generalizada. No entanto, críticas a fraudes vêm pressionando a adoção da biometria em programas de proteção social. Neste âmbito, uma avaliação de risco público deve ser cuidadosamente considerada e os dados biométricos não devem ser obrigatórios para autenticação de indivíduos para acesso a bens e serviços.

Conclusões para os usos apropriados de ID digital no setor

» Os governos devem criar um cadastro único para a proteção social, adotando uma perspectiva inclusiva da população vulnerável. É crucial simplificar e tornar os serviços de identificação mais acessíveis para a população não documentada, equilibrando os requisitos e as condições dos beneficiários.

» A integração de sistemas de gestão de informação e esquemas de identificação digital deve considerar o risco de excluir a população mais vulnerável e, ao mesmo tempo, atingir a efetividade das políticas públicas.

» A adoção da tecnologia biométrica na proteção social precisa ser precedida de uma avaliação holística do sistema nacional de identificação, no qual os marcos institucionais e legais devem ser avaliados através das lentes da inclusão e da promoção de direitos, garantindo que os pobres e os mais vulneráveis não sejam excluídos.

Estudo de caso: **Cadastro Único de Programas Sociais do Brasil**

O Cadastro Único de Programas Sociais (CadÚnico) é um registro administrativo desenvolvido em 2001 para permitir programas sociais integrados no Brasil, apoiando diversos programas de proteção social, como o Bolsa Família (PBF), um exemplo global de programa de transferência de renda condicionada (Lindert et al., 2007; Hellmann, 2015).

O CadÚnico é a ferramenta de identificação de beneficiários e diferencia as necessidades das populações-alvo de acordo com as características de cada família. O processo de registro é gratuito e descentralizado nos três níveis federativos do governo. Solicita-se durante a inscrição a coleta de informações sobre as famílias mais vulneráveis, contendo as condições de trabalho, a composição familiar, moradia, entre outras. Mais de 13 milhões de famílias em todas as regiões do país, quase um quarto da população brasileira, foram incluídas no programa.

O CadÚnico também tem um papel significativo na criação de demanda por registro de nascimento e identificação civil. Assim, ajuda a tornar populações invisíveis ao Estado elegíveis para programas como o Bolsa Família. Ser uma pessoa sem documentos no Brasil significa ser um cidadão de segunda classe, talvez ainda pior: uma pessoa que não possui documento de identificação pode se sentir desumanizada.

Por lei, o acesso a serviços públicos essenciais é gratuito para pessoas carentes, mas a complexidade do ecossistema de identidade impõe restrições aos indivíduos. É esse o caso, porque a regulamentação dos serviços requer a apresentação de documentos, conforme destacado por Raquel Chrispino, juíza do Rio de Janeiro:

"Existem regras brasileiras que impõem rotinas administrativas, por isso estamos falando de portarias, resoluções, de atos administrativos normativos que, para regular o serviço público, acabam obrigando os cidadãos a inserir alguns de seus números de identificação em um determinado sistema."(Chrispino, 2019).

Historicamente, os processos de inscrição para os grupos mais excluídos são diferentes dos da população em geral. Até indivíduos sem documentos são incluídos no registro e recebem instruções para emissão de registro de nascimento e documento de identidade (Ministério do Desenvolvimento Social do Brasil, 2015).

Com relação ao PBF, em sua maioria os beneficiários são mulheres negras ou pardas. A análise da composição familiar dos beneficiários do PBF revela que os núcleos familiares monoparentais chefiados por mulheres

representam a maior parte da população (Campello & Neri, 2014). Pesquisas qualitativas mostram que a inclusão de mulheres no Bolsa Família cria e expande oportunidades para as liberdades individuais, o que possibilita empoderamento das mulheres em geral (Campello & Neri, 2014). O papel essencial dos documentos pessoais para a emancipação do cidadão e o acesso aos serviços é evidente.

Apesar do reconhecimento global do programa de transferência condicionada de renda e de seu Sistema de Gestão de Informação, a inscrição no programa ocorre sob a condição prévia de que os beneficiários tenham seus dados totalmente exibidos no portal de transparência do governo. Embora a regulamentação brasileira de proteção de dados determine a necessidade de consentimento expresso e informado,[60] os dados sensíveis ainda são exibidos sob consentimento forçado, por ser um fator condicionante para acessar o PBF.

IMPRIMIR | BAIXAR | REMOVER/ADICIONAR COLUNAS | DETALHAMENTO DE BENEFÍCIOS AO CIDADÃO

DETALHAR	UF	MUNICÍPIO	CPF	NIS	BENEFICIÁRIO	VALOR DISPONIBILIZADO (R$)
Detalhar	CE	CATARINA	***.481.018-**	1.214	ADELINO	89,00
Detalhar	CE	CATARINA	***.268.023-**	1.613	ADRIANA	346,00
Detalhar	CE	CATARINA	***.896.003-**	1.614	ADRIANA	440,00
Detalhar	CE	CATARINA	***.898.933-**	2.031	ADRIANA	137,00
Detalhar	CE	CATARINA	***.030.691-**	1.616	ADRIANA	170,00
Detalhar	CE	CATARINA	***.044.408-**	2.003	ADRIANA	89,00
Detalhar	CE	CATARINA	***.460.293-**	1.60	ADRIANA	148,00
Detalhar	CE	CATARINA	***.000.000-**	1.613	ADRIANE	188,00

Fonte: Transparency Portal with full information of beneficiaries, Brazilian Federal Government <www.transparencia.gov.br>.

Um aspecto positivo é que o Número de Identificação Social (NIS) não está diretamente vinculado a um banco de dados biométricos. Se o governo pretende implementá-lo, isso deve ser feito com uma avaliação clara e ampla dos riscos, menções explícitas às salvaguardas da proteção de dados e por meio de consultas públicas.[61]

Por fim, um ponto-chave é o uso do Cadastro de Pessoas Físicas (CPF) como principal identificador no Brasil, pois é solicitado não apenas ao chefe da família, mas a todos os seus dependentes. O identificador de contribuinte não é uma identificação civil, e as irregularidades nos deveres eleitorais ou fiscais levam à exclusão daqueles que mais precisam. Portanto, deve haver uma reconsideração desse requisito para programas de proteção social ou uma reestruturação geral do sistema de identificação.

Seção 3

Lições aprendidas

Foto: Tales Duarte

3. Lições Aprendidas

A identidade alcança o núcleo essencial da dignidade humana. A identificação é uma questão anterior às agendas de transformação digital e governança de dados. No entanto, sua complexidade ainda é pouco compreendida e endereçada pelos elaboradores de políticas públicas. Essa faceta é frequentemente negligenciada, como resultado, os sistemas de identificação digital são implementados visando principalmente objetivos centrados no governo, ao contrário de uma abordagem centrada no usuário. Repete-se o que aconteceu durante a computarização das bases de dados governamentais na segunda metade do século passado.

Quais são os usos apropriados da identificação digital?

Durante a presente pesquisa, várias ideias importantes surgiram. Além das já destacadas nos casos de uso setoriais, esta seção apresenta quatro conjuntos de recomendações projetadas para formuladores de políticas e outras partes interessadas que enfatizam que o uso da identificação digital só pode ser apropriado quando se tratar de uma ferramenta que facilita o acesso a direitos e serviços pelo usuário. Além disso, esta seção também destaca que esses objetivos não podem ser alcançados quando o sistema de identificação digital não garantir inclusão, valor ao usuário, privacidade e segurança, porque pode significar uma barreira adicional - aprimorando a exclusão - ou uma forma discriminação. Esses parâmetros e suas recomendações subsequentes são:

1. Inclusão : A identificação digital só pode ser considerada apropriada quando for inclusiva.

» **Tenha cuidado para não reproduzir o problema de exclusão atual digitalmente.** Nos estudos de caso de todos os países, a identificação é obrigatória, legalmente ou *de facto*, para o plena fruição de direitos e serviços. A exclusão do acesso a serviços básicos devido à falta de identificação pode ser um problema analógico que não deve ser reproduzido ou ampliado digitalmente. Os principais documentos de identificação do Chile e do Peru (RUT e DNI, respectivamente) são essenciais para que os indivíduos realizem atos necessários e cotidianos. No entanto, a obtenção da ClaveÚnica, a chave chilena dos serviços digitais do governo, não é possível sem a RUT. A iniciativa peruana de inclusão

financeira (cuja principal barreira é a falta de meios de identificação) aborda apenas aqueles que possuem um número de celular, mas para obter um número de celular é necessário um documento nacional de identidade. O México parece estar seguindo o mesmo caminho, uma vez que a maioria dos procedimentos públicos e privados não pode ser realizada sem a identificação oficial e a identificação digital também tem sido gradualmente requerida.

» **O acesso a direitos e serviços básicos não deve depender da identificação digital.** Como observado, a identificação em qualquer formato não pode ser uma barreira para acessar serviços e direitos básicos. Conseqüentemente, tampouco em relação à identificação digital. Portanto, entender e considerar a desigualdade no acesso à infraestrutura de TIC e o contexto da educação digital é essencial ao implementar esse sistema. Muitos países latino-americanos ainda lutam contra a desigualdade no acesso à tecnologia e ao analfabetismo digital. Portanto, qualquer agenda que estabeleça a identificação digital como única via de acesso é excludente por concepção. O acesso multicanal é uma obrigação na região.

2. Valor ao usuário: Equilíbrio entre interesse individual e institucional.

» **Garanta que os esquemas de identificação digital promovam os direitos das pessoas, sem restringir suas liberdades e direitos civis.** Em relação aos usos setoriais, reflete-se a linha tênue entre a identificação como direito ou meio de intrusão, vigilância e um fator de aumento do desequilíbrio de poder entre instituições e indivíduos em um sistema de identificação fundacional. Portanto, o sistema de identificação deve ter claramente seus usos pretendidos, tanto no curto quanto no longo prazo. Isso também significa ser fundamental uma estratégia de implantação que trata da minimização de dados, com propósito claro e outras salvaguardas para proteger os usuários contra possíveis abusos.

» **Não faça parte do *hype* à custa do valor efetivo ao usuário.** A adoção de tecnologias emergentes, independentemente da adequação para um dado contexto, mostra um interesse predominante da instituição em parecer moderna, em vez de atender às reais necessidades de seus usuários. Por exemplo, alguns usos setoriais da identidade digital nas propostas do governo digital parecem ser principalmente propagandas políticas, pois, na realidade, a maioria dos serviços oferecidos não pode ser integralmente performados em meio digital ou, o pior, pode contribuir para aumentar a desigualdade de acesso serviços.

» **Quando a inovação agregar valor real ao usuário e promover inclusão, siga adiante.** Em certos contextos e usos setoriais, a identificação digital pode agregar valor real ao usuário e contribuir para a inclusão. Por exemplo, observou-se que, nos usos setoriais da inclusão financeira e proteção social, a identidade digital fornecia formas alternativas de determinar a unicidade de uma pessoa, ultrapassando eventuais barreiras ao acesso estabelecidas. No primeiro, a tecnologia contribuiu para facilitar transferências de dinheiro, remessas e pagamentos digitais, garantindo ao mesmo tempo o monitoramento financeiro, de forma a contribuir para a inclusão dos desbancarizados. No segundo, facilitou a inscrição no programa de proteção social. Fora dos estudos de caso da América Latina, também se diagnosticou o potencial de atualizações em tempo real para concessão de benefícios. Por exemplo, os usuários do sistema de identificação indiano (Aadhaar) afirmaram que a identificação biométrica viabilizou o controle pessoal de finanças e assegurou a regularidade nos pagamentos (Gelb, A. et. Al., 2017).

3. Privacidade : Priorize as leis de proteção de dados que salvaguardam a privacidade dos dados pessoais.

» **Estabeleça uma estrutura regulatória apropriada e abrangente.** Todos os quatro países do estudos de caso possuem leis de proteção de dados que protegem a privacidade de dados pessoais.[62] No entanto, como os estudos de caso deste relatório mostraram, a estrutura legal de proteção de dados deve ser apropriada e abrangente. A lei de proteção de dados do México carece de clareza. Por exemplo, o conceito impreciso de interesse legítimo (autorizar a coleta de dados pessoais sem o consentimento do titular dos dados) dificulta a avaliação da adequação da coleta de dados e, consequentemente, a coleta excessiva, mesmo de familiares, é uma prática comum no país. No Chile, a legislação atual permite que qualquer pessoa acesse legalmente uma grande parte dos dados pessoais derivados do número de identificação chileno (RUT), que é considerado informação pública por vias legais.

» **Verifique se a legislação é amplamente conhecida e aplicada.** Os casos do México e do Peru ilustram como a falta de discussão e publicização de legislação relevante entre as partes interessadas também minimiza a eficácia dos direitos legalmente reconhecidos. No caso mexicano, uma das barreiras ao cumprimento da legislação é a falta de mecanismos de conscientização e prestação de contas, enquanto no Peru há resistência devido às formas autoritárias percebidas de

conceber e impor essa legislação. No Chile, a legislação de proteção de dados pessoais não protege adequadamente a privacidade dos dados - ao não proteger o número RUT com um status privado, vários outros dados são acessíveis legalmente por qualquer pessoa, comprometendo significativamente a privacidade dos usuários.

4. Segurança: Análise de forma abrangente a segurança e a privacidade desde a concepção.

» **Garanta mecanismos robustos para proteger a privacidade e a integridade dos dados do usuário**. Sem um design tecnológico robusto, adequado e seguro que garanta a capacidade do sistema de proteger dados do usuário, a identidade digital não deve ser implementada. Os estudos de caso mostram explicitamente como os dados individuais estão extremamente expostos atualmente. Por exemplo, há um registro importante de vazamento de dados de identidade sob os auspícios do governo mexicano. O fato de que os dados financeiros e de saúde, exigidos nos usos setoriais da identificação digital, são muito sensíveis e seu uso indevido ou vazamento que podem levar à exclusão e discriminação não devem ser negligenciados. Para citar apenas alguns riscos, a exposição a um status de doença ou situação de vulnerabilidade econômica pode significar ter crédito negado ou taxas mais altas em seguros de saúde, perpetuando a exclusão socioeconômica e de acesso à serviços em vez de reduzi-las.

» **A coleta dados confidenciais deve ser minimizada.** Existem diferentes conjuntos de dados mínimos para fins de setores específicos. No entanto, a maioria deles captura mais dados para registro do que o necessário para sua finalidade original. Isso compromete a segurança porque a quantidade de dados coletados é proporcional ao risco de desvio de propósito e aos possíveis danos à privacidade dos usuários em caso de vazamento, uso indevido ou compartilhamento não autorizado. O caso do México ilustra requisitos injustificados de dados a serem adicionados aos prontuários eletrônicos dos usuários, como títulos de eleitor e impressões digitais do titular e de seus familiares.

Anexo I: Etapas da pesquisa

Na primeira etapa, realizamos uma sólida revisão da literatura sobre gestão de identidades por uma perspectiva cronológica, geográfica e multissetorial. As principais fontes de pesquisa foram periódicos, livros, sites e artigos. Entre eles, é relevante destacar o: Revolução da identificação: a identificação digital pode ser aproveitada para o desenvolvimento? (Gelb e Metz, 2018); Diagnósticos de governo digital da OCDE;[63] Avaliação do Access Now sobre Identidades Digitais Nacionais (2018);[64] Roteiro da União Internacional de Telecomunicações para Identidade Digital (2018);[65] Coleção ID4D do Banco Mundial, com foco no Guia do Profissional (2019)[66] e diagnóstico de países; e relatório da McKinsey Identificação Digital: uma chave para o crescimento inclusivo (2019).[67] Também realizamos pesquisas bibliográficas específicas sobre usos setoriais. Além disso, avaliamos documentos históricos de identificação da América Latina para entender melhor o cenário regional.

Na segunda etapa, analisamos os casos de uso setoriais. Focamos em serviços governamentais digitais, inclusão financeira, assistência médica e proteção social. A escolha foi porque esses setores poderiam fornecer uma visão geral relevante da identificação digital em termos de direitos fundamentais (saúde e proteção social) e serviços emergentes (governo digital e inclusão financeira). Cada um dos casos de uso setoriais foi acompanhado por um estudo de caso.

Na terceira etapa, realizamos análises específicas de paises e uma série de entrevistas em cada país. As escolhas do estudo de caso foram baseadas na discussão atual e nos dados disponíveis sobre esses usos setoriais em países latinos específicos. Descobrimos que seria apropriado focar no México para os cuidados de saúde, devido ao seu registro eletrônico de vacinação. Peru para inclusão financeira devido à sua referência às carteiras móveis digitais alavancadas pela identidade única. Chile, para serviços de governo digital por existir uma abordagem integrada da identificação e uma agenda governamental digital avançada. Por fim, o Brasil para proteção social, pois seu programa de transferência condicionada de renda e seu sistema de gestão de informação são mundialmente reconhecidos

Notas

1. Uma identidade estabelecida dentro de um sistema destinado a ser usado por outras entidades. Os Estados costumam operar sistemas de identificação fundacional por meio de agências de Registro Civil e Estatísticas Vitais (CRVS) com bancos de dados centralizados. O Aadhaar da Índia e o número de segurança social nos Estados Unidos são exemplos de IDs fundacionais e, em alguns casos, certidões de nascimento, passaportes e outras credenciais emitidas pelo governo são usados também como IDs fundacionais

2. Além dos benefícios potenciais descritos, as organizações sinalizam os riscos inerentes aos sistemas de identificação digital e os desafios e oportunidades mais específicos ao contexto dos países do Sul Global.

3. Para mais informações sobre o movimento Good ID, confira: https://www.good-id.org/en/about/

4. Aadhaar, na Índia, e o e-ID, na Estônia, são dois exemplos de identidades digitais fundacionais.

5. Os níveis de casamento infantil na região permaneceram em torno de 25% na última década, enquanto outras áreas do mundo tiveram um declínio significativo, particularmente no sul da Ásia, onde os níveis de casamento infantil caíram de quase 50% para 30% no mesmo período. Para mais detalhes, acesse: <https://www.unicef.org/press-releases/latin-america-and-caribbean-decade-lost-ending-child-marriage>

6. A facilidade de uso do sistema deve considerar os níveis de educação digital dos usuários, idioma e idade.

7. Diversamente, era um método para identificar indivíduos em suas relações civis com o Estado e com outros indivíduos.

8. A citação original, em espanhol, foi: "*La Identificación de todos los habitantes sin distinción, para garantizar, como lo he dicho, el derecho al nombre y contribuir eficaz y seguramente a que sea verdad el buen funcionamiento de las instituciones del Estado, para bien de la sociedad por ellas regida*".

9. O índice é composto por três fatores: índice de serviços digitais, índice de telecomunicações e índice de capital humano.

10. A maioria dos países da América Latina está entre 0,45 e 0,65.

11. Embora o uso de ferramentas tecnológicas conduza à melhoria da qualidade do serviço, procedimentos claros e padronizados também são necessários, além de uma identificação digital multiuso, para que o usuário possa executar o processo de maneira ágil e eficiente.

12. Um estudo realizado pelo Banco Interamericano de Desenvolvimento (BID) mostra que entre os vinte países que prestam serviços de registro civil, quatorze devem manter uma cópia física das certidões de nascimento ou certificadas processadas digitalmente (BID, 2019).

13. Por exemplo, em 2016, o Banco Mundial estimou que uma parte significativa da população, principalmente nas áreas rurais, ainda não tem acesso à eletricidade. Retirado de <World Bank, Sustainable Energy for All (SE4ALL) database from the SE4ALL Global Tracking Framework led jointly by the World Bank, International Energy Agency, and the Energy Sector Management Assistance Program. https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?view=map>.

14. Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe.300/5000 Publicado em 2017 pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (7, place de Fontenoy, 75352 París 07 SP, França) - UNESCO e o Escritório Regional de Ciências da América Latina e no Caribe, Escritório da UNESCO em Montevidéu (Luis Piera 1992, Piso 2, 11200 Montevidéu, Uruguai).

15. O termo é usado como uso setorial da identidade digital pela literatura de identificação para desenvolvimento do Banco Mundial (ID4D).

16. O Mudamos é um aplicativo móvel que permite às pessoas apoiar iniciativas de projetos de lei no Brasil por meio de assinaturas eletrônicas. Ao fazer uso do mecanismo constitucional da democracia direta e garantir os níveis de garantia da identidade digital inviolável. A ferramenta facilitou o engajamento cívico em várias casas legislativas. Para mais infromações: <https://www.mudamos.org/>.

17. Diversos governos estão experimentando novas abordagens, incluindo identidades baseadas em blockchain, por exemplo, esse está entre os principais casos de uso da Infraestrutura Europeia de Serviços de Blockchain. Para mais informações: <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=147458240>

18. O Reino Unido adota um sistema de garantia de identidade que visa fornecer um único login confiável em todos os serviços digitais do governo do Reino Unido. See: <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>.

19. Como exemplo, o sistema de identificação e registros administrativos públicos brasileiros é muito fragmentado. Isso levou à crescente adoção do número de contribuinte como o principal identificador do país. Veja <http://mapadainformacao.com.br/>.

20. Por exemplo, quando a proposta do governo digital é principalmente uma marca política, mas, na realidade, a maioria dos serviços oferecidos não é 100% digitalmente performado.

21. Um exemplo dessa tendência é o my GovID da Commonwealth, que está sendo testado este ano na Austrália com um recurso de reconhecimento facial. Para mais informações: <https://www.mygovid.gov.au/>. Por outro lado, evidências empíricas mostraram a existência de viés de algoritmo, resultando em discriminação por idade, raça e etnia, levantando preocupações em seu estágio prematuro de adoção maciça. Para mais informações: <https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon>.

22. É importante enfatizar que a forma de identificação digital necessária deve garantir a segurança e a privacidade do usuário e, como um caso de utilidade pública, essa identidade digital necessária deve ser acessível a todos que desejam usá-la, o que significa que deve ser livre de discriminação e fácil de proteger.

23. Ao considerar os métodos de autenticação, o sistema de identificação do Reino Unido pode servir como exemplo, pois utiliza diferentes níveis de garantia de identidade em vez de uma única identidade "padrão ouro" necessária para acessar serviços governamentais on-line. A estrutura de garantia de identidade e os padrões desenvolvidos para determinar quais formas de evidência de identidade atendem a cada nível de garantia de identidade fornecem orientações valiosas para outros países e podem ser facilmente adaptados a diferentes contextos (Whitley, 2018).

24. Faz-se necessário ir aos escritórios do Registro Civil e de Identificação com o bilhete de identidade, fornecer um email, registrar-se no site e validar com o RUN.

25. Na instrução presidencial sobre transformação digital. Para mais informações: <https://digital.gob.cl/instructivo/acerca-de>.

26. Disponível em: <https://www.leychile.cl/Navegar?idNorma=141599>.

27. Para mais informações: <https://www.uncdf.org/financial-inclusion-and-the-sdgs>.

28. Segundo o Banco Mundial, a qualidade de vida pode ser melhorada mediante acesso aos serviços financeiros, considerando os possíveis investimentos, gerenciamento de riscos e seguros. Para mais informações: <https://www.worldbank.org/en/topic/financialinclusion/overview>.

29. O que difere é o conjunto de dados necessário. Os programas de inclusão financeira tendem a solicitar um número de identificação e um contato telefônico, enquanto os bancos tradicionais solicitam informações sobre o histórico financeiro de alguém - biográfico, biométrico, evidência de apoio e metadados

30. o centro do CDD, como um subconjunto do KYC, está o processo de garantir a identificação, verificação e capacidade de cumprir determinadas regras no setor financeiro. Destina-se a monitorar e entender a natureza das transações.

31. Para mais informações: <https://www.accessnow.org/whyid-letter/> e <https://privacyinternational.org/long-read/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk>.

32. Lançado em 2007 usando SMS para transferências em dinheiro, o M-PESA é o caso mais famoso de dinheiro móvel. Foi o resultado de uma grande empresa de telecomunicações do país (Safaricom) e de uma estrangeira (Vodafone). Após esse episódio, o setor de telecomunicações desenvolveu carteiras digitais baseadas em dispositivos móveis em todo o mundo.

33. No que diz respeito à autenticação sem senha, conceitos como prova de conhecimento-nulo, do ingês *Zero-Knowledge Proof*, e *Proof-Bullets* também estão no centro da identidade digital baseada em blockchain. Permite, por exemplo, que uma pessoa saiba se outra é compatível com regras específicas sem que esta divulgue informações confidenciais.

34. Vários bancos digitais dependem do reconhecimento de imagens de documentos oficiais, registros de vídeo e até mesmo transmissão ao vivo para prova de identidade.

35. Nesse sentido, a Força-Tarefa de Ação Financeira (FAFT) lançou um rascunho de consulta no final de 2019, identificando a relevância da identificação digital para garantir eficiência, confiabilidade, segurança e inclusão.

36. O procedimento KYC exige identificar e coletar uma série de dados de clientes de um ou mais serviços financeiros como critério de elegibilidade com base em princípios como: pontualidade a capacidade de executar todos os procedimentos de mitigação de riscos em um dado e tempo suficiente para uma tomada de decisão. Veracidade: a capacidade de expressar a verdade (considerando que enganosas e algumas omissões são moralmente equivalentes a mentiras) e integridade.

37. Com o crescimento dos serviços financeiros digitais, o consentimento está se tornando um tópico central da identidade digital no setor (Loufield e Vashish, 2020).

38. O sistema é ativado por uma maneira simplificada de estabelecer um KYC por meio da validação de identidade de uma autoridade central do estado para uma Lei específica sobre Dinheiro Eletrônico, regulando os recursos básicos do dinheiro eletrônico como um instrumento de inclusão financeira. Ley del Dinero Electrónico 2013 (Peru). Para mais informações: <https://www.bcrp.gob.pe/docs/Transparencia/Normas-Legales/ley-29985.pdfl>.

39. O representante do BIM argumentou que, apesar de quererem se tornar totalmente digitais em 2020, inclusive utilizando biometria, o custo para acessar o banco de dados da RENIEC é comparativamente mais alto do que outros países, mesmo para a abertura de contas bancárias. Um equivalente a 50 centavos de soles peruanos por pessoa que pode ser caro se considerarmos um cenário de centenas de milhares de carteiras sendo abertas diariamente.

40. Desde 2011, o Peru possui uma lei de proteção de dados pessoais e uma Autoridade Nacional de Proteção de Dados Pessoais (*Autoridad Nacional de Protección de Datos Personales*, ANPDP). No entanto, não é um órgão independente e funciona sob os auspícios do Ministério da Mulher e Justiça. De acordo com o Artigo 7 da Lei Orgânica da RENIEC, a entidade é responsável por "garantir a privacidade dos dados pessoais". Embora a ANPDP esteja em vigor há quase dez anos, eles confiam profundamente na RENIEC para garantir a proteção de dados. Para mais informações: <http://www.minedu.gob.pe/otd/pdf/normas/01-ley-26497-ley-organica-del-reniec.pdf>

41. Miguel Morachimo manifestou destacando que a RENIEC é responsável pelo cumprimento de suas próprias normas e não implementou mecanismos que possibilitem mecanismos de participação e revisão. Para alguns defensores da privacidade, os funcionários da autoridade de identificação apóiam a idéia da "cultura do sigilo"

42. A identificação incorreta de pacientes foi citada em mais de 100 análises de causa raiz individuais pelo Centro Nacional de Segurança do Paciente do Departamento de Assuntos dos Veteranos dos Estados Unidos (VA) de janeiro de 2000 a março de 2003. Fonte: Mannos D. NCPS patient misidentification study: a summary of root cause analyses. VA NCPS Topics in Patient Safety. Washington, DC, United States Department of Veterans Affairs, June–July 2003 (http://www.va.gov/ncps/TIPS/Docs/TIPS_Jul03.doc, 11 June 2006) + World Alliance for Patient Safety (2004, WHO); Nine Patient Safety Solutions (2007, WHO).

43. Os serviços eletrônicos de saúde (eHealth) também podem ser entendidos como o uso da Internet e outras tecnologias relacionadas no setor da saúde para melhorar o acesso, a eficiência, a eficácia e a qualidade dos processos clínicos e de negócios usados por organizações de saúde, médicos, pacientes, e consumidores, com o objetivo final de melhorar o estado de saúde dos pacientes. Vide. Eysenbach G. What is e-health? J Med Internet Res 2001;3(2):E20

44. O processo de correspondência deve estar vinculado ao sistema de indexação de pacientes e pode exigir um poder computacional significativo, uma infraestrutura de comunicação amplamente disponível e recursos consideráveis para implementá-lo on-line. Além disso, o uso de algoritmos está sujeito a problemas de precisão.

45. Isso depende de medidas de segurança, como segurança de acesso baseada em função, comunicações seguras e infraestrutura de tecnologia apropriada. Além disso, também são necessários controles adequados sobre o acesso às informações nos sites de assistência médica.

46. Embora essas preocupações sejam verdadeiras para qualquer sistema de identificação, elas aumentam no contexto de saúde, principalmente se identificadores únicos estiverem vinculados a registros de saúde ou outros dados sensíveis.

47. Por exemplo, dados confidenciais devem ser anonimizados, impedindo que o paciente seja reidentificado.

48. Esta é uma recomendação reconhecida em vários documentos internacionais, como a Convenção Internacional sobre a Proteção dos Direitos de Todos os Trabalhadores Migrantes e Membros de suas Famílias (art. 28) e o Relator Especial de Saúde do Escritório do Alto Comissário das Nações Unidas para os Direitos Humanos da ONU.

49. É gerado pelo Sistema Eletrônico Estabelecido (e-SINAC). Segundo o governo mexicano, o sistema já foi implementado em 21 estados e, em 2017, mais de 200 mil certificados eletrônicos foram emitidos. Para mais informações: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento-142911>.

50. Para mais informações: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento>.

51. Como se manifesta por um entrevistado, existe uma questão relacionada ao tráfego clandestino de dados de identidade e até houve vazamentos maciços de dados na posse do Instituto Nacional Eleitoral (INE), que fizeram o controle das pessoas sobre sua identidade. problemático.

52. Em comparação com a GDPR, que possui uma penalidade clara de 4% da receita anual de uma empresa como multa por não conformidade.

53. Em 2015, um banco de dados contendo registros de eleitores foi publicado on-line, expondo as informações pessoais de 93,4 milhões de cidadãos mexicanos. Em 2016, ocorreu um grande vazamento de dados do aplicativo de aluguel de carros Uber. Em outubro de 2017, foi revelado que a MoneyBack, empresa responsável por devolver imposto sobre valor agregado a turistas estrangeiros que visitaram o México, deixou um banco de dados não seguro na internet com 400 GB de arquivos de informações pessoais sensíveis, como números de passaporte, cartões de crédito e identificações oficiais de cidadãos estrangeiros. Para mais informações: <https://privacyinternational.org/state-privacy/1006/state-privacy-mexico>.

54. Em 2016, o Banco do México estimou o valor da fraude ligada ao roubo de identidade em 108 milhões de pesos, o que coloca o país na oitava posição do mundo nesse tipo de crime. Em 2017, fraudes com cartões bancários, roubo de identidade e acesso não autorizado ou uso indevido de informações pessoais foram as principais preocupações dos consumidores mexicanos, de acordo com o mais recente Índice de Segurança Unisys. Para mais informações: <https://mundocontact.com/preocupa-a-mexicanos-robo-de-identidad/>; <https://mundocontact.com/robo-de-identidad-y-fraude-bancario-angustia-a-mexicanos/>.

55. Não é possível afirmar que existe uma causalidade entre a redução da pobreza e o acesso à documentação pessoal, mas podemos afirmar que as estratégias que combinaram esses dois elementos criaram condições favoráveis para melhorar os dois problemas.

56. O continente vem alcançando resultados valiosos. Em vinte anos, os países latino-americanos obtiveram progressos significativos em relação à cobertura do registro de nascimento. Em 2000, o continente tinha 76% de cobertura para crianças menores de cinco anos e, agora, de acordo com um relatório recente da UNICEF, esse percentual cresceu para 94%. Para mais informações: <https://www.unicef.org/reports/birth-registration-every-child-2030>.

57. Mesmo com um quarto da população recebendo transferência de renda, muitos beneficiários ainda permanecem em situações vulneráveis (UNU-WIDER, 2016).

58. O caso Aadhaar é emblemático porque coletou dados biométricos de mais de um bilhão de pessoas, fornecendo, portanto, identificação digital exclusiva para quase toda a população. No entanto, existem alguns casos de pensões alimentícias negadas devido à falhas na autenticação do sistema, bem como casos de discriminação de grupos marginalizados. Para mais informações <https://www.hrw.org/news/2018/01/13/india-identification-project-threatens-rights>.

59. A biometria pode fazer as pessoas *"se sentirem vigiadas, rastreadas, etiquetadas e perfiladas, e isso terá consequências na maneira como elas constituem sua política e sua expressão. A vulnerabilidade da pobreza agrava essa ameaça à liberdade. Certamente, haverá alguém em algum lugar que dirá que os pobres não têm utilidade para a liberdade "*, como destacado por Ramanathan (2014).

60. O Ministério responsável também disponibiliza via internet os bancos de dados anonimizados para fins de pesquisa. No entanto, o governo deve esclarecer como eles impedem a reidentificação por meio da inferência de dados.

61. Surgem preocupações adicionais quanto à proteção de dados com o decreto que criou o Cadastro Base do Cidadão visando a interoperabilidade entre bancos de dados do governo, mas sem divulgar, se houve, a avaliação de risco de dados e sem o engajamento com a sociedade civil. A propósito, as organizações da sociedade civil ficaram surpresas com a medida. Para mais informações: <http://www.in.gov.br/en/web/dou/-/decreto-n-10.046-de-9-de-outubro-de-2019-221056841>.

62. A legislação brasileira de proteção de dados foi aprovada em 2018 e deveria entrar em vigor em agosto de 2020. Todavia, não se sabe com precisão quanto efetivamente entrará.

63. A OCDE possui um conjunto de diagnósticos nacionais de governo digital que classifica uma estrutura de identidade digital como um elemento fundamental. Neste projeto, usamos principalmente as análises do Brasil, México, Peru e Chile. Disponível em: <http://www.oecd.org/gov/digital-government/>.

64. O Access Now analisou, como representante do terceiro setor, algumas identidades digitais nacionais específicas e apresentou recomendações específicas sobre o uso de dados biométricos. Disponíveis em: <https://www.accessnow.org/national-digital-identity-programmes-whats-next/>.

65. O roteiro da União Internacional de Telecomunicações (UIT) sobre identidade digital fornece o diagnóstico dos países, bem como recomendações sobre as melhores práticas, e padrões. Disponível em: <https://www.itu.int/pub/D-STR-DIGITAL.01-2018>.

66. Lançado oficialmente em meados de 2019, este relatório é uma diretriz estendida para tomadores de decisão e profissionais de operações para desenvolver uma estratégia de identidade digital, levando em consideração o status quo do contexto fornecido, suas particularidades, o conjunto de opções de política, design e tecnologia. e suas implicações. Disponível em: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-Guide-Draft-for-Consultation.pdf>.

67. O McKinsey Global Institute lançou, no primeiro semestre de 2019, um relatório extenso que também examinou diferentes fontes de criação de valor por meio do uso da identificação digital. Destacou o enorme potencial de aumento do PIB até 2030, tanto em países desenvolvidos (3%) quanto em países em desenvolvimento (6%), em média. Para mais informações: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>.

Referências

Aadil, A., Gelb, A., Giri, A., Mukherjee, A., Navis, K., Thapliyal, M. (2018). Digital Governance: Is Krishna a Glimpse of the Future?. Center for Global Development Notes. Retrieved from <https://www.cgdev.org/sites/default/files/digital-governance--krishna-glimpse-future-working-paper.pdf>.

Access Now. (2018). National Digital Identity Programmes: What's next?. Retrieved from: <https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf>.

ACP. (2019). Extreme poverty and digital welfare: New report from UN Special Rapporteur on extreme poverty raises alarm about the rise of a digital welfare dystopia. Retrieved 30 March, from: <https://www.apc.org/en/news/extreme-poverty--and-digital-welfare-new-report-un-special-rapporteur-extreme-poverty-raises>.

Appaya, S., Varghese, M. (2019). Digital ID – a critical enabler for financial inclusion. Retrieved 28 March, from: <https://blogs.worldbank.org/psd/digital-id-critical-enabler-financial-inclusion>.

Banco Central do Brasil. (2009). Perspectivas e desafios para inclusão financeira no Brasil: visão de diferentes atores. Brasília. Retrieved from: <https://www.bcb.gov.br/Nor/Deorf/projincfin/livro_inclusao_financeira_internet.pdf>.

Baya, V. (2019). Digital Identity: Moving to a decentralized future. Retrieved 30 March, from: <https://www.citi.com/ventures/perspectives/opinion/digital-identity.html>.

Barca, V., Makin, P & Bamezai, A. (2018). Integrating digital identity into social protection. An Analysis of potential benefits and risks. Discussion Paper. Oxford Policy Management.

Bhadra, S. (2019). Five Surprisingly Consequential Decisions Governments Make About Digital Identity. Retrieved 30 Msfrom: <https://www.omidyar.com/blog/five-surprisingly-consequential-decisions-governments-make-about-digital-identity>

Centre of Excellence for CRVS Systems. (2020). Gender Equality. Retrieved 30 May from: <https://crvssystems.ca/gender-equality>.

Center for Financial Inclusion (2019). Digital Financial Inclusion in Peru; A Promising Trend to Watch. Retrieved from: <https://www.centerforfinancialinclusion.org/digital-financial-inclusion-in--peru-a-promising-trend-to-watch>.

Chirchir, R., Barca, V. (2020). Building an integrated and digital social protection information system. Retrieved from: <https://socialprotection.org/sites/default/files/publications_files/GIZ_DFID_IIMS%20in%20social%20protection_long_02-2020.pdf>.

The Bureau of National Affairs. (2015). Privacy in Latin America and the Caribbean. Retrieved from: <https://www.bna.com/uploadedFiles/BNA_V2/Legal/Pages/Custom_Trials/PVRC/Privacy_Laws_Latin_America.pdf>.

Campello, T., Neri, M. C. (2014). Bolsa Família Program: a decade of social inclusion in Brazil. Brasília. Ipea.

Carmona, S. C. (2019). Biometric technology and beneficiary rights in social protection programmes. International Social Security Review. 4 (72), 3-28.

Caruso, C. (2016). Digital Financial Inclusion in Peru; A Promising Trend to Watch. Retrieved 30 March, from: <https://www.

centerforfinancialinclusion.org/digital-financial-inclusion-in-peru-a-promising-trend-to-watch>.

Center for Global Development. (2017a). Identification Revolution: Can Digital ID Be Harnessed for Development?. Retrieved from: <https://www.cgdev.org/sites/default/files/identification-revolution-can-digital-id-be-harnessed-development-brief.pdf>.

Center for Global Development (2017b). Identification as a National Priority: The Unique Case of Peru. Retrieved from: <https://www.cgdev.org/sites/default/files/identification-national-priority-unique-case-peru.pdf>.

Center of Excellence for CRVS Systems. (2020). Gender equality. Retrieved 30 March, from: <https://crvssystems.ca/gender-equality>.

Clavijo, S., Vera, N., Londoño, J., Beltrán, D. (2019). Digital Financial Services (FINTECH) in Latin America. Retrieved from: <https://www.anif.com.co/sites/default/files/investigaciones/anif-fintech-wpaper0219.pdf>.

Chrispino, R. (2019, September). Identidade como acesso à cidadania. (COSTA. J, Interviewer).

Comisión Multisectorial de Inclusión Financiera. (2015). Estrategia Nacional de Inclusión Financiera. Retrieved from: <http://www.mef.gob.pe/contenidos/archivos-descarga/ENIF.pdf>.

Comisión Nacional de Arbitraje Médico. (2018). El expediente clínico electrónico universal en México. Mexico. Retrieved from <http://www.conamed.gob.mx/gobmx/boletin/pdf/boletin18/expediente.pdf>.

Cortés, R. A. (2019). El nuevo entorno regulatorio de la protección de datos personales en Chile. Retrieved 30 March, from: <https://iapp.org/news/a/el-nuevo-entorno-regulatorio-de-la-proteccion-de-datos-personales-en-chile/>.

Dreze, J., Khalid, N., Khera, R., Somanchi, A. (2017). Pain without gain? Aadhaar and food security in Jharkhand.Economic and political weekly. Vol. 52, Issue No. 50. Retrieved 30 March, from: <https://www.epw.in/journal/2017/50/special-articles/aadhaar-and-food-security-jharkhand.html>.

Domínguez, M. (2018). Access and use of information and communication technologies in Mexico: determining factors. PAAKAT: Revista De Tecnología Y Sociedad. Vol. 8 No. 14. Retrieved 30 March, from <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072018000200002&lang=pt>.

ECLAC (2015). Inclusive social development: The next generation of policies for overcoming poverty and reducing inequality in Latin America and the Caribbean. Santiago de Chile. Retrieved from: <https://repositorio.cepal.org/bitstream/handle/11362/39101/4/S1600098_en.pdf>.

Enríquez, O. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Revista IUS, 12(41), 267-291. Retrieved 10 December 2019, from <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870=21472018000100267-&lng=es&tlng=es>.

Escócia, F. (2019a). Invisíveis: uma etnografia sobre identidade, direitos e cidadania nas trajetórias de brasileiros sem documento. Retrieved from: <http://www.mprj.mp.br/documents/20184/151138/escossiafernandameloda.invisiveis_umaetnografiasobreidentida.pdf>.

Escóssia, F. (2019b, September). Identidade

como acesso à cidadania. (COSTA. J, Interviewer). Retrieved 30 March, from: <https://www.youtube.com/watch?v=8yK3FHEnpnA>.

FAFT. (2014). Guidance for a Risk-Based Approach The Banking Sector. Retrieved from: <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>.

FATF. (2019). Public consultation on FATF draft guidance on digital identity. Retrieved 30 March, from: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html>.

Ferrari, M. G. Marcas de identidad. Juan Vucetich y el surgimiento transnacional de la dactiloscopia (1888-1913). Rosario: Prohistoria Ediciones, 2015.

Gelb, A., Metz, A. D. (2018). Identification Revolution: Can Digital ID Be Harnessed for Development? Center for Global Development. Washington, DC.

Gelb, A., Mukherjee, A., Navis, K., Thaplyal, M., Giri, A. (2017). What a New Survey of Aadhaar Users Can Tell Us About Digital Reforms: Initial Insights from Rajasthan. Center for Global Development. CGD Notes. Retrieved 30 March, form: <www.cgdev.org/publication/what-a-new-survey-aadhaar-users-can-tell-us-about-digital-reforms-initial-insight>.

Gelb, A., Mukherjee, A., Navis, K., (2020). How Can Digital ID and Payments Improve State Capacity and Effectiveness? Center for Global Development Notes. Retrieved from <https://www.cgdev.org/sites/default/files/citizens-and-states-how-can-digital-id-and-payments-improve-state-capacity.pdf>.

Gobierno Digital Chile. (2019). División de Gobierno Digital. Retrieved 30 March, from <https://digital.gob.cl/plan/identidad-digital>.

Gobierno Digital Chile. (2018). Estrategia de Transformación Digital del Estado: Estado al Servicio de las Personas. Retrieved from: <https://digital.gob.cl/doc/estrategia_de_transformacion_digital_2019_.pdf>.

GSMA. (2016.) Digital identity as a key enabler for e-government services. Retrieved from: <https://www.gsma.com/identity/wp-content/uploads/2016/02/MWCB16-Digital-Identity-as-a-Key-Enabler-for-eGovernment-Services-Marta-Ienco.pdf>.

GSMA. (2016). Digital Identity: a prerequisite for Financial Inclusion?. Retrieved 30 March, from: <https://www.gsma.com/mobilefordevelopment/country/global/digital-identity-a-prerequisite-for--financial-inclusion/>.

Hellmann, A. G. (2015). How does Bolsa Familia work?: Best practices in the implementation of conditional cash transfer programs in Latin America and the Caribbean. IADB. Retrieved 30 March, from: <https://publications.iadb.org/en/how-does-bolsa-familia-work-best-practices-implementation-conditional-cash-transfer-programs--latin>.

Hunter, W., Brill, R. (2016). “Documents, Please”: Advances in Social Protection and Birth Certification in the Developing World. World Politics, 68(2), 191-228. doi:10.1017/S0043887115000465

Hunter, W. (2019). Identity Documents, Welfare Enhancement, and Group Empowerment in the Global South. The Journal of Development Studies, 55(3), 366-383, doi: 10.1080/00220388.2018.1451637

IADB. (2017). La gestión de la identidad y su impacto en la economía digital. Retrieved from: <https://www.alejandro-barros.com/wp-content/uploads/2016/04/

Gestion-de-la-identidad-y-su-impacto-en-la-economia-digital.pdf>.

IADB. (2019). Registros civiles y oficinas de identificación: Análisis y fichas de país. Retrieved from: <https://publications.iadb.org/publications/spanish/document/Registros_civiles_y_oficinas_de_identificaci%C3%B3n_an%C3%A1lisis_y_fichas_de_pa%C3%ADs_es.pdf>.

Ibarra, A. B., Byanyima, W. (2016). Latin America is the world's most unequal region. Here's how to fix it. Retrieved 30 March, from: <https://www.weforum.org/agenda/2016/01/inequality-is-getting-worse-in-latin-america-here-s-how-to-fix-it/>.

ITU News. (2019). Unique, legal and digital: Three characteristics of ID crucial to financial inclusion. Retrieved 30 March, from: <https://news.itu.int/unique-legal-digital-id-financial-inclusion/>.

Laval, C. E. P. (2018). Utopías de control detrás de la identificación civil: los proyectos de identificación de Clodomiro Cabezas Cabezas. Chile, 1927-1938, Revista Historia y Justicia. Retrieved 30 March, from: <https://doi.org/10.4000/rhj.1260>.

Lindert, K., Linder, A., Hobbs, J., Briere, B. (2007). The Nuts and Bolts of Brazil's Bolsa Família Program: Implementing Conditional Cash Transfers in a Decentralized Context. World Bank Group. Retrieved from: <http://documents.worldbank.org/curated/pt/972261468231296002/pdf/398530SP1709.pdf>.

Loufield, E., Vashisht, S. (2020). Data Consent: Let's Share the Burden for Effective Consumer Protection. Center for Financial Inclusion. Retrieved 30 May from: <https://www.centerforfinancialinclusion.org/data-consent-lets-share-the-burden-for-effective-consumer-protection>.

Masiero, S. (2017). Digital governance and the reconstruction of the Indian anti-poverty system. Oxford Development Studies, 45 (4), 393-408.

Masiero, S. (2019). The Digitalization of Anti-poverty Programs: Aadhaar and the Reform of Social Protection in India. Digital Economies at Global Margins. Ed. Mark Graham. MIT Press Direct.

Mastercard. (2019a). Digital Identity: Restoring Trust in a Digital World. Retrieved from: <https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf>.

Mastercard. (2019b). Examining the Latin American and Caribbean E-commerce Market. Retrieved from: <https://newsroom.mastercard.com/latin-america/files/2019/12/Whitepaper-Digital-Security-mastercard-ENG-simples-FINAL2.pdf>.

McKinsey Global Institute (2019). Digital identification: A key to inclusive growth. Retrieved 30 March, from: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>.

Mexico Digital. (2018). Certificado Electrónico de Nacimiento. Retrieved 13 December 2019, from: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento-142911>.

Mexico Digital. (2014). Certificado Electrónico de Nacimiento. Retrieved 13 December 2019, from: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento>.

Ministry of Social Development Brazil. (2015). Guia de Cadastramento de Famílias Indígenas. MDS. Brasília.

Muralidharan, K., Niehaus, P., Sukhtankar, S (2020). Identity Verification Standards in Welfare

Programs: Experimental Evidence from India. National Bureau of Economic Research Working Paper, 26744

Muralidharan, K., Niehaus, P. & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. American Economic Review 106 (10), 2895-2929.

Murthy, G. & Medine, D. (2018). Data Protection and Financial Inclusion: Why Consent Is Not Enough. Blog Series: Data Privacy and Protection. Consultative Group to Assist the Poor. Retrieved 30 March, from: <http://cgap.org/blog/data-protection-and-financial-inclusion-why-consent-not-enough>.

Muzzi, M. (2010). Good Practices in Integrating Birth Registration into Health Systems (2000-2009). Unicef. Retrieved from: <https://www.unescap.org/sites/default/files/UNICEF-birth-registration-in-health-systems.pdf>.

OEA. (2008). Diagnóstico del marco jurídico-institucional y administrativo de los sistemas de Registro Civil en América Latina. PUICA. Retrieved from: <http://www.oas.org/sap/docs/puica/diagnostico_legal_administrativo.pdf>.

OECD. (2001). Understanding the Digital Divide. OECD Digital Economy Papers, No. 49, OECD Publishing, Paris, page 5. Retrieved 30 March, from: <https://doi.org/10.1787/236405667766>.

OECD. (2009). The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers. OECD Digital Economy Papers. (Report No. 160). OECD Publishing, Paris. Retrieved 30 March, from <https://doi.org/10.1787/20716826>.

OECD. (2019a). Shaping the Digital Transformation in Latin America: Strengthening Productivity, Improving Lives, OECD Publishing, Paris. Retrieved 30 March, from: <https://doi.org/10.1787/8bb3c9f1-en>.

OECD. (2019b). Harnessing the Digital Transformation to Boost Productivity in Latin America and the Caribbean. Retrieved 30 March, from: <https://www.oecd.org/about/secretary-general/harnessing-digital-transformation-to-boost-productivity-in-lac-colombia-october-2019.htm>.

OECD. (2019c). Digital Government in Chile – Digital Identity. Retrieved from: <https://www.oecd-ilibrary.org/sites/9ecba35e-en/index.html?itemId=/content/publication/9ecba35e-en&mimeType=text/html>.

OECD (2019d). Strengthening Digital Government. Retrieved from: <https://www.oecd.org/going-digital/strengthening-digital-government.pdf>.

OECD (2019e). Digital Government in Chile – A Strategy to Enable Digital Transformation, OECD Digital Government Studies, OECD Publishing, Paris. Retrieved from: <https://doi.org/10.1787/f77157e4-en>.

Pan American Health Organization (PAHO). (2016). eHealth in the Region of the Americas: breaking down the barriers to implementation. Retrieved 30 March, from: <https://iris.paho.org/bitstream/handle/10665.2/31286/9789275119259-eng.pdf?sequence=6&isAllowed=y>.

Peirano, M. (2009). O paradoxo dos documentos de identidade: relato de uma experiência nos Estados Unidos. Retrieved from: <http://www.mprj.mp.br/documents/20184/151138/peirano,mariza.oparadoxodosdocumentosdeidentidade.pdf>.

Privacy International. (2012). Medical privacy and security in developing countries and emergency situations. Retrieved from:

<https://privacyinternational.org/sites/default/files/2018-11/Privacy_International_Medical_Privacy.pdf>.

Privacy International. (2018). Liliana: "If you don't have RUT, you can't do it.". Retrieved 30 March, from: <https://privacyinternational.org/case-study/2545/liliana-if-you-dont-have-rut-you-cant-do-it>.

Ramada-Sarasola, M. (2012). Can Mobile Money Systems Have a Measurable Impact on Local Development?. Retrieved 30 May from: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2061526>.

Ratcliffe, R. (2019). How a glitch in India's biometric welfare system can be lethal. Automating poverty Series. The Guardian. Retrieved 30 March, from <https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation>.

Ramanathan, U. (2014). Biometrics Use for Social Protection Programmes in India Risk Violating Human Rights of the Poor. Retrieved 30 March, from: <http://www.unrisd.org/sp-hr-ramanathan>.

Sepúlveda, M. (2019). Data Protection is Social Protection. Retrieved 30 May from: <https://www.project-syndicate.org/commentary/social-protection-biometric-data-privacy-by-magdalena-sepúlveda-2019-04?barrier=accesspaylog>.

Tase TH, Lourenção DCA, Bianchini SM, Tronchin DMR (2013). Patient identification in healthcare organizations: an emerging debate. Rev Gaúcha Enferm.;34(2):196-200.

UN. (2018). E-Government Survey: Gearing e-government to support transformation towards sustainable and resilient societies. Retrieved from: <https://publicadministration.un.org/Portals/1/Images/E-Government%20Survey%202018_FINAL%20for%20web.pdf>.

UN Secretary-General. (2019). Secretary-General's opening remarks to the High-level Event on "10 Years of Financial Inclusion - Vast Progress and Challenges Ahead". Retrieved 30 March, from: <https://www.un.org/sg/en/content/sg/statement/2019-09-25/secretary-generals-opening-remarks-the-high-level-event-10-years-of-financial-inclusion-vast-progress-and-challenges-ahead-delivered>.

UNAIDS. (2014). Considerations and guidance for countries adopting national health identifiers., Geneva, 17 April 2014. Retrieved from: <https://www.unaids.org/sites/default/files/media_asset/JC2640_nationalhealthidentifiers_en.pdf>.

UNCDF. (2020). Financial Inclusion and the SDGs. Retrieved 30 May from: <https://www.uncdf.org/financial-inclusion-and-the-sdgs>.

UNESCO and the Regional Bureau for Sciences in Latin America and the Caribbean (2017). Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe. Retrieved 30 March, from: <https://unesdoc.unesco.org/ark:/48223/pf0000262860>.

UNESCO. (2009). Regional overview: Latin America and the Caribbean. Retrieved from: <https://en.unesco.org/gem-report/sites/gem-report/files/178428e.pdf>.

UNICEF. (2018). Latin America and the Caribbean: a decade lost in ending child marriage. Retrieved 30 May from: <https://www.unicef.org/press-releases/latin-america-and-caribbean-decade-lost-ending-child-marriage>.

UNRISD. (2010). Combating Poverty and Inequality: Structural Change, Social Policy and Politics. Retrieved from: <http://www.unrisd.

org/80256B3C005BCCF9/(httpAuxPages)/92B-1D5057F43149CC125779600434441/$file/PovRep%20(small).pdf>.

UNU-WIDER. (2016). Cash transfers in Latin America: Effects on poverty and redistribution. Retrieved 30 May from: <https://www.wider.unu.edu/publication/cash-transfers-latin-america>.

Villarreal, F. G. (ed.). (2017). Inclusión financiera de pequeños productores rurales, Libros de la CEPAL, N° 147 (LC/PUB.2017/15-P), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2017. Retrieved 30 March, from: <https://repositorio.cepal.org/bitstream/handle/11362/42123/S1700277_es.pdf?sequence=1&isAllowed=y>.

Vucetich, J (1916). Comment in the Creation of the Identity Law of (Ley de Registro de Identidad de las Personas). Registro General de Identificación. Argentina.

Whitley, E. A. (2018). Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach. CGD Policy Paper. Washington, DC: Center for Global Development. Retrieved 30 March, from: <https://www.cgdev.org/publication/trusted-digital-identity-provision-gov-uk-verify-federated--approach>.

World Bank (2016). Identification Principles for Sustainable Development: toward the digital age. Retrieved from World Bank ID4D website <http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples--Folder-web-English-ID4D-IdentificationPrinciples.pdf>.

World Bank. (2018a). G20 Digital Identity Onboarding. Retrieved from: <https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf>.

World Bank. (2018b). Global ID Coverage, Barriers, and Use by the Numbers: Insights from the ID4D-Findex Survey. Retrieved from: <http://documents.worldbank.org/curated/en/953621531854471275/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-Insights-from-the-ID4D-Findex-Survey.pdf>.

World Bank (2018c). The Role of Digital Identification for Healthcare: The Emerging Use Cases. Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO); Retrieved from World Bank ID4D website <http://documents.worldbank.org/curated/en/595741519657604541/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf>.

World Bank. (2018d). Guidelines for ID4D Diagnostics. Retrieved from: <http://documents.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf>.

World Bank (2019a). Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable. Retrieved 13 December, from: <https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds--most-vulnerable>.

World Bank (2019b). ID4D Practitioner' Guide, Version 1.0 (October 2019). Washington, DC. Retrieved from: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>.

WHO. (2007). Patient Identification. Retrieved from: <https://www.who.int/patientsafety/solutions/patientsafety/PS-Solution2.pdf>.

WHO & ITU. (2012). National eHealth Strategy Toolkit. Retrieved from: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.05-2012-PDF-E.pdf>.

World Economic Forum (2018). The appropriate use of Customer Data. Retrieved from: <http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf>.

World Economic Forum. (2020). Passwordless Authentication: The next breakthrough in secure digital transformation. Retrieved 30 March, from: <https://www.weforum.org/whitepapers/passwordless-authentication-the-next-breakthrough-in--secure-digital-transformation>.

Financiado por

OMIDYAR NETWORK

Encuéntranos

itsrio.org