

INSPER
Programa Avançado em Gestão Pública

Guilherme Martelato Campos

Identidade Digital Única: uma revisão da abordagem brasileira

SÃO PAULO - SP

2020

Guilherme Martelato Campos

Identidade Digital Única: uma revisão da abordagem brasileira

Trabalho de Conclusão de Curso
apresentado ao Programa Avançado em
Gestão Pública do Insper como requisito
parcial para obtenção do título de
Especialista em Gestão Pública.

Orientador: Prof. Manuel Ruas
Pereira Coelho Bonduki

SÃO PAULO - SP

2020

CAMPOS, Guilherme Martelato.

Identidade Digital Única: uma revisão da abordagem brasileira. /
Guilherme Martelato Campos. – São Paulo, 2020.

48 f.

Trabalho de Conclusão do Curso Programa Avançado em Gestão
Pública (Especialista) – Pós-Graduação em Gestão Pública - INSPER,
2020.

Orientador: Prof. Manuel Ruas Pereira Coelho Bonduki.

1. Políticas Públicas. 2. Transformação Digital. 3. Identidade Digital. 4.
Governo como Plataforma. I. Campos, Guilherme Martelato. II. Identidade
Digital Única: uma revisão da abordagem brasileira.

Guilherme Martelato Campos

Identidade Digital Única: uma revisão da abordagem brasileira

Trabalho de Conclusão de Curso
apresentado ao Programa Avançado em
Gestão Pública do Insper como requisito
parcial para obtenção do título de
Especialista em Gestão Pública.

Orientador: Prof. Manuel Ruas
Pereira Coelho Bonduki

Banca Examinadora

Prof. Manuel Ruas Pereira Coelho Bonduki
Insper

Prof. Eduardo Colagrossi Paes Barbosa
Insper

RESUMO

Estudos indicam que a implementação de uma identidade digital (ID) pode ajudar a alavancar a economia de um país, enquanto endereça aspectos da desigualdade social, e a comunidade internacional tem se posicionado em torno do que vem sendo entendido como uma *Good ID* (boa identidade), visando garantir a construção de um sistema de ID confiável, inclusivo e sustentável. Ao mesmo tempo, o Brasil tem se engajado na construção de um sistema de identidade única capaz de aumentar a eficiência do Estado, favorecer o combate a fraudes e simplificar a vida do cidadão há pelo menos 20 anos, mas ainda não conseguiu disponibilizar uma solução efetiva para toda a população. Esse trabalho, então, faz uma pesquisa exploratória e descritiva sobre o tema “Identidade Digital”, a partir de pesquisa documental em sites da web, relatórios e estudos de organizações nacionais e internacionais. E, em seguida, analisa qualitativamente a abordagem brasileira, segundo princípios de uma *Good ID*, e discute possíveis avanços em relação a modelo de solução, estrutura de governança e instrumentos legais e de regulação para o cenário brasileiro. O trabalho mostra que no complexo ecossistema de identificação brasileiro ainda não foi concebida, segundo uma visão sistêmica e integrada, uma identidade digital alinhada aos princípios de uma *Good ID*, mas que passos importantes para a sua construção já foram dados. E para avançar nesse sentido, o país poderia investir na integração de soluções existentes (DNI, Conta Gov.Br, certificados digitais ICP-Brasil); adotar práticas de identidades digitais de outros países para garantir a privacidade, segurança e transparência no uso dos dados pessoais dos cidadãos; estabelecer o papel de Autoridade de ID, para definir padrões e diretrizes para interoperabilidade; e atuar segundo o conceito de Governo como Plataforma, não sendo o único prestador de serviços de identificação e empoderando outros agentes para construir e sustentarem em conjunto a solução de identidade digital.

Palavras-chave: Políticas Públicas, Transformação Digital, Identidade Digital, Governo como Plataforma

ABSTRACT

Studies indicate that the implementation of a digital identity (ID) can help boost a country's economy, while addressing aspects of social inequality, and the international community has been positioning itself around what has been understood as a Good ID, aiming to guarantee the implementation of a reliable, inclusive and sustainable ID system. At the same time, Brazil has been engaged in the construction of a unique identity system capable of increasing the efficiency of the State, fighting fraud and simplifying citizens' lives for at least 20 years, but has not yet managed to provide an effective solution for the entire population. This work, then, performs an exploratory and descriptive research on the theme "Digital Identity", based on documentary research on web sites, reports and studies by national and international organizations. Then, it qualitatively analyzes the Brazilian approach, according to the principles of a Good ID, and discusses possible advances in relation to the solution model, governance structure and legal and regulatory instruments for the Brazilian scenario. This work shows that in the complex Brazilian identification ecosystem, a digital identity has not yet been conceived, according to a systemic and integrated vision and aligned with the principles of a Good ID, but important steps for its construction have already been taken. And to move in this direction, the country could invest in the integration of existing solutions (DNI, Conta Gov.Br, ICP-Brasil digital certificates); adopt practices of digital identities from other countries to ensure privacy, security and transparency in the use of citizens' personal data; establish the role of ID Authority, to define standards and guidelines for interoperability; and act according to the concept of Government as a Platform, not being the only provider of identification services and empowering other agents to jointly build and sustain the digital identity solution.

Keywords: Public Policies, Digital Transformation, Digital Identity, Government as a Platform

LISTA DE FIGURAS

Figura 1 - Registro e Identificação Cíveis e Identidade Funcional.....	12
Figura 2 - Ciclo de Vida da Identidade	13
Figura 3 - Potenciais Impactos da Identidade Digital	17
Figura 4 - Potencial Econômico Viabilizado pela ID Digital	21
Figura 5 - Visão geral do Mapa da Informação	31
Figura 6 - Processo de Identificação Digital na Conta Gov.Br	33
Figura 7 - Controle de Acesso de um Serviço aos Dados Pessoais de um usuário..	34

LISTA DE QUADROS

Quadro 1 - Papéis e Atores envolvidos nos sistemas de identidade.....	13
Quadro 2 - Arranjos possíveis para os sistemas de identificação	15
Quadro 3 - Marcos Regulatórios no Brasil	27
Quadro 4 - Exemplos de taxas para os serviços de verificação e autenticação de identidade.....	42

SUMÁRIO

1. INTRODUÇÃO.....	9
2. ASPECTOS METODOLÓGICOS	10
3. REVISÃO BIBLIOGRÁFICA	11
3.1. Identidade digital.....	11
3.2. O impacto da identidade digital e o cenário internacional.....	16
3.3. Princípios para uma boa identidade digital	18
3.4. <i>Frameworks</i> de análise.....	19
3.5. Riscos das abordagens de identidade digital	20
4. O PANORAMA BRASILEIRO	21
4.1. Histórico de iniciativas de identidade nacional	22
4.2. Há algum documento de identidade digital disponível para os brasileiros?..	24
4.3. Marcos regulatórios	26
4.4. Limitações do mecanismo de identificação atual.....	29
4.5. A solução vislumbrada pelo Governo Federal	32
5. POSSÍVEIS AVANÇOS PARA A IDENTIFICAÇÃO DIGITAL NO BRASIL	35
5.1. Modelo de Solução	36
5.2. Estrutura de Governança.....	40
5.3. Instrumentos legais e de regulação	43
6. CONCLUSÃO.....	44
REFERÊNCIAS.....	46

1. INTRODUÇÃO

O isolamento social realizado em resposta à pandemia provocada pelo coronavírus (COVID-19) obrigou pessoas e organizações a se adaptarem a uma nova realidade e a explorarem novas formas de se relacionar, acelerando um processo de transformação que já vinha acontecendo nas últimas décadas. Quem ainda relutava a aderir a esse processo, se deparou com a necessidade de se reinventar. Governos no mundo todo precisaram encontrar formas para chegar aos cidadãos que mais precisavam do seu auxílio, ao mesmo tempo em que precisavam garantir a continuidade na prestação dos seus serviços, tendo que migrar muitos deles para o mundo digital.

Nesse cenário, um desafio se mostrou muito presente: como comprovar a identidade de quem está do outro lado da relação sem poder ter contato físico e ainda garantir o acesso dessas pessoas a serviços e direitos? No cenário internacional, países como Estônia e Índia, que já vinham há anos passando por um intenso processo de transformação digital, se mostraram mais preparadas para responder com rapidez a uma situação atípica, como a do distanciamento social. E um dos fatores que mais contribuíram para a capacidade de resposta deles foi a existência de um sistema robusto e consolidado de identidade digital disponível para toda a população.

A pauta “Identidade Digital” não é nova e, nos últimos anos, diversas organizações internacionais têm recomendado os países a adotarem em suas agendas, por conta do seu potencial de impacto. Segundo estudo de MCKINSEY GLOBAL INSTITUTE (2019), por exemplo, cerca de 1 bilhão de pessoas no mundo não possuem qualquer identificação legal reconhecida e a ampla adoção da identidade digital em alguns países poderia gerar um crescimento entre 3% e 13% de seus PIB em 2030. Dada a importância do tema e o risco de usos indevidos, as mesmas organizações têm recomendado atenção a alguns princípios norteadores para se construir boas identidades digitais.

No caso do Brasil, o país vem tentando implementar um sistema de identidade única capaz de aumentar a eficiência do Estado, favorecer o combate a fraudes e simplificar a vida do cidadão há pelo menos 20 anos. Iniciativas recentes, como a

Conta Gov.Br e o Documento Nacional de Identidade (DNI), foram tentativas de se avançar na pauta em questão e a crise provocada pela pandemia pode ser a oportunidade que faltava para consolidar e evoluir esses projetos.

Nesse sentido, o presente trabalho visa contribuir para o debate público, analisando a iniciativa brasileira de identidade digital frente às recomendações internacionais e, com base na experiência de outros países, discutir possíveis melhorias para o modelo que está sendo planejado e implementado no Brasil.

2. ASPECTOS METODOLÓGICOS

O presente trabalho se propõe a fazer uma pesquisa exploratória e descritiva sobre o tema “Identidade Digital Única” e sobre o cenário brasileiro, seguido de uma análise qualitativa do modelo que está sendo planejado e implementado no país e articulado pela Secretaria de Governo Digital do Ministério da Economia do Governo Federal.

Os dados usados para a análise foram coletados a partir de pesquisa documental na web e em fontes oficiais dos entes da União. Para o estabelecimento do referencial teórico, foram consultados, em especial, relatórios de consultorias internacionais, como McKinsey, estudos de organizações internacionais, como OCDE e Banco Mundial, bem como materiais de pesquisas nacionais, como os produzidos pelo ITS Rio, organização sem fins lucrativos que se dedica, entre outras áreas de pesquisa, a fomentar discussões sobre identidade digital no Brasil. Para a análise do panorama brasileiro foram consultados principalmente notícias, apresentações e materiais de referência disponíveis no portal Gov.Br, além de legislações disponíveis no site do Planalto. Para a discussão sobre os possíveis avanços para a identificação digital brasileira (Capítulo 5), além do respaldo dos materiais do referencial teórico, foram consultados também sites de iniciativas de identidade digital de outros países, como da Estônia, Índia e Reino Unido.

3. REVISÃO BIBLIOGRÁFICA

3.1. Identidade digital

Identidade pode ter significados diversos em contextos diferentes. Porém, para o propósito desse trabalho, a identidade será tratada como o instrumento para o estabelecimento de relações de confiança entre indivíduos, entes privados e instituições públicas, garantia de acesso a serviços e cumprimento de direitos e deveres. Para tal, é suficiente entendê-la como a combinação de características que permitem diferenciar uma pessoa de qualquer outra num determinado contexto. Normalmente, para a identificação de alguém, são usados atributos pessoais como dados biográficos (ex.: nome, data e local de nascimento) e certas características biométricas (ex.: imagem do rosto, impressões digitais, leitura de íris e de retina). E quando esses dados são registrados por uma autoridade competente, como um cartório de registro civil, por exemplo, uma certidão é emitida (ex.: certidão de nascimento, carteira de identidade) e tem-se, então, uma identidade legal, respaldada por lei e reconhecida como válida por todas as partes interessadas. Esse será o principal tipo de identidade considerada nesse trabalho (BANCO MUNDIAL, 2019).

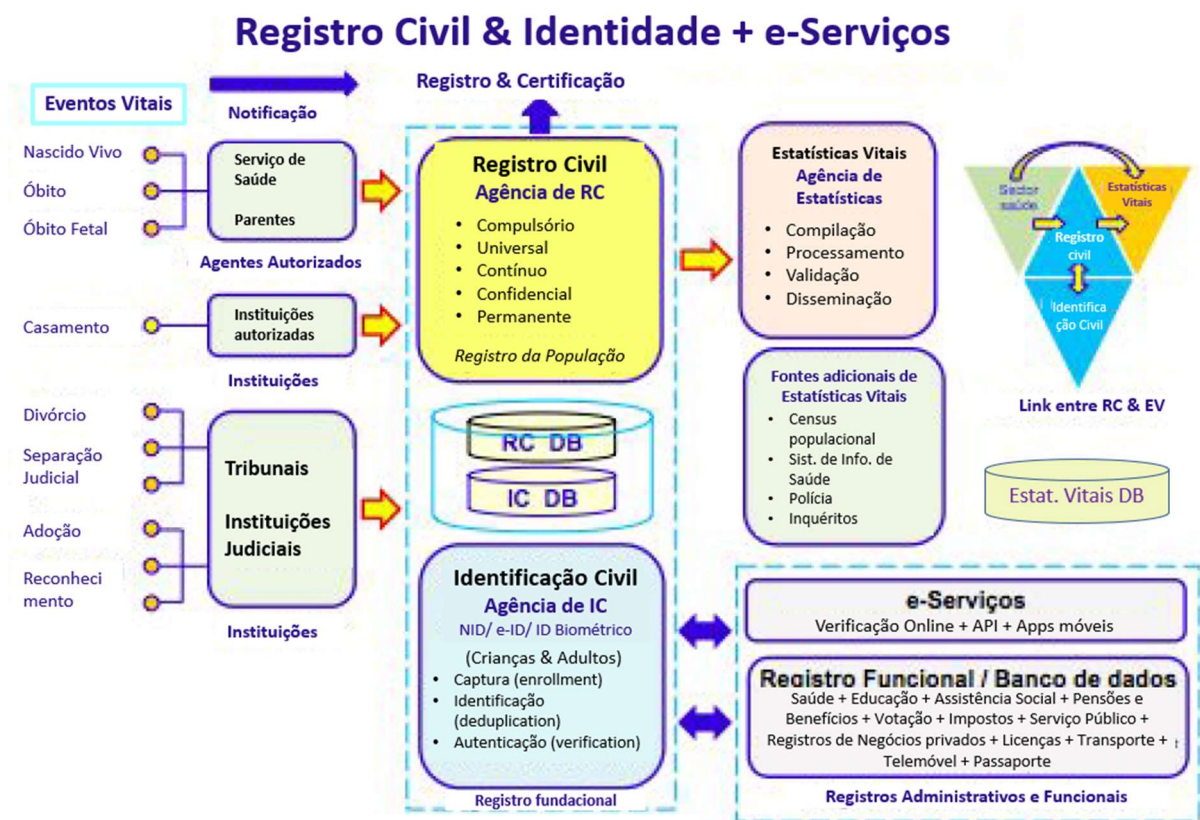
Para se estabelecer essa relação de confiança, de forma geral, sistemas de identificação procuram oferecer meios para se responder 3 perguntas: i) quem é você? (identificação); ii) você é quem diz ser? (autenticação); iii) você está autorizado ou é elegível para um serviço ou direito? (autorização). Normalmente, as duas primeiras perguntas fazem parte do escopo de sistemas de identidade fundacionais, enquanto sistemas funcionais se preocupam mais com a terceira. Para isso, esses sistemas coletam e validam atributos de alguém para estabelecer a identidade da pessoa e, então, emitem uma credencial (ex: número único de identificação, cartão, certificado, ID móvel), que poderá ser usada para comprovar a identidade. (BANCO MUNDIAL, 2019)

É importante fazer a distinção entre esses dois tipos de identidade (fundacional e funcional). A identidade funcional tem como objetivo servir uma função específica, num determinado setor, de forma que o cidadão possa ter seu acesso a certo serviço ou direito autorizado ou não (ex.: título de eleitor, carteira de motorista, cartão de saúde). A identidade fundacional, em contrapartida, procura garantir apenas que um

indivíduo é quem ele afirmar ser, sem conectá-lo a um serviço específico. Tipicamente, a identidade fundacional é uma abordagem integrada de registro civil e identificação civil e é a que é considerada como identidade legal. Essa distinção é importante, pois os diferentes sistemas de identificação têm características, funcionalidades e riscos diferentes, conforme o setor em que é usado. (BARBOSA et al., 2020)

Registro civil e identificação civil também são conceitos diferentes. Segundo Machado (2015), o registro civil contém os dados biográficos de um indivíduo, onde são registrados de forma contínua e permanente informações sobre a sua vida, enquanto a identidade civil possui as suas informações biométricas. No Brasil, há ainda os cadastros administrativos, como CPF (Cadastro de Pessoa Física), NIS (Número de Identificação Social) e CadSUS, entre outros. Estes, porém, não são considerados identidades legais, apenas registros administrativos. A Figura 1 ilustra a relação entre esses conceitos.

Figura 1 - Registro e Identificação Cíveis e Identidade Funcional

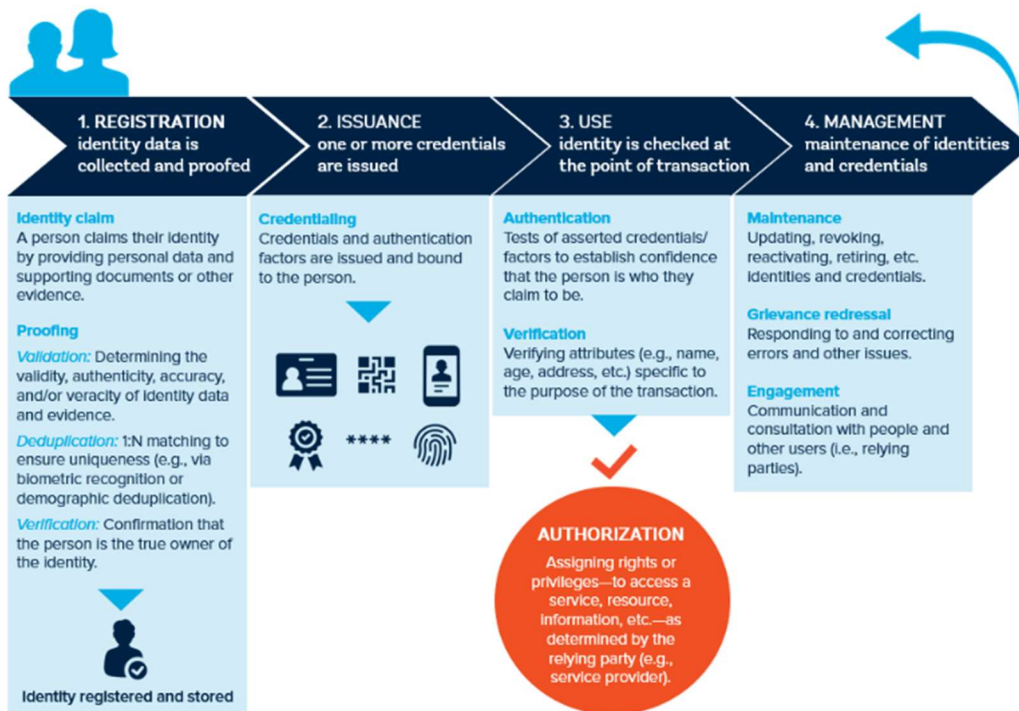


Fonte: Machado, 2020

O processo de estabelecer a identidade de uma pessoa e depois usá-la em transações no dia a dia envolve vários estágios, que podem ser compreendidos como o “ciclo de vida da identidade” e estão representados na Figura 2. (BANCO MUNDIAL, 2019)

Além disso, conforme Banco Mundial (2019), múltiplos atores são envolvidos ao longo do ciclo de vida das identidades emitidas e reconhecidas pelo Estado, seja para estabelecê-las, mantê-las ou mesmo somente usá-las. Tipicamente, os principais atores podem ser agrupados em papéis conforme o Quadro 1.

Figura 2 - Ciclo de Vida da Identidade



Fonte: Banco Mundial, 2019

Quadro 1 - Papéis e Atores envolvidos nos sistemas de identidade

Papel	Atores	Atividades Principais
Usuário Final (sujeitos do sistema de identidade)	Pessoas (ex.: cidadãos, beneficiários de programas, clientes de empresas)	<ul style="list-style-type: none"> • Registrar-se em sistema de identificação • Usar credenciais para comprovar identidade e ter acesso a direitos e serviços • Atualizar e controlar uso de dados pessoais

Provedores de Identidade (emissores e gestores de identidades)	Agências de Governo (ex.: autoridade de registro civil, Ministério da Saúde, da Cidadania) Empresas (ex.: operadoras de telefonia, provedores de serviços financeiros, de saúde, agências de classificação de crédito)	<ul style="list-style-type: none"> • Registrar pessoas nos sistemas de identificação • Emitir e gerir credenciais • Gerenciar e atualizar informações das identidades • Prover serviços de autenticação e verificação com diferentes níveis de confiabilidade • Tratar queixas de usuários
Partes Dependentes (“ <i>Relying Parties</i> ”)	Agências de Governo (ex.: órgãos de assistência social) Empresas (ex.: provedores de serviços)	<ul style="list-style-type: none"> • Usar os serviços dos provedores de identidade para autenticar e/ou verificar a identidade dos usuários • Autorizar o acesso de pessoas a direitos e serviços
Habilitadores (suportam desenvolvimento, implementação e supervisão de sistemas de identificação)	Entidades Reguladoras Entidades Padronizadoras Parceiros Locais e de Desenvolvimento	<ul style="list-style-type: none"> • Promulgar e fiscalizar regulamentações • Promover padrões técnicos e de segurança da informação • Fornecer financiamento e assistência técnica para a construção de sistemas de ID

Fonte: adaptado de Banco Mundial, 2019

É possível classificar como digital a identidade que usa tecnologia ao longo do seu ciclo de vida, seja para capturar e armazenar eletronicamente os atributos exclusivos de cada pessoa ou fornecer um método online de comprovação de identidade (BANCO MUNDIAL, 2019). Com isso, muitos documentos de identidade tradicionais, baseados em papel, foram simplesmente digitalizados e disponibilizados num formato de aplicativos de celular. Porém, a transformação digital da sociedade vem desafiando os paradigmas estabelecidos e instigando uma nova forma de pensar as relações entre as pessoas e as instituições. É possível, então, se ter uma visão mais sistêmica, integrada, e pode-se considerar “ID digital como um mecanismo técnico para identificação digital e segura de indivíduos, em que não há contato pessoal, ao mesmo tempo em que mantém as características desejáveis da identificação civil: inclusiva, acessível, portátil e persistente”. (Barbosa et al., 2020)

Ser inclusiva e acessível significa não deixar cidadão algum para trás. Segundo Barbosa et al. (2020), a identidade é um direito em si e “está intrinsecamente ligada ao direito à nacionalidade e ao reconhecimento em todo lugar do indivíduo perante a lei”. Portanto, todos que desejarem ter uma identidade, devem ter acesso aos meios para obtê-la. E isso requer atenção especial a grupos marginalizados e vulneráveis, como a população em situação de rua e aqueles potencialmente sujeitos a perseguição cultural, política ou ideológica, por exemplo. Igualmente importante, é garantir que não haja discriminação no uso da identidade. A pessoa ou sistema de informática que

precisar verificar a identidade de alguém para autorizar acesso a um serviço ou direito deve receber somente as informações que necessitar para tal atividade. De acordo com Banco Mundial (2019), é preciso cuidar também para que o custo da identidade e a exclusão digital não sejam obstáculos para os cidadãos que precisam dela.

Além disso, ser portátil implica estar disponível e poder ser utilizada onde quer que o usuário esteja e a partir de múltiplas credenciais (ex: aplicativo de celular, cartão inteligente, cédula de papel). Já a identificação ser persistente implica ela não mudar e acompanhar o indivíduo ao longo de toda a sua vida. (ID2020, 2020)

Em adição a essas características essenciais de uma identidade digital, é importante observar alguns princípios norteadores para a construção de um sistema de identificação que seja confiável e sustentável no longo prazo. A comunidade internacional tem se engajado no estudo e proposição de princípios direcionadores para o que consideram ser uma “boa” identidade digital (“*Good ID*”). Tais princípios serão abordados no item 3.3. Princípios para uma boa identidade digital. (BANCO MUNDIAL, 2019)

Por fim, sistemas de identificação (digitais ou não) podem ainda ser classificados, de um modo geral, conforme os seguintes tipos de arranjos:

Quadro 2 - Arranjos possíveis para os sistemas de identificação

Arranjo	Centralizado	Federado	Descentralizado
Definição	Uma única organização estabelece e gerencia a identidade	Diferentes organizações, cada uma com seu próprio sistema de identificação, estabelecem uma relação de confiança entre si para um aceitar o documento de identidade emitido pelo outro	Múltiplas entidades contribuem para um sistema de identificação sem um controle central; usuários controlam o compartilhamento dos dados de identidade
Exemplos	Título de Eleitor (Brasil) e Carteira de Identidade – Aadhaar (Índia)	GOV.UK Verify (Reino Unido), Itsme (Bélgica), NemID (Dinamarca), Carteira de Identidade – RG (Brasil)	Governo de Malta (piloto)

Fonte: adaptado de Banco Mundial, 2019

É importante observar que não há uma forma de organização padrão ou mais indicada. A escolha por um arranjo ou outro depende do contexto de cada país e pode, inclusive, envolver a participação do setor privado de diversas formas. O setor público não precisa, por exemplo, desempenhar o papel de provedor da identidade digital, fornecendo o serviço diretamente à população, apesar de possuir papel fundamental

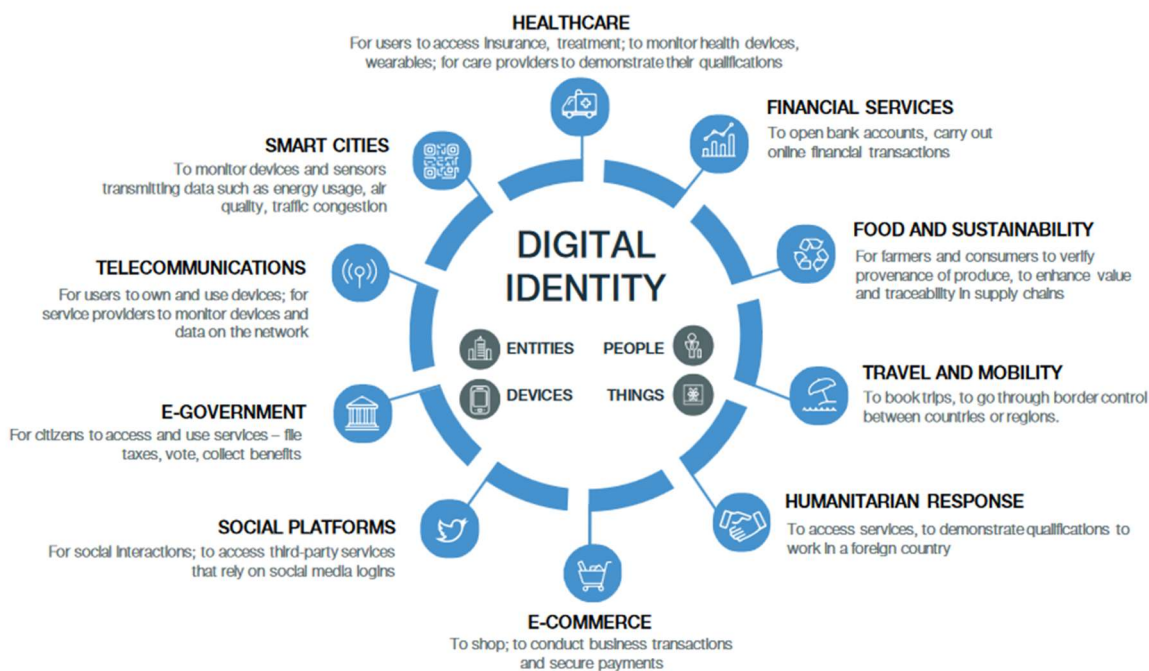
na estruturação da estratégia de identificação e na regulamentação do ambiente em que ela será fornecida.

3.2. O impacto da identidade digital e o cenário internacional

De acordo com o estudo de MCKINSEY GLOBAL INSTITUTE (2019), “cerca de 1 bilhão de pessoas no mundo não possuem qualquer identificação legal reconhecida; 3.4 bilhões de pessoas possuem alguma forma de identificação legal, mas encontram restrições para usá-la no mundo digital; e os outros 3.2 bilhões, possuem identidade legal reconhecida e participam da economia digital, mas podem não conseguir tirar todo o proveito dela online”. Nesse cenário, a identidade digital é vista como uma ferramenta em potencial para liberar a criação de valor econômico, pois pode possibilitar maior inclusão desses grupos, aumento da formalização nas relações – o que ajuda a reduzir fraudes e proteger direitos – e a digitalização de serviços – o que pode promover aumento de eficiência e facilidade de uso. Ainda segundo o estudo, os países analisados podem conseguir liberar entre 3% e 13% de seus PIB em 2030, considerando altos índices de adoção de uma identidade digital.

Além disso, segundo o Banco Mundial (2019), “uma boa implementação de identidade digital (*‘Good ID’* – inclusiva e confiável) é crucial para se atingir um desenvolvimento sustentável” e, por isso, “garantir que todos tenham acesso a identificação é um objetivo explícito nos Objetivos para Desenvolvimento Sustentável da ONU - ODS (16.9 – prover identidade legal para todos, incluindo registro de nascimento)”. Ainda segundo o estudo, a identidade digital pode ajudar a atingir outros ODS, como os relacionados à inclusão financeira, igualdade de gênero e acesso à saúde e educação básicas. A Figura 3 ilustra alguns dos potenciais impactos da ID.

Figura 3 - Potenciais Impactos da Identidade Digital



Fonte: WORLD ECONOMIC FORUM, 2018

A partir de experiências positivas de países como Estônia, Índia, Dinamarca e Uruguai na implementação de sistemas de identidade digital e do patrocínio de órgãos internacionais, como Banco Mundial, OCDE e BID, o tema vem se consolidando cada vez mais na agenda internacional e cada vez mais países o incorporam nas suas estratégias de transformação digital, incluindo o Brasil.

Não há uma solução de identidade digital que sirva para todo mundo. O desenho de um sistema de identificação precisa levar em consideração o contexto de cada país para se chegar no modelo mais adequado. No entanto, iniciativas internacionais, como o *“Identity for Development”* (ID4D) do Banco Mundial e o movimento *“Good ID”*, uma coalizão multissetorial, vem contribuindo para o debate público com análises dos potenciais riscos, oportunidades, princípios norteadores e *frameworks* para ajudar a construir o que vem sendo entendido como uma “boa” identidade (*“Good ID”*). Dentre os princípios de uma *“Good ID”*, pode-se citar ser inclusiva, centrada no cidadão, segura e protetora da privacidade. São esses princípios e *frameworks* que nortearão a análise da iniciativa brasileira.

3.3. Princípios para uma boa identidade digital

Uma boa identidade digital é, primordialmente, aquela capaz de entregar valor para pessoas, governos e empresas. E para isso, organizações internacionais recomendam se atentar a uma série de princípios orientadores ainda no início do desenho de uma política de identificação.

A política deve ser **inclusiva** e garantir cobertura universal a todos os indivíduos, do nascimento à morte, e ser livre de qualquer discriminação. Como exposto por Barbosa et al (2020), ela deve permitir “que todos os indivíduos participem plenamente da sociedade e economia em que vivem”. E não deve ser usada como uma ferramenta para segregar, perseguir ou infringir qualquer direito individual ou coletivo. (BANCO MUNDIAL, 2019)

A identidade deve ser **acessível** também. É importante cuidar para que não haja barreiras no acesso ou uso da identidade digital. Tais barreiras podem estar associadas às taxas de emissão da identidade ou aos custos para se deslocar até o local da emissão, por exemplo. O nível de acesso à infraestrutura tecnológica (ex.: celulares e internet) e o analfabetismo digital também são pontos de atenção para garantir o acesso do maior número de pessoas possível. Por isso, é importante que o usuário sempre possua alternativas para obter e conseguir usar o mecanismo de identificação onde quer que ele esteja, o que remete ao terceiro princípio: ser centrada no usuário. (BANCO MUNDIAL, 2019)

Ser **centrada no usuário** implica ser flexível o suficiente para atender às suas necessidades e garantir que ele possua a melhor e mais fluída experiência possível quando precisar comprovar a sua identidade. Indo além, a identidade digital deve empoderar os indivíduos, garantindo **privacidade e segurança** e eles devem sempre **estar no controle do seu uso**, conforme GoodID (2020). Isso significa que ao ter a sua identidade solicitada, a pessoa ou sistema solicitante não obterá mais informações do que o estritamente necessário e só o fará mediante autorização do usuário. Ser **transparente** é também um ponto central de um bom mecanismo de identidade digital e o cidadão deve ser capaz de monitorar quem acessou os seus dados pessoais e revogar o acesso automático, se assim desejar.

Um bom sistema de identificação digital precisa ser **confiável**. Para isso, ele deve conseguir garantir a identificação inequívoca dos indivíduos e possuir uma infraestrutura tecnológica **robusta**, que garanta a escalabilidade da solução, para que os usuários não deixem de ser atendidos quando mais precisarem e que proteja os seus dados pessoais contra ataques cibernéticos. É importante também que os mecanismos de identificação sejam **interoperáveis** e a identidade possa ser reconhecida por diferentes entidades dentro e fora das fronteiras do país. O sistema também deve ser financeiramente e operacionalmente **sustentável**. Para tal, é importante procurar usar padrões abertos e cuidar para que não haja dependência de uma tecnologia ou fornecedor específico – o que, no longo prazo, pode elevar os custos do sistema de identificação. (BANCO MUNDIAL, 2019)

Para se garantir a confiabilidade do sistema de identificação, há aspectos de governança que precisam ser observados também. Privacidade, segurança e direitos do usuário devem ser garantidos por **instrumentos regulatórios e legais** compreensivos, cujo cumprimento deve ser **supervisionado por autoridades independentes**. (BANCO MUNDIAL, 2019)

3.4. *Frameworks* de análise

Um sistema de identidade digital deve ser projetado conforme as necessidades e contexto de um país. E para garantir que ele atenda aos objetivos pretendidos, é importante fazer o adequado diagnóstico da situação atual, identificando as forças, fraquezas, restrições e oportunidades existentes nos mecanismos de identificação atuais, e, então, definir a visão de onde se quer chegar. De modo geral, os *frameworks* de análise elaborados pelos órgãos internacionais estruturam tanto o diagnóstico, quanto o projeto da política desejada em três eixos: modelos de solução, estruturas de governança e instrumentos legais e de regulação.

De acordo com Banco Mundial (2019), o diagnóstico da situação atual inicia-se com o mapeamento do ecossistema de identificação vigente e com a identificação das partes interessadas. Em seguida, avalia-se a cobertura, as lacunas e a confiabilidade

dos sistemas existentes e, posteriormente, os instrumentos legais e regulatórios em vigor.

Os passos que sucedem o diagnóstico, conforme Banco Mundial (2019), são a definição de uma visão compartilhada de identidade digital e a identificação dos potenciais usuários (atuais e futuros), o que ajudará a garantir que a ID seja projetada vinculada a um propósito específico. A Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2019) também avalia o que pode ser usado para alavancar a política e a adoção da identidade digital, como serviços públicos e privados potencialmente impactados pela ID e os modelos de financiamento.

3.5. Riscos das abordagens de identidade digital

De acordo com Banco Mundial (2019), um sistema de identificação mal desenhado pode não só não resolver problemas existentes de exclusão social, econômica e cultural. A possibilidade do acesso a um serviço por canais digitais, por exemplo, pode agravar a situação de grupos já marginalizados, que não possuem acesso à infraestrutura tecnológica ou têm algum nível de analfabetismo digital. Mesmo que haja a alternativa por meios tradicionais, o aumento da eficiência pelos meios digitais pode ser suficiente para aumentar a desigualdade entre as classes sociais.

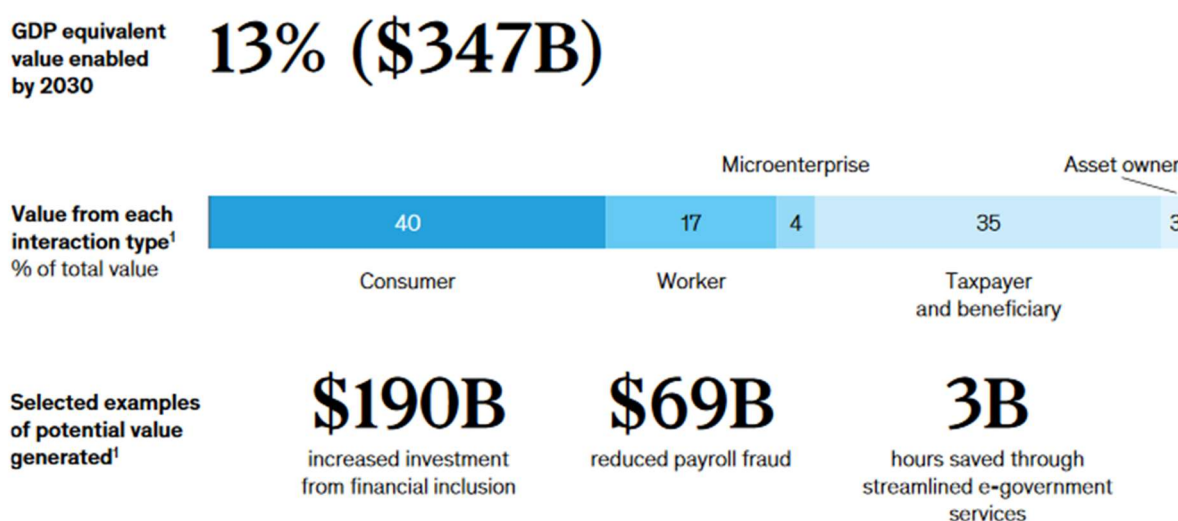
Há o risco também de violação da privacidade e da segurança. O armazenamento de dados sensíveis (ex: informações biométricas, como impressões digitais, dados de reconhecimento facial ou de íris) em uma base de dados centralizada, por exemplo, cria um ponto único de falha. E uma vez que esses dados sejam vazados, as pessoas podem ser expostas a fraudes de identidade difíceis de serem revertidas. O armazenamento de dados pessoais não imprescindíveis para o fornecimento de determinados serviços pode ser um problema também. Em países com uma tradição ditatorial, particularmente, corre-se maior risco de subversão dos objetivos do sistema de identificação, que pode acabar sendo usado para fins de vigilância e perseguição. (BANCO MUNDIAL, 2019)

Ainda conforme Banco Mundial (2019), há riscos relacionados à dependência de tecnologias e fornecedores específicos, o que tende a aumentar os custos ao longo do tempo e restringir a flexibilidade do sistema de identificação, para melhor atender às necessidades específicas do país. Instrumentos inadequados para compras públicas e viabilização de boas parcerias também apresentam riscos, pois podem levar a uma empreitada que fique apenas no papel ou que seja má implementada e não consiga estabelecer um nível de confiança necessário para se garantir a adesão das pessoas.

4. O PANORAMA BRASILEIRO

A identidade digital única faz parte da Estratégia de Governo Digital 2020-2022 do Governo Federal e, sob o eixo “Governo Confiável”, o governo espera emitir aos cidadãos 40 milhões de identidades digitais até 2022. A expectativa com o avanço do trabalho nessa frente é poder capturar, ao menos em parte, os resultados projetados pelo estudo de MCKINSEY GLOBAL INSTITUTE (2019), que estima o potencial econômico que poderia ser habilitado pela ID digital em 2030. (GOVERNO DO BRASIL, 2020)

Figura 4 - Potencial Econômico Viabilizado pela ID Digital



Fonte: MCKINSEY GLOBAL INSTITUTE, 2019

O comprometimento do Brasil com a Agenda 2030 da ONU, em especial com o 16.9 – “Prover identidade legal para todos, incluindo registro de nascimento”, aliado

a questões já enfrentadas pelo país, como o combate a fraudes, ajudou a consolidar na agenda brasileira uma política que ganhou destaque no cenário internacional nos últimos anos: a identidade digital única.

Porém, antes de se debruçar sobre o modelo que está sendo planejado e implementado pelo governo, é importante entender como está o ecossistema de identificação brasileiro, quais são as suas limitações, seus principais marcos regulatórios e os atores que fazem parte dele.

4.1. Histórico de iniciativas de identidade nacional

Um dos principais documentos de identidade do brasileiro é a carteira de identidade (RG), que serve de base para que o cidadão possa comprovar sua identidade e acessar diversos serviços públicos e privados, incluindo a emissão de outros documentos de identificação. Segundo Doneda et al (2016), o RG é emitido pela Secretaria de Segurança Pública de cada estado e, por não haver um sistema de cadastro centralizado ou comunicação adequada entre esses órgãos, a sociedade fica mais exposta a casos de fraude. Uma pessoa pode, por exemplo, emitir uma carteira de identidade diferente em cada estado (talvez, até com dados falsos) e tentar obter acesso ao mesmo serviço público mais de uma vez.

A preocupação para prevenir fraudes relacionadas à identificação não é nova e o executivo federal, há mais de duas décadas, busca uma forma de unificar as suas bases de dados. Em adição, conforme OCDE (2018), “a digitalização das interações entre o setor público e os seus cidadãos fez com que o Brasil aumentasse os seus esforços para desenvolver um sistema de identificação digital”. Nesse sentido, em 1997, foi proposto o Registro de Identidade Civil (RIC), que culminou na Lei nº 9.454 de 07 de abril de 1997. O seu principal objetivo era a institucionalização de um novo documento de identidade civil mais moderno e que instrumentasse melhor o estado para combater fraudes. Doneda et al (2016) explica que:

O RIC faria convergir vários documentos, como: a carteira de identidade (RG), a carteira de habilitação (CNH), o cadastro da pessoa física (CPF), o título de eleitor, a carteira de trabalho (CTPS), o cadastro do indivíduo no PIS/PASEP, e o número de registro do INSS.

Porém, somente após 13 anos a referida lei foi regulamentada, com o Decreto nº 7.166 de 05 de maio de 2010, que criou o Sistema Nacional de Registro de Identificação Civil – SINRIC e o seu Comitê Gestor, tendo como órgão central o Ministério da Justiça, mas contendo representantes de outros órgãos da União e dos entes federados. O decreto, no entanto, enfrentou críticas como a desproporcionalidade na composição do Comitê Gestor entre União e suas unidades federativas. Segundo Lopes (2010), por exemplo, os estados não conseguiriam influenciar na decisão dos seus interesses, por serem minoria, e o Governo Federal passaria a se apropriar de um serviço que não lhe incumbia. Além disso, Doneda et al (2016) aponta que o sistema proposto (SINRIC) implicaria uma mudança na “distribuição de poder entre indivíduo e Estado (bem como certas entidades privadas) em relação ao controle efetivo de seus próprios dados pessoais”.

O RIC até chegou a ser testado em um projeto piloto, mas, segundo Brasil (2020a), a necessidade de aperfeiçoamento em questões técnicas, levou o Ministério da Justiça a firmar um termo de cooperação técnica com a Fundação Universidade de Brasília (FUB) para estudar a reestruturação do projeto e a sua viabilização. O RIC, entretanto, nunca foi implementado e as razões para tal não são claras. Doneda et al (2016) diz que “ao que parece, as razões para isso foram os altos custos que estariam envolvidos em sua eventual implementação”.

A necessidade de possibilitar um relacionamento mais simples e seguro entre cidadão e órgãos públicos e privados permanecia latente. Em 2015, então, um projeto de lei (PL 1775/2015) foi enviado para o Congresso Nacional propondo a criação do Registro Civil Nacional (RCN) e do Documento Nacional de Identificação (DNI). A intenção do projeto era integrar as bases de dados da Justiça Eleitoral, que desde 2008 já vinha identificando biometricamente o eleitorado brasileiro e construindo uma base de dados com registros individualizados dos cidadãos, e a base de dados do Sistema Nacional de Informações de Registro Civil – SIRC, além de outras informações não contidas no SIRC, mas pertencentes a bases da Justiça Eleitoral ou fornecidas por outros órgãos.

O PL 1775/2015 foi aprovado e convertido na Lei nº 13.444, de 11 de maio de 2017, mudando o nome de RCN para Identificação Civil Nacional (ICN) e suscitando alguns pontos de atenção importantes em relação à política de identificação brasileira. O primeiro ponto refere-se à falta de delimitação dos dados que podem compor a base

da ICN e a agregação deles num único lugar. De acordo com, Doneda *et al* (2016), “essa agregação em massa dos dados não só atinge o princípio da finalidade, mas também traz um maior risco de cyber-ataques e uso indevido ou ilegítimo do banco de dados”.

O segundo ponto de atenção é a extensão do compartilhamento da base do ICN - que pode ser compartilhada com outros órgãos do Executivo ou Legislativo da União, Estados e Municípios - e a falta de diretrizes para esse compartilhamento e previsão de regulamentação posterior. O último ponto de atenção está relacionado à participação social na aprovação da lei. Apesar de terem sido realizadas audiências públicas, a sociedade civil praticamente não se envolveu nelas, algo de extrema importância, dado que estava ficando mais evidente o dilema entre garantir a privacidade, proteger os dados pessoais e garantir a segurança pública e prevenir fraudes.

Um ponto importante sobre o DNI é que apesar de ele ter sido criado na lei supracitada, ele ainda não foi disponibilizado para toda a população. O Decreto nº 9.278, de 5 de fevereiro de 2018, que regulamenta a expedição das carteiras de identidade, prorrogou para 1º de março de 2021 o prazo para que os órgãos de identificação adotem os padrões do novo documento. De acordo com DNI (2020), somente 9 estados aderiram ao formato do Documento Nacional de Identificação para emissão de suas Carteiras de Identidade.

4.2. Há algum documento de identidade digital disponível para os brasileiros?

Ao longo dos últimos anos, muitos dos documentos com credenciais físicas tiveram suas versões digitais criadas no formato de aplicativos de celular. São exemplos o título de eleitor, a Carteira Nacional de Habilitação e Carteiras de Identidade emitidas por alguns estados. Até mesmo o DNI seria disponibilizado nesse formato. Porém, eles se mostraram meras digitalizações dos documentos físicos e não se enquadram na definição de identidade digital utilizada por esse trabalho, pois ainda demandam interação humana (face a face) para autorizar o acesso das pessoas a serviços.

Quando se procura um mecanismo capaz de comprovar a identidade de um brasileiro sem a necessidade de uma outra pessoa verificando a sua credencial, talvez o que mais se aproxima do conceito de identidade digital adotado por este trabalho seja o certificado digital ICP-Brasil.

De acordo com o Mapa da Informação (ITS Rio, 2018),

“O certificado digital ICP-Brasil funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora - AC que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. O certificado digital da ICP-Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados com o seu uso”.

A Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil) foi criada em 2001 e é mantida e auditada pelo Instituto Nacional de Tecnologia da Informação (ITI), que deve seguir as regras e políticas estabelecidas pelo Comitê Gestor da ICP-Brasil, composto por membros dos poderes públicos, sociedade civil e academia. Essa é uma infraestrutura tecnicamente muito robusta, que confere ao sistema de identificação elevado grau de confiabilidade. Ela compõe a base para que duas ou mais partes (pessoas ou sistemas de informática) que não se conhecem e não se veem nas redes de computadores em âmbito nacional possam estabelecer uma relação de confiança e realizar uma transação de interesse de ambos.

Desde a sua criação, a ICP-Brasil se consolidou como base para a comunicação entre sistemas de informática, mas não conseguiu obter o mesmo desempenho para a comunicação online entre pessoas. De acordo com Lemos (2020), somente 2% da população brasileira possui acesso atualmente aos certificados digitais. Uma das causas para isso é possivelmente o elevado custo para se adquirir um deles (entre R\$100,00 e R\$400, variando conforme o tipo e validade –

1 a 3 anos¹) em uma das autoridades de registro (entidades privadas) credenciadas à cadeia de confiança da ICP-Brasil.

Esses certificados digitais atualmente são comercializados em diversos formatos. Eles podem ser armazenados em uma mídia criptográfica, como cartões inteligentes ou token (assemelha-se a um pen drive e usa a porta usb dos dispositivos eletrônicos), em computadores, celulares ou até na nuvem. Entretanto, muitas vezes eles demandam uma certa familiaridade com tecnologia para poderem ser usados adequadamente no dia a dia, restringindo-se a um nicho de pessoas. Além disso, eles, por si só, não eliminam a necessidade das pessoas de portar outras credenciais para confirmação de identidade presencial (face a face), como o documento físico ou aplicativo de celular da Carteira Nacional de Habilitação (CNH). Isso faz com que as pessoas precisem carregar consigo mais de um item diferente para poder comprovar a sua identidade em situações diferentes. Esses certificados, portanto, não estão tão aderentes ao conceito e princípios de uma boa ID, adotados por esse trabalho.

É importante mencionar também que em recente iniciativa, o Governo Federal, por meio da Secretaria de Governo Digital, vem desenvolvendo uma solução para autenticação online dos brasileiros, para ser usada nos serviços públicos digitais. Essa solução, que será detalhada no item 4.5, apesar de ser eficaz para já apoiar a transformação digital do governo, não se enquadra, por si só, no conceito de identidade digital estabelecido no referencial teórico desse trabalho. Mas representa um passo importante para que o Brasil avance na construção de uma abordagem mais sistêmica e integrada para o sistema de identificação nacional.

4.3. Marcos regulatórios

Alguns marcos legais são particularmente importantes para o ecossistema de identificação e, conseqüentemente, para a ID digital, pois delimitam a construção e o uso dos sistemas de identidade. Barbosa *et al* (2020) cita que a existência das seguintes legislações precisa ser observada: i) Lei de Registro Civil; ii) Lei de Acesso

¹ Consulta realizada no sites das Autoridades Certificadoras Imprensa Oficial (<https://certificadodigital.imprensaoficial.com.br/>) e Certisign (<https://loja.certisign.com.br/Certificados/E-CPF>)

à Informação; iii) Lei de Documento Único de Identificação; iv) Iniciativa de Governo Eletrônico; v) Lei de Proteção de Dados; vi) Lei de Assinatura Digital; vii) Lei de Igualdade e Identidade de Gênero. Em adição a elas, é importante verificar a existência de legislação e regulamentação referente ao compartilhamento de dados e interoperabilidade entre os órgãos de todas as esferas públicas.

O Brasil teve avanços significativos nos últimos anos, consolidando leis e estabelecendo marcos importantes relacionados aos pontos de atenção mencionados, conforme quadro a seguir.

Quadro 3 - Marcos Regulatórios no Brasil

Marco Regulatório	
Lei de Registro Civil	Lei nº 6.015, de 31 de dezembro de 1973
Lei de Acesso à Informação	Lei nº 12.527, de 18 de novembro de 2011
Lei de Documento Único de Identificação	Lei nº 13.444, de 11 de maio de 2017 Decreto nº 9.278, de 5 de fevereiro de 2018
Governo Digital	Projeto de Lei 3443/2019 (Governo Digital) Decreto nº 10.332, de 28 de abril de 2020 (Estratégia de Governo Digital 2020 - 2022) Decreto nº 9.637, de 26 de dezembro de 2018 (Política Nacional de Segurança da Informação) Decreto nº 9.319, de 21 de março de 2018 (Sistema Nacional para Transformação Digital) Portaria nº 23, de 4 de abril de 2019 (Rede Nacional de Governo Digital – Rede Gov.Br)
Lei de Proteção de Dados	Lei nº 13.709, de 14 de agosto de 2018. (Lei Geral de Proteção de Dados)
Lei de Assinatura Digital	Lei nº 14.063, de 23 de setembro de 2020
Lei de Igualdade e Identidade de Gênero	Projeto de Lei nº 672, de 2019
Integração de bases de dados do cidadão e compartilhamento com outros entes	Decreto nº 8.936, de 19 de dezembro de 2016 (Plataforma da Cidadania Digital) Decreto nº 10.046, de 9 de outubro de 2019 (Cadastro Base do Cidadão)

Fonte: Elaboração Própria

Ao mesmo tempo em que esses marcos legais ajudam a criar um ambiente mais favorável para transformação digital no governo, na qual a identidade digital desempenha papel fundamental, e criar e aperfeiçoar mecanismos de proteção dos cidadãos, eles também suscitam um debate em torno de um dilema que se forma entre aumentar eficiência do Estado e respeitar à privacidade e garantir a proteção dos dados dos cidadãos.

O Cadastro Base do Cidadão (CBC), por exemplo, foi criado com o intuito de instrumentar a administração pública para melhor formular, implementar e monitorar políticas públicas e simplificar a oferta de serviços públicos. A intenção é que ele possa funcionar como uma base integradora e que o CPF do cidadão possa ser a chave para conectar as diversas bases temáticas que fazem parte de órgãos da administração pública.

Enquanto isso, a Lei Geral de Proteção de Dados (LGPD) estabelece regras a serem seguidas por órgãos públicos e empresas sobre como deve ser feito o tratamento dos dados pessoais dos brasileiros. Segundo ela, dados pessoais somente devem ser coletados com o consentimento das pessoas, que precisam ter clareza sobre a finalidade para a qual o dado está sendo coletado.

O CBC foi instituído por meio de decreto e não pode contrariar o exposto na LGPD, o que abre espaço para questionamentos judiciais, inclusive. A implementação de uma identidade digital única deve, portanto, observar esses possíveis conflitos, cuidando para que a política pública não sofra com questionamentos que minem a confiança no sistema de identificação.

Ainda em relação ao compartilhamento de dados, é importante observar que a previsão para que ele aconteça entre os órgãos públicos consta em mais de um instrumento legal. A Lei nº 13.444, de 11 de maio de 2017 (Identificação Civil Nacional - ICN), por exemplo, prevê que o poder público forneça meios para o cruzamento de informações das bases de dados oficiais, a partir do número do CPF dos indivíduos, para que seja possível verificar a elegibilidade dele para a concessão e manutenção de benefícios sociais. É importante notar que a mesma lei já estabelece diretrizes para como o compartilhamento deve acontecer. Além do uso do CPF, ela também estabelece requisitos adicionais para a troca de informações entre a base de dados da ICN e outras bases e sistemas governamentais, como o respeito às recomendações técnicas da arquitetura dos Padrões de Interoperabilidade de Governo Eletrônico (e-Ping).

Em adição, o Decreto nº 9.278, de 5 de fevereiro de 2018, que regulamenta a expedição das Carteiras de Identidade pelos órgãos de identificação dos estados, prevê que na emissão delas seja verificada a base de dados da ICN para garantir conformidade com o DNI e que o CPF seja adicionado às Carteira de Identidade, por

padrão e sempre que o órgão emissor possuir acesso à base de dados da Receita Federal.

O direcionamento para que haja compartilhamento de dados entre os órgãos de identificação e a utilização do CPF como chave para identificar os indivíduos nos cruzamentos das bases são marcos importantes para o ecossistema de identificação, pois contribuem para que ele possa ser mais seguro, facilitando o processo de remoção de duplicidade dos registros das pessoas, mas ao mesmo tempo podem suscitar questões relacionadas à privacidade, como exposto anteriormente.

Por fim, um outro marco importante que vale ser mencionado é a instituição da Rede Gov.Br, feita pela Portaria nº 23, de 4 de abril de 2019. De acordo com Brasil (2020e), a Rede Gov.Br “tem como finalidade promover a colaboração, o intercâmbio, a articulação e a criação de iniciativas inovadoras relacionadas a temática de Governo Digital no setor público”. Podem aderir a ela Estados e Municípios, os quais devem se comprometer com algumas diretrizes do Governo Federal sobre a oferta de serviços públicos digitais (Decreto nº 8.936, de 19 de dezembro de 2016) e a simplificação do atendimento prestado aos usuários dos serviços (Decreto nº 9.094, de 17 de julho de 2017). Esse é um instrumento importante, pois é através dele que Estados e Municípios poderão ter acesso facilitado à plataforma de serviços digitais do Governo Federal, incluindo o serviço de autenticação único, Conta Gov.Br.

4.4. Limitações do mecanismo de identificação atual

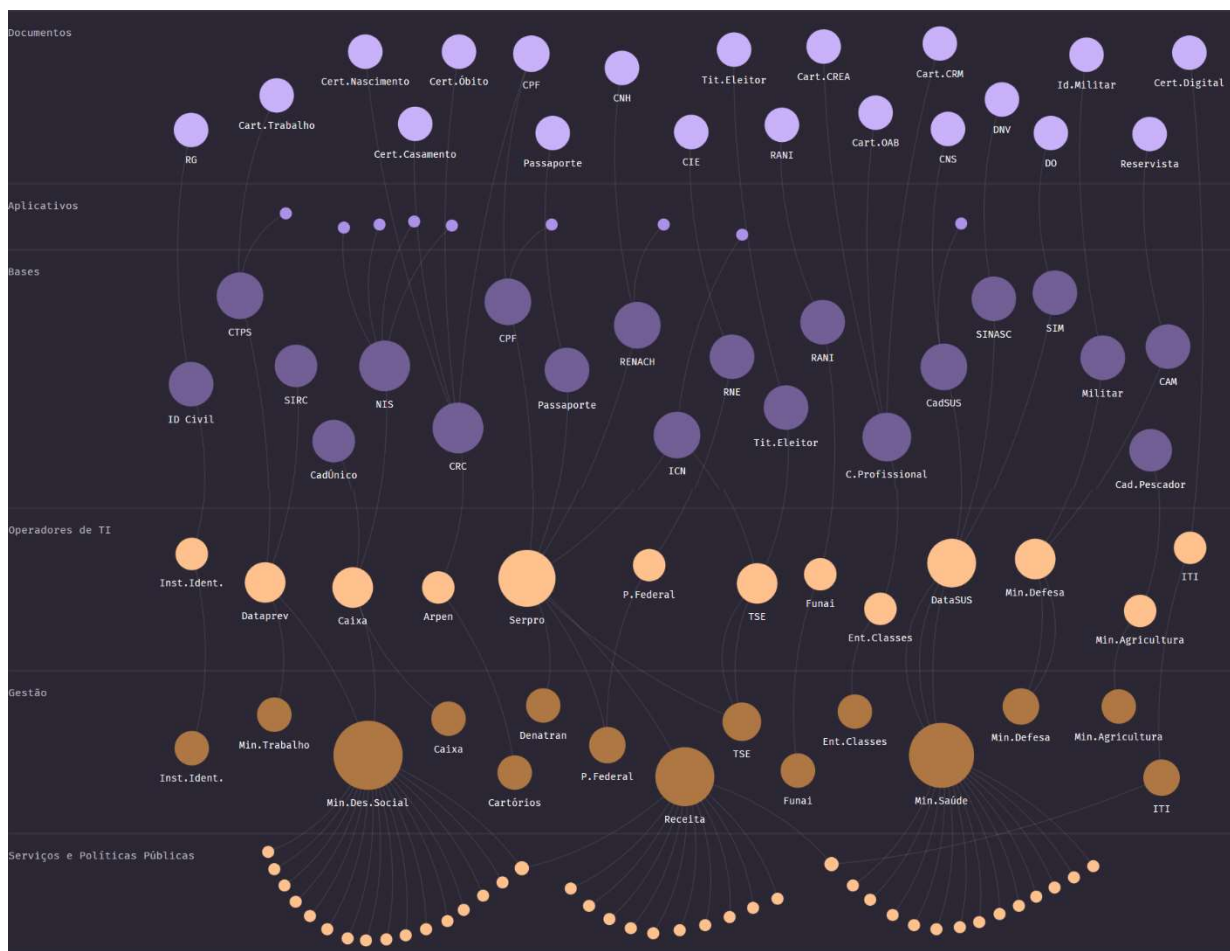
A análise do panorama brasileiro revela a complexidade do ecossistema de identificação do país. A necessidade de o cidadão possuir diversos documentos e ter que solicitar a emissão deles em diferentes órgãos, sempre tendo que passar pelo processo de se deslocar até o local da emissão, pagar taxas, informar outros documentos que comprovem a sua identidade (mesmo que as informações necessárias já constem nas bases dos governos) já suscita questionamento quanto à inclusão e acessibilidade do sistema de identificação como um todo. Se para cada serviço público ou privado, o cidadão precisa usar meios diferentes para comprovar

que ele está apto a acessá-lo, a dificuldade para se obter os documentos necessários pode se tornar um fator de exclusão social e econômica.

A existência de múltiplas bases de dados também representa um desafio para a gestão pública, que precisa, eventualmente, consolidar ou cruzar as informações dessas bases para tentar evitar fraudes nos serviços que o estado presta, por exemplo. Além disso, pode ser necessário que cada órgão solicite aos cidadãos informações que já existem em outras bases do próprio governo. Tudo isso aumenta o custo de transação para os cidadãos, que podem enfrentar lentidão para ter algum direito seu atendido ou até ficar sem acesso a serviços públicos por conta de inconsistências entre as bases. Isso traz à tona o seguinte questionamento: será que a interface do cidadão com o governo não poderia ser mais simples, menos burocrática?

A complexidade do ecossistema brasileiro de identificação pode ser observada no Mapa da Informação (Figura 5). Ele é um mapeamento em contínua construção dos documentos de identidade (funcional e fundacional) existentes no território brasileiro. Ele conta atualmente com 20 registros de documentos diferentes, identificando para cada um “o órgão gestor, os operadores de tecnologia da informação, as bases de dados, os aplicativos e os serviços e políticas relacionados”. (ITS Rio, 2018).

Figura 5 - Visão geral do Mapa da Informação



Fonte: ITS Rio, 2018

A necessidade de comprovação de identidade no mundo digital expõe ainda mais as fragilidades do sistema atual, pois para tal seria necessário arcar com um elevado custo para emitir um certificado digital ou seria necessário fornecer cópias digitais dos documentos físicos, expondo-se ao risco de os dados pessoais vazarem e serem usados de forma indevida, como em fraudes. Em adição, para se usar um certificado digital, ou mesmo digitalizar documentos, é necessário um nível mínimo de conhecimento tecnológico, o que pode excluir uma parcela da população.

As soluções de identidade disponíveis atualmente aparentam servir mais às entidades públicas e privadas, que precisam resguardar a sua atuação no fornecimento de produtos, serviços e garantia de acesso a direitos, do que aos cidadãos. Isso fica evidente também quando é posto à mesa o dilema entre privacidade e segurança e a sociedade civil não encontra espaço adequado para

participar do debate público. Com isso, os indivíduos podem acabar perdendo o controle sobre os seus próprios dados pessoais e sobre quem os obtém e utiliza.

No que tange a segurança do ecossistema de identificação atual, é importante observar que um dos documentos básicos para a emissão de diversos outros, como a carteira de identidade, pode ser emitido pela mesma pessoa em cada uma das unidades federativas, que ao não se comunicarem entre si, podem acabar emitindo documentos com informações divergentes. Nesse sentido, vale ressaltar também a baixa interoperabilidade entre as bases de dados e sistemas dos órgãos de todas as esferas.

Assim, considerando o já exposto em relação ao panorama brasileiro, é possível notar que princípios de uma boa identidade (*GoodID*) não estão sendo observados no sistema de identificação do país. A partir disso, é possível, então, idealizar a situação desejada, que poderia ser definida como “ter um sistema de identificação digital disponível para todos os brasileiros, que seja confiável, seguro, inclusivo, acessível, de fácil utilização, que seja transparente e respeite a privacidade”. E, considerando que um problema público pode ser definido pela diferença entre a situação desejada e a situação atual, ele pode ser definido, então, como a falta desse sistema de identificação digital.

4.5. A solução vislumbrada pelo Governo Federal

A fim de facilitar a identificação e a autenticação dos cidadãos nos serviços públicos digitais, o Governo Federal implantou a Conta Gov.Br. A intenção é que o cidadão possa acessar todos os serviços públicos digitais a partir de uma única credencial (ex: usuário e senha), independentemente dos órgãos que os fornecerem. Segundo Brasil (2020c), a Conta Gov.Br privilegia “a governança e a convergência autoritativa, e finalmente o controle de acesso unificado”, fornecendo ainda “um nível de segurança compatível com o grau de exigência, natureza e criticidade dos dados e das informações pertinentes ao serviço público solicitado”.

Conforme Brasil (2020d), os serviços públicos digitais podem ser categorizados em comuns (48%), sigilosos (43%) e serviços mais críticos, como os que envolvem

patrimônio (9%). E cada categoria demanda um nível de segurança (básica, verificada ou comprovada) e confiabilidade da Conta Gov.Br, que pode ser assegurada por validações em bases de outros serviços que lhe dão “selos de confiança”.

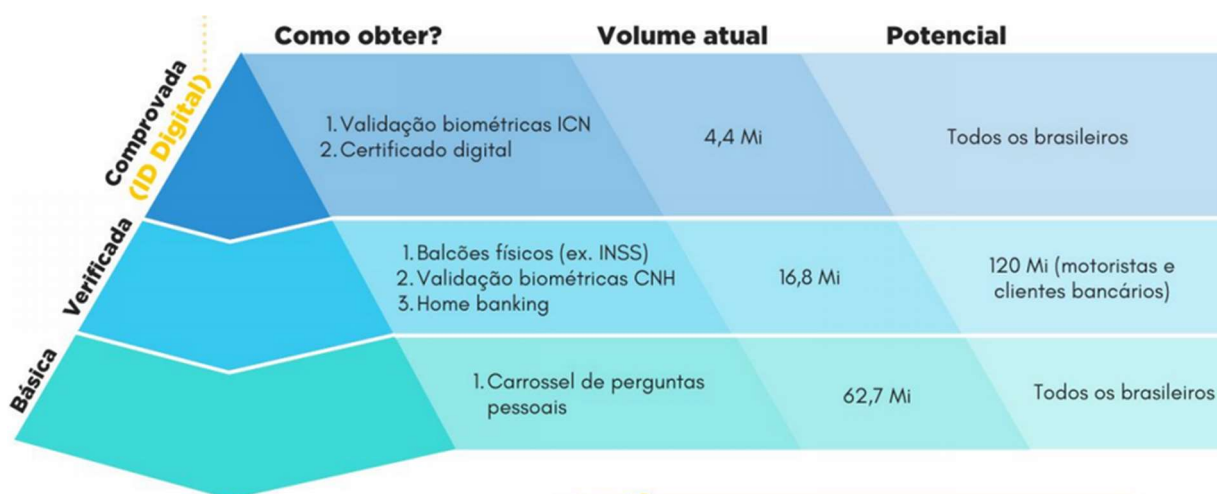
Sobre o grau de confiança de cada conta Gov.Br, Brasil (2020d) explica que:

“Os Selos de Confiabilidade estão presentes em cada nível de autenticação e consistem em orientar para qualificação das contas com a obtenção dos atributos autoritativos do cidadão a partir das bases oficiais de governo, por meio das quais permitirão a utilização da credencial de acesso em sistemas internos dos clientes e serviços providos diretamente ao cidadão”

Com essa estratégia, o governo poderia avançar na pauta de transformação digital, redesenhando diversos serviços e os integrando à plataforma de identificação online, sem precisar rever todo o sistema de identificação brasileiro. A Conta Gov.Br poderia evoluir aos poucos, agregando mais funcionalidades e mecanismos de segurança, até atingir o nível dos sistemas de identidade digital mais avançados do mundo. (BRASIL, 2020d)

A figura a seguir ilustra como é estruturado o processo de identificação na Conta Gov.Br:

Figura 6 - Processo de Identificação Digital na Conta Gov.Br



Fonte: Brasil, 2020d

Ainda de acordo com Brasil (2020d), vislumbra-se que a Conta Gov.Br se torne uma importante interface de relacionamento com serviços públicos e privados, consolidando e agregando funcionalidades como caixa postal, para notificações enviadas pelos órgãos públicos; carteira digital, armazenando documentos digitais

como e-CNH, e-Título, DNI; assinatura eletrônica (com certificados digitais ICP – Brasil, inclusive), para viabilizar a assinatura de contratos e realizar a transferência de veículos; autenticação digital, para acesso aos canais online de serviços públicos digitais; compartilhamento de dados, com os usuários tendo maior controle sobre o que compartilham e com quem, podendo revogar o compartilhamento quando lhe for conveniente; integração com serviços privados, como os serviços bancários que poderiam buscar automaticamente dados dos usuários através de APIs;

Um exemplo de como pode se dar esse compartilhamento de dados e como o cidadão pode controlá-lo é o recurso de autorização de uso de dados já existente na Conta Gov.Br, como mostra a figura a seguir:

Figura 7 - Controle de Acesso de um Serviço aos Dados Pessoais de um usuário



Autorização de uso de dados pessoais

Serviço:

Este serviço precisa utilizar as seguintes informações pessoais do seu cadastro:

- Utilizar sua identidade gov.br
- Seu nome e foto
- Seu endereço de e-mail validado no gov.br
- Seu número de telefone validado no gov.br
- Dados de Empresa do Gov.br

A partir da sua aprovação, a aplicação acima mencionada e a plataforma gov.br utilizarão as informações listadas acima, respeitando [os termos de uso e a política de privacidade](#).

Fonte: Brasil, 2020c

Por se propor a ser uma plataforma única de autenticação capaz de simplificar a vida do cidadão, a Conta Gov.Br pode ser integrada aos serviços dos Estados e Municípios que quiserem fazer uso dela. Para isso, basta que eles façam parte da Rede Gov.Br.

A Conta Gov.Br tem mostrado um crescimento importante em termos de contas ativas e de serviços conectados. Segundo Brasil (2020d), em outubro de 2020, o serviço de autenticação já contava com 80,2 milhões de contas criadas e 2.116

serviços conectados entre serviços federais, estaduais e municipais, dos quais somente 863 são federais.

É importante observar que a Conta Gov.Br não se propõe a ser, por si só, uma identidade única, substituindo (ao menos num primeiro momento) os demais documentos de identificação. Isso fica evidente quando se observa a necessidade de o cidadão já ter emitido outros documentos de identidade para, então, conseguir se registrar no serviço de autenticação do Governo Federal. O Conta Gov.Br procura ser um agregador de funcionalidades para identificação e autenticação online de usuários, construído a partir de toda a infraestrutura tecnológica do Estado brasileiro e que possa simplificar a vida do cidadão nas suas relações digitais.

5. POSSÍVEIS AVANÇOS PARA A IDENTIFICAÇÃO DIGITAL NO BRASIL

Os esforços empregados pelo Brasil nas últimas décadas, e especialmente nos últimos anos, para avançar na pauta de Governo Digital e tentar consolidar seus sistemas de identificação ajudou a criar um ambiente mais favorável para a implantação de uma identidade digital única no país, aderente ao conceito de *GoodID*, difundido por organizações internacionais.

O Brasil conta atualmente com uma legislação abrangente e marcos regulatórios importantes para o ecossistema de identificação, como os discutidos no item 4.4. (Marcos Regulatórios), têm procurado desenvolver soluções nacionais de identificação, como o DNI e a Conta Gov.Br, os quais tem como base o compartilhamento de dados do governo. Conta ainda com a articulação da Secretaria de Governo Digital (Ministério da Economia) junto às diversas partes interessadas no desenvolvimento do modelo brasileiro de ID, procurando trabalhar, inclusive, com o conceito de governo como plataforma.

O caminho para o país avançar na pauta de identidade digital, então, parece ser consolidar o trabalho que já vem sendo feito, convergindo as diferentes soluções existentes e mantendo o foco na entrega de valor para o cidadão. Com base nisso, oportunidades de melhoria e possíveis avanços serão discutidos a seguir quanto a

modelos de solução, estruturas de governança e instrumentos legais e de regulação, buscando respaldo na experiência internacional, sempre que possível.

5.1. Modelo de Solução

DNI, Conta Gov.Br, certificados digitais ICP-Brasil e Carteiras de Identidade (disponibilizadas no modelo físico ou de aplicativo de celular) se propõe a resolver o mesmo problema: comprovar que uma determinada pessoa é quem ela diz ser no mundo físico ou digital. Nenhum deles, entretanto, atende os dois cenários. E todos possuem estruturas, processos e formas de funcionar diferentes para que o cidadão possa obter a sua identidade, o que pode significar gastos desnecessários e complexidade extra tanto para o Estado, quanto para os cidadãos.

Um primeiro ponto a ser observado, então, é a possibilidade desses modelos convergirem para uma única identidade fundacional sólida, baseada na estrutura de identificação já estabelecida no país. Como a base da ICN já agrega dados biométricos e biográficos dos cidadãos e há previsão legal para que os institutos de identificação do Estados consultem tanto ela quanto a base da Receita Federal para obter e validar os dados dos cidadãos, é imprescindível consolidar a interoperabilidade entre essas bases e sistemas de informação para que ela esteja disponível a todos os órgãos emissores de identidade no momento da emissão dos documentos e, assim, a confiabilidade das informações possa ser garantida.

Como o DNI não conta com meios para comprovar a identidade de um indivíduo sem que haja a necessidade de contato humano, é interessante que a Conta Gov.Br e ele possam ser integrados para compor uma solução de identidade digital única, de forma que a existência de mais de um sistema seja transparente para o cidadão. Assim, quando uma carteira de identidade for emitida em um Estado ou pelo Tribunal Superior Eleitoral, credenciais para uso da Conta Gov.Br poderiam já ser disponibilizadas por padrão para o cidadão. Essa abordagem pode permitir, inclusive, que os cidadãos recebessem já instruções sobre como tirar proveito da identidade digital.

Além disso, certificados digitais ICP-Brasil poderiam também já ser emitidos no mesmo momento e vinculados à identidade digital dos usuários, dando a eles a possibilidade de ter ainda mais segurança nas suas interações digitais. Para isso, os próprios institutos de identificação dos Estados poderiam se credenciar como Autoridades Certificadoras (AC) junto ao ITI e emitir os certificados a custo zero ou muito baixo para os cidadãos. Outra possibilidade seria esses institutos atuarem como Autoridades de Registro (AR) e, no momento da emissão das carteiras de identidade, certificados digitais em nuvem, que são mais fáceis de se utilizar, poderiam ser gerados junto a uma AC integrada a Conta Gov.Br. Nesse caso, seria interessante até avaliar se seria possível estimular um novo modelo de negócios no mercado de certificados digitais, onde se cobraria pelo uso deles ao invés da emissão, o que poderia ajudar a popularizar a emissão dos certificados.

A convergência das soluções mencionadas para compor uma solução de identidade digital, tentando tirar proveito da infraestrutura já instalada para identificação das pessoas pode ajudar a tornar o processo de registro e emissão mais simples, eficiente e acessível. Mas para que o modelo possa ser mais inclusivo e de mais fácil utilização, é imprescindível observar as credenciais que são disponibilizadas para os usuários.

De acordo com Banco Mundial (2019), é comum países mais digitais, com maior oferta de serviços públicos e privados nesse modelo e ampla cobertura de infraestrutura de telecomunicações, adotarem um modelo onde apenas credenciais digitais (ex.: *mobile-ID*, usuários e senha) são ofertadas. É o caso do Reino Unido (*Gov.UK Verify*), Suécia e Noruega (*BankID*), que possuem uma identidade fundacional cujas credenciais são armazenadas apenas em computadores, dispositivos móveis e servidores e usam como base apenas biometria e outros fatores para autenticação das pessoas. Na Índia, credenciais digitais podem ser utilizadas, inclusive, para comprovação face a face, processo que se dá através da combinação do número único de ID (UID – *unique id number*) com o fornecimento de uma impressão digital ou de uma OTP (*one time password* – senha gerada para uma única utilização).

No caso brasileiro, entretanto, é importante garantir que as pessoas tenham acesso a múltiplas credenciais, por conta até da falta de familiaridade que pode haver com mecanismos digitais. Um exemplo disso é o que é feito na Estônia, onde são

disponibilizados cartões inteligentes com e sem os dados pessoais impressos, cartões SIM com chaves criptográficas e um aplicativo móvel para seus cidadãos (BANCO MUNDIAL, 2019). No Brasil, é importante que as pessoas sejam capazes de comprovar a sua identidade tanto online quanto offline, mitigando riscos de limitações no acesso à internet. Emitir credenciais seguras para autenticação offline, como um cartão inteligente com chaves criptográficas embutidas (nos moldes dos certificados digitais ICP-Brasil), tem um custo elevado. Mas é importante que os indivíduos possam escolher as credenciais que melhor lhe atenderão. Assim, uma abordagem integrada do DNI/ Carteira de Identidade (credenciais físicas) com a Conta Gov.Br (credenciais digitais), que também conta com um aplicativo móvel, pode ser a chave para atender um número maior de pessoas.

Ainda em relação às credenciais, um avanço possível para o modelo brasileiro é a utilização de níveis de confiabilidade para transações baseadas no método de autenticação utilizado. O Conta Gov.Br já conta com níveis de confiabilidade de contas de usuários, que podem ser usados para autorizar o cidadão a usar um serviço ou outro, dependendo do nível que a sua conta possuir. Esse mesmo conceito pode ser utilizado para liberar acesso a um determinado serviço, de acordo com o método de autenticação utilizado para uma certa operação. Por exemplo, para consultar o andamento do processamento da restituição do imposto de renda, o cidadão poderia entrar na Conta Gov.Br usando somente o usuário e senha. Mas para poder enviar a declaração do imposto para a Receita Federal, ele precisaria utilizar um método de autenticação multi-fator, que poderia levar em conta algo que a pessoa sabe (ex.: usuário e senha), algo que ela possua (ex.: celular) e algo que ela seja (ex.: validação facial). Isso poderia colocar o modelo brasileiro de ID em linha com padrões internacionais, como a norma ISO/IEC 29115, e com que vem sendo praticado, por exemplo, nos Estados Unidos, que segue a norma NIST 800-630-3 definida pelo *US National Institute of Standards and Technology* (NIST). (BANCO MUNDIAL, 2019)

Um ponto importante a ser observado no modelo brasileiro é o direcionamento para a utilização do CPF como identificador único dos indivíduos, tanto nas bases de dados governamentais, quanto em credenciais, como para se autenticar na Conta Gov.Br. Essa prática levanta algumas questões quanto a garantia da privacidade dos usuários. Se o identificador único é utilizado para autenticar os usuários nos mais diversos tipos de serviços (públicos e privados), é possível que ele seja utilizado para

construir um perfil de uso deles também. Além disso, a utilização desse identificador para individualizar os registros dos cidadãos nas bases de governo representa um risco para a exposição indevida das pessoas, especialmente nos casos de vazamento de dados pessoais sensíveis de bases temáticas do governo (ex.: dados de saúde). (BANCO MUNDIAL, 2019)

Para lidar com esse tipo situação, é importante trabalhar com o conceito de *Privacy by Design*, onde técnicas para garantir a privacidade dos cidadãos podem ser incorporadas desde a concepção da solução. Uma delas é a chamada “tokenização”, que consiste em gerar um novo identificador (*token*) a partir de um identificador único sensível, como o CPF. Esse token, como feito na solução indiana *Aadhaar*, pode ser gerado pelo próprio usuário em um serviço online e depois usado em transações digitais no lugar do identificador original. O problema dessa abordagem é que os usuários precisam ter um certo conhecimento em tecnologia para usá-la. (BANCO MUNDIAL, 2019)

Uma alternativa, então, é fazer a tokenização de forma automática e transparente para os usuários. Esse é o caso da Áustria, que usa identificadores diferentes para o mesmo cidadão em cada uma das seções da administração pública do país. Quando duas seções precisam trocar informações sobre a mesma pessoa, elas fazem uso de um terceiro ator: a *SourcePIN Register Authority*, que é o próprio sistema de tokenização e é o único que conhece o mapeamento entre o identificador original e os vários tokens gerados. Com ele, a troca de informações é feita sem que uma seção precise saber o identificador do cidadão usado pela outra. (BANCO MUNDIAL, 2019)

Em adição, pode-se proteger os dados pessoais minimizando a quantidade de informação que é transferida entre dois atores (sejam eles departamentos ou sistemas de informação dos órgãos públicos) para somente o essencial para uma transação específica. E, sempre que possível, ao invés de um ator enviar para outro os dados em si sobre um indivíduo, ele pode enviar uma resposta do tipo “Sim/ Não” para algum questionamento feito. Por exemplo, para a prestação de determinado serviço público não é necessário obter os dados pessoais junto à Receita Federal, mas sim, saber apenas se o cidadão está regular ou não com suas obrigações. (BANCO MUNDIAL, 2019)

Outro ponto central para a proteção da privacidade dos cidadãos é a capacidade de eles estarem no controle dos seus dados e poderem autorizar ou revogar o acesso a eles quando bem entenderem. A Conta Gov.br permite esse tipo de controle já, mas é possível dar um passo além, já no modelo atual. Para que os usuários estejam de fato no controle, eles precisam ter informações claras sobre como e em que situação se dará o compartilhamento dos seus dados para que eles possam consentir ou não. Além disso, eles precisam de uma ferramenta para poder monitorar quem acessou os seus dados, quando e por quê. Para isso, é importante garantir também que os registros de acesso a esses dados sejam à prova de adulteração, adicionando maior confiança ao sistema. Um bom exemplo de implementação desse recurso é o Portal do Cidadão da Estônia, onde as pessoas podem verificar e contestar acessos não autorizados aos seus dados. Em adição, é interessante também que seja incorporado nesse tipo ferramenta um mecanismo para notificar os usuários quando seus dados pessoais tiverem sido expostos no vazamento de alguma base de dados governamental. (BANCO MUNDIAL, 2019)

A adoção de medidas como as supracitadas, que visam garantir maior transparência e respeito à privacidade das pessoas, pode contribuir para que elas confiem no sistema de identidade digital e se sintam seguras em utilizá-lo. Pode contribuir, inclusive, para amenizar o aparente dilema entre privacidade, segurança e eficiência do Estado. E isso pode ajudar a favorecer a expansão do uso da ID no Brasil.

5.2. Estrutura de Governança

Os pontos tratados até o momento buscaram contribuir com possíveis avanços na construção de uma identidade digital que possa ser disponibilizada para todos os brasileiros e esteja alinhada às características de uma *Good ID*. O sucesso de um sistema de identificação, no entanto, não depende apenas dos seus atributos. As pessoas precisam ver utilidade nele e, para isso, é necessário cuidar para que cada vez mais serviços públicos e privados façam uso dele. E isso traz à tona alguns aspectos importantes quanto a mecanismos de governança para ajudar nessa expansão.

Quando se pensa na convergência de sistemas de identificação já existentes, apesar da previsão legal para que alguns deles se integrem, na prática, é possível que haja um desafio para articular os múltiplos atores envolvidos, que podem possuir interesses divergentes e dificultar a integração das soluções. Esse desafio pode ser ainda maior porque o Brasil, conforme disposto na legislação do DNI, optou por integrar o arranjo federado para emissão das carteiras de identidade com o arranjo centralizado da ICN para emissão do DNI. E ainda conta com a Conta Gov.Br, que está sob tutela da Secretaria de Governo Digital do Ministério da Economia e funciona de forma centralizada também. Nesse cenário, dois pontos podem ajudar o Brasil a avançar na pauta de ID: o estabelecimento do papel de uma Autoridade de ID e procurar trabalhar com o conceito de Governo como Plataforma.

De acordo com Banco Mundial (2019), há vários arranjos possíveis para uma Autoridade de ID, mas sendo ela uma organização autônoma, ela poderia ser vista como “neutra” e, assim, contar com mais confiança da população e das demais partes interessadas no sistema de identificação para estabelecer políticas e padrões técnicos relacionados a identidade digital. Isso seria interessante para o cenário brasileiro, pois ela poderia estabelecer as diretrizes para assegurar a interoperabilidade entre os sistemas de identificação do país, garantindo que eles se comuniquem e políticas para que eles pudessem convergir para uma solução que fosse única sob a perspectiva do cidadão. Ela poderia estabelecer, por exemplo, qual seria o mecanismo padrão para validação online de credenciais físicas (que poderia ser por meio de um QR Code com informações padronizadas), ajudando a mitigar o risco de algum órgão implementar uma solução restrita a um único fornecedor e o risco de se ter vários mecanismos diferentes sendo usados no país, que acarreta custos maiores para a implantação do sistema de identificação.

Prestar diretamente o serviço de autenticação online, Conta Gov.Br, permite ao Governo Federal maior controle sobre como ele pode ser ajustado para melhor apoiar a sua própria transformação digital. Porém, com diretrizes para interoperabilidade bem definidas por uma Autoridade de ID, o governo poderia começar a focar mais em disponibilizar APIs e ferramentas para que os entes federativos, órgãos de outros poderes e a própria iniciativa privada pudessem construir soluções para o compor o ecossistema de identificação. A partir de uma identidade digital fundacional, por exemplo, órgãos que emitem identidades funcionais poderiam modernizar os seus

mecanismos de identificação de forma mais fácil e alinhada ao que estaria sendo praticado no resto do país.

Essa abordagem poderia permitir ainda que o governo abrisse espaço, ao longo do tempo, para a iniciativa privada participar em outras etapas do ciclo de vida da identidade digital, a exemplo do que é feito no Reino Unido com o *Gov.UK Verify*. Nesse serviço, o governo não presta diretamente o serviço de autenticação online para os cidadãos. Ele, na verdade, criou uma plataforma federada onde múltiplos provedores privados de identidade digital podem se credenciar para prestar o serviço de autenticação online à população. Esse modelo poderia, inclusive, ser aproveitado no cenário brasileiro, com os entes federativos atuando também como provedores de identidade digital. (BANCO MUNDIAL, 2019)

Abrir mais espaço para a participação da iniciativa privada pode ser interessante também para ajudar na expansão da ID no país, pois o Estado poderia aproveitar o conhecimento e presença de mercado que alguns provedores de identidade privados já possuem, somando forças com eles.

Atuar seguindo a ideia de governo como plataforma pode ainda possibilitar um modelo de financiamento do sistema de identificação que o torne mais sustentável. Segundo Banco Mundial (2019), os provedores de identidade de outros países normalmente geram receita a partir de cobrança de terceiros pelos serviços de verificação e autenticação de identidades, ao invés da emissão de credenciais, e a partir da cobrança por recursos extras no serviço de autenticação, conforme quadro a seguir.

Quadro 4 - Exemplos de taxas para os serviços de verificação e autenticação de identidade

País	Cobrança para o Setor Público	Cobrança para o Setor Privado
Argentina	Gratuito	Taxa por consulta: <ul style="list-style-type: none"> • \$ 0,125 (básica) • \$ 0,375 (impressão digital) • \$ 2,500 (outras biometrias)
Chile	Gratuito	Taxa por consulta: <ul style="list-style-type: none"> • \$ 0,040 (básica) • \$ 0,054 (foto) • \$ 0,040 (assinatura) • \$ 0,135 (biometria)
Colômbia	Gratuito	Taxa baseada no volume de consultas: <ul style="list-style-type: none"> • \$ 0,095 por consulta (biometria), até 100.000 consultas • \$ 0,014 por consulta (básico), até 12M de consultas

Índia	Gratuito	Taxa por consulta: <ul style="list-style-type: none"> • \$ 0,007 (resposta de autenticação com Sim/ Não) • \$ 0,030 (transações de e-KYC)
-------	----------	--

Fonte: Adaptado de Banco Mundial (2019)

Não cobrar do setor público por APIs e ferramentas voltadas ao sistema de identificação pode ajudar na expansão dele pelo país. Porém, cobrar da iniciativa privada pelo uso dos serviços para validar dados fornecidos pelos seus clientes pode ajudar o sistema de identificação a ser sustentável financeiramente.

Por fim, o último ponto em relação à governança refere-se ao envolvimento da sociedade no processo como um todo. Conforme Banco Mundial (2019), é importante considerar engajar a sociedade civil em consultas e audiências públicas ao longo do processo para que seja possível conhecer as impressões e preocupações dela acerca do modelo que está sendo concebido no país. Isso poderia ajudar a corrigir rumos e mitigar riscos de implementação de uma solução incapaz de ganhar tração em setores da sociedade. Um exemplo de consulta pública feita para ajudar nesse aspecto foi a realizada no Reino Unido após alguns anos da implantação do *Gov.UK Verify*, onde a população foi consultada sobre o que ela esperava de uma solução de identidade digital, de forma que o governo pudesse identificar oportunidades de melhoria e se alinhar melhor às expectativas da população. (REINO UNIDO, 2020)

5.3. Instrumentos legais e de regulação

No âmbito legal, o Brasil já conquistou marcos importantes, aproximando-se de muitos dos países que já possuem uma identidade digital consolidada. Um passo importante para o país no momento, então, é consolidar a aplicação das legislações que estabeleceram esses marcos, como a LGPD, e a adequação dos órgãos a elas.

A LGPD, por exemplo, entrou em vigor em setembro, mas a Agência Nacional de Proteção de Dados, prevista nela e responsável pela fiscalização do seu cumprimento, ainda está sendo estruturada, conforme Brasil (2020f). Esse é um ponto de atenção importante, pois apesar de a lei já estar em vigor, as sanções previstas nela ainda não podem ser aplicadas, como as relacionadas ao uso indevido de dados.

Além disso, é importante observar possíveis conflitos entre a lei de proteção de dados e privacidade e outras legislações que estimulam um amplo e, em alguns casos, automático compartilhamento de dados entre os órgãos públicos, como a que criou o Cadastro Base do Cidadão. Esses conflitos podem gerar insegurança e atrapalhar a maturação da identidade digital no Brasil. Nesse caso, é imprescindível compatibilizar tais regulamentações para mitigar o risco de questionamentos judiciais.

Em adição, dado que a interoperabilidade e o compartilhamento de dados são peças fundamentais para o sistema de identificação, é imprescindível que sejam estabelecidas no âmbito dos órgãos que tratam dados pessoais, políticas claras e transparentes de governança de dados, alinhadas à LGPD, e políticas de segurança da informação. Isso ajudaria a criar um ambiente mais favorável ao desenvolvimento da ID no país.

Por fim, é interessante o Brasil se atentar a regulações internacionais quanto a interoperabilidade das identidades digitais entre países, como a eIDAS (*electronic Identification, Authentication and trust Services*) da União Européia. Conforme Banco Mundial (2019), a eIDAS visa prover “ambiente regulatório previsível, padrões e mecanismos de governança para facilitar e permitir interações seguras entre negócios, cidadãos e autoridades públicas na União Européia”. Esse é um ponto importante, pois pode ajudar a criar um modelo de identidade digital que possa ser utilizado futuramente pelos cidadãos brasileiros em outros países.

6. CONCLUSÃO

O presente trabalho mostrou que no complexo ecossistema de identificação brasileiro ainda não foi concebida, segundo uma visão sistêmica e integrada, uma identidade digital alinhada aos princípios de uma *Good ID*, mas que passos importantes para a sua construção já foram dados. A partir dessa percepção, o trabalho, então, explorou possíveis avanços nos eixos modelo de solução, estrutura de governança e instrumentos legais e de regulação, contribuindo para o debate em torno da concepção de uma ID única no Brasil.

Em relação ao modelo de solução, conclui-se que um caminho possível para o Brasil é integrar e fazer convergir as diferentes soluções existentes (DNI, Conta

Gov.Br, certificados digitais ICP-Brasil, Carteiras de Identidade) de modo que, sob a perspectiva dos cidadãos, haja apenas um sistema de identificação seguro e confiável, e não haja a necessidade de o cidadão apresentar mais do que uma de suas credenciais para ter acesso concedido a serviços e direitos garantidos.

Para se atingir esse objetivo, é fundamental possibilitar que o cidadão tenha acesso a credencial (cartão físico, aplicativo de celular, usuário e senha etc.) que melhor atenda às suas necessidades quando ele precisar comprovar a sua identidade. Além disso, é importante disponibilizar uma plataforma tecnológica eficiente e segura, que permita que todos os atores envolvidos no ecossistema de identificação se comuniquem respeitando a privacidade dos cidadãos e deixando-os no controle dos seus dados pessoais, a exemplo do que a Estônia fez com a construção do *X-Road* e do Portal do Cidadão. (BANCO MUNDIAL, 2019)

Plataforma é um conceito chave para o desenvolvimento da solução de identidade digital no Brasil. E, em vez de prover diretamente todo o serviço de identificação, o país poderia focar na construção da infraestrutura tecnológica, legal e de governança para permitir a evolução do ecossistema de identificação brasileiro em conjunto por atores do setor público, setor privado, meio acadêmico e sociedade civil, procurando aproveitar o que cada um pode oferecer de melhor.

Assim, a partir de uma abordagem mais integrada e sistêmica, acredita-se que o sistema brasileiro de identificação possa evoluir para uma identidade digital única, alinhada às práticas internacionais, disponível para todos os brasileiros e que seja confiável, segura, inclusiva, acessível, de fácil utilização, transparente e que respeite a privacidade.

Por fim, o presente trabalho aborda a identidade digital no cenário brasileiro a partir de uma visão holística de componentes importantes para essa política pública (modelo de solução, estrutura de governança e instrumentos legais e de regulação). Mas, apesar de discutir possíveis avanços em cada um deles, não detalha e nem propõe, por exemplo, um modelo de governança ou um modelo de negócio para sustentar financeiramente os serviços relacionados à política de identidade digital. Trabalhos futuros podem, portanto, procurar se aprofundar nesses tópicos, se valendo de entrevistas com gestores públicos e privados, para explorar oportunidades e dificuldades e tentar propor alguns modelos para o Brasil.

REFERÊNCIAS

BANCO MUNDIAL. ID4D Practitioner' Guide, Version 1.0. Washington, DC: October, 2019. Disponível em: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>. Acesso em: 11 set. 2020

BARBOSA, A.; CARVALHO, C.; Costa, J., MACHADO, C. Good ID na América Latina: Fortalecendo usos apropriados da identidade digital na região. Disponível em: https://itsrio.org/wp-content/uploads/2020/07/GoodIDnaAmericaLatina_PT-1.pdf. Acesso em: 11 set. 2020

BRASIL (a). Registro de Identidade Civil - RIC. Ministério da Justiça e Segurança Pública. Disponível em: <https://www.justica.gov.br/Acesso/governanca/ric>. Acesso em: 17 nov. 2020.

BRASIL (b). Instituto Nacional de Tecnologia da Informação (ITI). Disponível em: <https://www.gov.br/iti/pt-br>. Acesso em: 17 nov. 2020.

BRASIL (c). Conta Gov.Br. O que é. Disponível em: http://faq-login-unico.servicos.gov.br/en/latest/_perguntasdafaq/oquee.html. Acesso em: 19 nov. 2020.

BRASIL (d). Webinar Transformação Digital de Serviços Públicos – Automação de Serviços Públicos, Login Único e Identidade Digital. Ministério da Economia. Secretaria de Governo Digital. Disponível em: https://drive.google.com/file/d/1o1Gyji8MTvkZQPv4DbDnSPhJZ9R-h2_B/view. Acesso em: 19 nov. 2020.

BRASIL (e). Rede Nacional de Governo Digital. Ministério da Economia. Secretaria de Governo Digital. Disponível em: <https://www.gov.br/governodigital/pt-br/transformacao-digital/rede-nacional-de-governo-digital>. Acesso em: 05 dez. 2020.

BRASIL (f). Governo Federal publica a estrutura regimental da Autoridade Nacional de Proteção de Dados. Disponível em: <https://www.gov.br/secretariageral/pt-br/noticias/2020/agosto/governo-federal-publica-a-estrutura-regimental-da-autoridade-nacional-de-protacao-de-dados>. Acesso em: 06 dez. 2020

DNI. DNI – Documento Nacional de Identificação: o que é, como funciona, como solicitar o DNI. Disponível em: <https://dni-br.com/>. Acesso em: 05 dez. 2020.

DONEDA, D.; SANTOS, M.; KANG, M. Políticas de Identidade na Era Digital e o Registro Civil Nacional. Em Debate, Belo Horizonte, v.8, n.6, p.41-64, ago. 2016.

GOODID. 2020. Good ID Explained. Disponível em: <https://www.good-id.org/en/about/>. Acesso em: 17 nov. 2020.

GOVERNO DO BRASIL. Estratégia de Governo Digital 2020-2022. Disponível em: <https://www.gov.br/governodigital/pt-br/EGD2020>. Acesso em: 8 set. 2020

ID2020. The need for good digital ID is universal. The ID2020 Alliance, 2020. Disponível em: <https://id2020.org/digital-identity>. Acesso em: 16 nov. 2020.

ITS RIO. 2020. Mapa da Informação. Disponível em: <http://mapadainformacao.com.br/>. Acesso em: 31 jul. 2020.

LEMOS, R. Brasil perdeu a luta das IDs digitais. Disponível em: <https://itsrio.org/pt/artigos/brasil-perdeu-a-luta-das-ids-digitais/>. Acesso em: 17 nov. 2020.

LOPES, João. A nova carteira de identidade e o projeto RIC. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 15, n. 2711, 3 dez. 2010. Disponível em: <https://jus.com.br/artigos/17931>. Acesso em: 17 nov. 2020.

MACHADO, C. Identidade Legal na Internet. VI Seminário de Proteção à Privacidade e aos Dados Pessoais. 2015. Disponível em: <https://seminarioprivacidade.cgi.br/2015/files/ApresentacaoClaudioMachado.pdf>. Acesso em: 10 set. 2020

MACHADO, C. O Registro Civil frente à Pandemia do COVID-19: Recomendações internacionais e a resposta brasileira. Maio, 2020. Disponível em: <https://www.conjur.com.br/dl/registro-civil-versao-final-lieg.pdf>. Acesso em: 10 set. 2020

MCKINSEY GLOBAL INSTITUTE. Digital Identification: a key to inclusive growth. April, 2019. Disponível em: <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.pdf>. Acesso em: 22 ago. 2020

OECD. Digital Government Review of Brazil: Towards the Digital Transformation of the Public Sector, OECD Digital Government Studies, OECD Publishing, Paris. 28 nov. 2018. Disponível em: <https://doi.org/10.1787/9789264307636-en>. Acesso em: 17 nov. 2020

REINO UNIDO. Digital Identity: Call for Evidence Response. Disponível em: <https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response>. Acesso em: 06 dez. 2020

WORLD ECONOMIC FORUM. Identity in a Digital World: a new chapter in the social contract. September, 2018. Disponível em: http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf. Acesso em: 26 ago. 2020