Banco Interamericano de Desenvolvimento

A gestão da identidade e seu impacto na economia digital

Setor de Instituições para o Desenvolvimento

Divisão de Inovação para Servir o Cidadão

DOCUMENTO PARA DISCUSSÃO Nº IDB-DP-*529*

Alejandro Pareja
Mari Pedak
Carlos Gómez
Alejandro Barros

Agosto de 2017

A gestão da identidade e seu impacto na economia digital

Alejandro Pareja
Mari Pedak
Carlos Gómez
Alejandro Barros

Agosto de 2017

BID
Banco Interamericano de Desenvolvimento

Contatos: Alejandro Pareja, apareja@iadb.org.

A GESTÃO DE IDENTIDADE E SEU IMPACTO NA ECONOMIA DIGITAL

BID

Resumo

A identidade digital é a pedra fundamental da transformação digital da América Latina e do Caribe (ALC). É um aspecto cada vez mais relevante no sistema de identidade das pessoas, cujos fundamentos são registros civis de qualidade. Ela conforma um instrumento essencial para a inclusão e a redução de custos de transações em toda a economia, contribuindo, assim, para melhorar a qualidade dos serviços, tanto do setor público quanto do privado. Este documento oferece um panorama geral da identidade digital, mostrando custos/benefícios e vantagens/desvantagens das distintas alternativas de implementação. Em especial, inclui uma análise aprofundada de duas experiências bastante distintas, a da Estônia e a da Espanha.

Classificações JEL: D02, D73, K23, L14, L81, L86, L88

Palavras-chave: identidade digital, economia digital, governo digital, autenticação, biometria, certificado digital, assinatura digital, Estônia, Espanha, Canadá, PKI, DNI eletrônico

Índice

Prólogo

A identidade digital é a pedra fundamental da transformação digital da América Latina e do Caribe (ALC). Para o ano 2030, de acordo com os objetivos do desenvolvimento sustentável, todos os cidadãos deverão ter uma identidade jurídica, incluindo o registro de nascimento. Ao possuir uma identidade digital, existe o potencial de desencadear uma série de benefícios dos quais todo cidadão deveria gozar. A taxa de registro da população na região aumentou de 82% para 90%. Entretanto, apesar dos avanços, 1 de cada 10 cidadãos não pode comprovar sua identidade, portanto, não pode acessar serviços básicos como educação, atendimento médico, benefícios sociais, acesso ao capital ou outro serviço financeiro, tampouco votar, cruzar fronteiras legalmente ou possuir bens, dentre outros.

O registro e a gestão da identidade são instrumentos essenciais para a inclusão, já que reduzem os custos de transações em toda a economia, permitindo melhorar a qualidade dos serviços para o setor público e privado. Esse processo enfrenta alguns desafios, por exemplo, a privacidade, por um lado, e possíveis fraudes, por outro. Os atuais desafios do desenvolvimento só podem ser sustentáveis se o setor privado também fizer parte da solução. Entretanto, são os governos que estabelecem os fundamentos para promover o investimento e gerar prosperidade.

Nesse sentido, o presente documento de discussão, elaborado no marco da agenda digital da Divisão de Inovação para Servir o Cidadão (ICS),[1] explora o potencial da identidade digital em sua transformação dos diferentes setores da economia através de dois casos emblemáticos.

O Banco Interamericano de Desenvolvimento espera poder oferecer aos países recursos financeiros, conhecimento e soluções inovadoras que promovam a adoção da identidade digital universal, permitindo que os cidadãos melhorem sua qualidade de vida.

Luiz Ros
Assessor Especial de Inovação
da Iniciativa de Economia Digital

1 a ICS integra o Departamento de Instituições para o Desenvolvimento (IFD). Tem como missão melhorar as vidas por meio de governos melhores (mais eficazes, eficientes e transparentes). Suas áreas de intervenção incluem uma agenda digital mediante a qual se objetiva o desenvolvimento do governo digital e o fortalecimento e a modernização de registros civis e sistemas nacionais de identidade.

Resumo executivo

É muito difícil encontrar um resumo em português sobre o panorama da identidade digital, que ponha em claro as decisões que podem ou deveriam ser tomadas, ou que mostre custos/benefícios e vantagens/desvantagens das distintas alternativas disponíveis na hora de desenvolver um sistema efetivo de identidade digital. Este documento pretende contribuir para preencher essas lacunas, com lições gerais da experiência internacional, além de uma análise aprofundada de duas experiências bastante distintas, a da Estônia e a da Espanha. O conteúdo deste trabalho reflete os temas tratados no seminário "Gestão da Identidade e seu Impacto na Economia Digital" realizado pelo BID em outubro de 2016.[2] Durante o seminário, foram discutidos os aspectos mais relevantes da gestão da identidade, tais como o valor da confiança como um facilitador do sistema, a necessidade ou não de incluir biometria, os fatores críticos de sucesso, os sistemas em uso no nível internacional e os papéis do setor privado e do governo.

Possivelmente, a principal conclusão que pode ser extraída do seminário é que existe, em nível mundial, uma grande variedade de regimes de identidade legal física, que condiciona as alternativas que são levadas em conta em cada país para o desenvolvimento da identidade digital. Toda solução deve ser coerente com o contexto local. Os fatores que levam cada país a adotar um modelo são: i) culturais (por exemplo, a captura rotineira, por parte do Estado, dos dados biométricos de cada pessoa é feita com total naturalidade em alguns países, enquanto que, em outros, é inadmissível); ii) políticos ou de tradição administrativa (por exemplo, a existência ou não de um federalismo forte), e iii) técnicos (por exemplo, as decisões a respeito da unicidade ou obrigatoriedade de um documento nacional são tomadas depois de realizar uma análise de custo-eficácia). Na tabela 1, é possível avaliar as principais dimensões desses regimes e os países onde as distintas alternativas são aplicadas.

Tabela 1. Diferentes sistemas de identidade

Característica	Alternativas	Exemplos
Documento Nacional de Identidade (único e obrigatório, válido em território nacional)	Sim	Espanha, América Hispânica
	Não	Estados Unidos, Reino Unido, Jamaica
Sistemas federados (emissões subnacionais com validade nacional)	Sim	Estados Unidos, Canadá
	Não	Estônia, América Hispânica
Documento com biometria digital ou da íris	Sim	América Hispânica, Índia
	Não	Estônia, Estados Unidos
Documento com chip (identidade digital) obrigatório para maiores de idade	Sim	Estônia, Uruguai, Espanha
	Não	Estados Unidos

Fonte: Elaboração própria.

[2] O seminário foi organizado como parte da agenda de conhecimento da Divisão ICS, em coordenação e com o apoio do programa "Cutting Edge" do Setor de Conhecimento e Aprendizagem (KNL). O objetivo do seminário teve dois componentes: i) aprofundar o conhecimento a respeito do estado atual das tecnologias relacionadas com a identidade, em termos de alternativas, além do grau de uso efetivo das mesmas, procurando compreender a variedade de situações no mundo todo, e ii) tomar conhecimento de experiências internacionais avançadas, abrangendo não só a tecnologia, como também fatores de implementação e sustentabilidade que podem levar a um regime de sucesso.

Uma segunda conclusão é que o aproveitamento, por cada pessoa, das oportunidades que a era digital oferece depende basicamente de possuir: i) conectividade; ii) um dispositivo de conexão e conhecimento para utilizá-lo, e iii) identidade digital.[3] Claramente, sem a terceira, a Internet poderá ser utilizada e algumas de suas vantagens podem ser aproveitadas, por exemplo, no acesso à informação. Entretanto, não poderão ser realizadas transações que exigem a verificação da identidade, como muitas das relacionadas ao governo digital e ao setor financeiro.

Uma terceira conclusão surge da comparação dos processos de adoção na Estônia e na Espanha. Talvez um modelo centralizado, praticamente obrigatório e baseado em um número muito reduzido de alternativas, simplifique e facilita a adoção. No entanto, pode ser difícil de aplicar em países com burocracias de longa e complexa trajetória. O contexto estoniano era propício para esse regime, pois se trata de um país pequeno cuja burocracia teve que se reinventar no início dos anos 1990.

Por fim, casos de êxito como o da Estônia e do Canadá, mostram que os esforços coordenados entre o setor público e privado são a chave para o desenvolvimento de sistemas de identidade digital sólidos. Deve-se levar em conta, sobretudo, o papel do sistema financeiro como principal consumidor de serviços de identificação e autenticação da economia. Um regime acordado entre o setor público e financeiro não só gera economias, mas catalisa o processo de adoção por parte da população.

O seminário foi dirigido por Alejandro Pareja (Especialista de ICS), coordenado em conjunto com Carlos Molina (Especialista Líder de KNL), e contou com o apoio técnico de Alejandro Barros (Consultor Especialista em Inovação no Setor Público). A experiência do Canadá foi apresentada por Joni Brennan (Presidente, *Digital ID & Authentication Council of Canada* [DIACC]) e Rita Whittle (Diretora Executiva de Políticas de Gestão da Identidade e Segurança, *Treasury Board of Canada Secretariat*). Também contou com Mari Pedak (Consultora Sênior da *e-Governance Academy* da Estônia), Carlos Gómez Muñoz (Chefe da área de informática do Ministério da Fazenda e Administrações Públicas da Espanha) e Paul Musser (Vice-presidente de Associações Público-privadas, MasterCard).[4]

A edição deste documento esteve a cargo de Alejandro Pareja, revisado com o apoio de Ben Roseth (Especialista de ICS), Phil Keefer (Assessor Principal de IFD) e Estefanía Calderón y Florencia Serale (Consultoras de ICS). O documento está organizado do seguinte modo: primeiro, foi incluída uma breve introdução, onde os conceitos mais importantes são repassados; em seguida, são apresentadas as experiências da Estônia e da Espanha, a cargo de Mari Pedak y Carlos Gómez.[5]

---

[3] As pessoas que satisfazem essas três condições podem ser consideradas cidadãs digitais completas.

[4] Este documento é complementado por quatro vídeos com entrevistas dos conselheiros: Joni Brennan (https://vimeo.com/223474418); Carlos Gómez (https://vimeo.com/223474381); Paul Musser (https://vimeo.com/223474614) e Mari Pedak (https://vimeo.com/223476203).

[5] É importante declarar que os textos de Pedak e Gómez refletem suas respectivas opiniões, ou seja, não devem ser considerados análises realizadas pelo BID, nem se deve supor, necessariamente, que o BID compartilha suas opiniões plenamente.

Introdução[6]

O significado mais amplo do termo “identidade” implica que a pessoa pode ser reconhecida durante toda sua vida. As características utilizadas para a identificação mudam com o tempo de forma objetiva (atributos de biometria, mudanças de nome, etc.) ou podem ser mudadas pela pessoa (nome de usuário ou senha, etc.). Um desafio importante na atualidade é conseguir administrar os atributos significativos da identidade de uma pessoa, interferindo, o menos possível, em sua privacidade.

A identidade legal é organizada segundo o que se conhece como **documentos de identidade fundamentais** (certidões de nascimento para cidadãos naturais, registros de imigração para cidadãos legais ou residentes, ou documento nacional de identidade em ambos os casos). A partir desses documentos, é possível gerar os **documentos de identidade funcionais** (passaporte, carteira de habilitação etc.) e as identidades digitais legais.

A criticidade dos sistemas de identidade está aumentando por diversas razões. Por exemplo, para o setor financeiro, é possível destacar as seguintes (Fórum Econômico Mundial, 2016): i) o crescente volume de transações que requerem a verificação de identidade derivada do aumento do uso dos canais digitais e da conectividade entre entidades financeiras; ii) requisitos de transparência por parte dos reguladores e o risco de fraudes e danos à reputação das entidades.

Todo sistema de identidade conta com três tipos de atores básicos (Deloitte, 2016): i) os **usuários de serviços**, que obtêm uma identidade para cumprir com a regulação e poder realizar transações; ii) os **fornecedores de identidade**, que capturam e armazenam os atributos da identidade dos usuários, asseguram a veracidade e chegam a concluir as transações em nome deles, e iii) os **prestadores de serviços** (basicamente, as empresas e o governo), que se apoiam nos fornecedores de identidade para cumprir com o requisito KYC (do inglês “know your customer”, que pode ser traduzido como “saiba quem é seu cliente”), em todos os casos nos quais isso seja recomendado pelas boas práticas ou exigido pela regulação.

A gestão desses sistemas de identidade combina processos e tecnologias que potencializam o uso dos dados identificadores das pessoas, e requer: i) um **modelo de governança e um modelo de negócio**; ii) um **marco legal** apropriado e atualizado; iii) a **simplificação e padronização de processos e sistemas**; iv) o estabelecimento de mecanismos de **interoperabilidade** que facilitem a coordenação entre os diferentes organismos, e v) a promoção e coordenação do **ecossistema de uso da identidade**.

Com o advento da **economia digital,**[7] as interações e transações que até o momento eram realizadas de forma presencial estão começando a ser executadas por meio de sistemas de informação interconectados e pela internet. Daí surgiu a necessidade de se levar em conta a **identidade digital** de cada pessoa, compreendida como os elementos de hardware ou software que permitem que uma pessoa se identifique e seja autenticada, obtenha as permissões para acessar determinados recursos de informação ou físicos (por exemplo, o acesso a uma área) e realizar transações pela Internet ou redes privadas.

---

6 Esta seção foi elaborada por Alejandro Pareja baseado no conhecimento reunido para o seminário.

7 No contexto deste documento, entende-se por “economia digital” aquela onde a geração de valor seja fortemente baseada nas tecnologias da informação (ou, dito de outro modo, no processamento digital das informações).

A identidade digital pode ser classificada em duas categorias:

1) **Identidade digital legal**: é a que deve estar vinculada à identidade legal de uma pessoa física ou jurídica. É necessária, por exemplo, para realizar transações com o governo ou com instituições financeiras regulamentadas.
2) **Identidade digital simples**: é aquela que não precisa estar vinculada a uma identidade legal física. É utilizada, por exemplo, para se conectar às redes sociais.

Uma das formas mais comuns de identidade digital é o nome de usuário. No caso da identidade digital legal, é esse nome de usuário que está vinculado a uma identidade física. A vinculação é produzida no momento do cadastro.

A identidade digital é geralmente válida em um determinado domínio: pode ser válida unicamente para interagir com uma instituição ou em uma rede social determinada ou pode, por outro lado, ter um reconhecimento mais geral (por exemplo, em todo um país). Isso implica que uma pessoa física pode ter mais de uma identidade digital e utilizar cada uma para uma função ou contextos diferentes. O que não pode acontecer é que duas pessoas físicas tenham a mesma identidade digital legal.[8]

Para muitos tipos de interação, as pessoas e as organizações, tanto públicas como privadas, exigem que seja possível verificar com segurança a identidade da outra parte. No mundo físico, o processo de verificação da identidade se baseia em credenciais físicas, tais como cédula de identidade (RG, registro geral), carteira de habilitação ou outro tipo de documento, que, de alguma forma, creditam a identidade de seu portador.

Na economia digital, é necessário identificar as pessoas à distância, sem mediar uma interação física, na maioria dos casos sem conhecimento prévio da outra parte e, muitas vezes, sendo esse processo executado por um computador. Consequentemente, a gestão da identidade traz, por um lado, desafios em termos de privacidade, proteção de dados e novos riscos de fraude e, por outro lado, a necessidade de revisar e ajustar os esquemas de governança, os marcos legais[9] e as tecnologias que podem estar se tornando obsoletas.

Nesse novo contexto, o grau de complexidade do processo de verificação da identidade das pessoas depende do objetivo final procurado. Em particular, a complexidade depende do risco associado a um possível erro na verificação. A comprovação da identidade será tão forte quanto o mecanismo utilizado para realizá-la. Os sistemas fortes de autenticação de usuários são significativamente mais caros.

---

8 Neste documento, a menos que declarado o contrário, de agora em diante será utilizado o termo “identidade digital” para se referir à “identidade digital legal”.

9 Por exemplo, as leis que regulam a validade de uma assinatura, em especial, a digital.

Os principais processos de um sistema de identidade digital são os seguintes:[10]

1) Registro em um sistema de identidade digital. Cria-se um usuário do sistema que recebe uma credencial digital.[11] O cadastro pode ser presencial ou on-line. No primeiro caso, deve-se assinar um compromisso de responsabilidade para o uso da identidade digital. No segundo caso, é comum incluir uma etapa de confirmação por meio de outro link ou uma senha, enviados ao e-mail ou telefone do usuário.
2) Identificação e autenticação. Ocorre quando o usuário tenta acessar algum sistema de informação. As pessoas são identificadas por uma credencial física ou digital e, por meio da autenticação, é possível verificar se a pessoa realmente é quem diz ser.
3) Assinatura digital. É um mecanismo de informática que permite demonstrar a autenticidade de um documento ou mensagem.

A autenticação é um processo central no mundo digital. Historicamente, está sustentado em três elementos (fatores) utilizados para melhorar a robustez e a segurança do método, a saber:

1) Algo que a pessoa saiba: uma senha ou resposta a uma pergunta pessoal.
2) Algo que a pessoa seja: biometria dáctila, de íris, facial ou voz.
3) Algo que a pessoa tenha: um cartão de identidade ou de crédito, um certificado digital.[12]

As boas práticas recomendam que, para operações de alto risco, deve-se usar uma combinação de pelo menos dois desses elementos.

A inovação no terreno da autenticação é constante. Entre as novidades mais recentes para alguns serviços on-line, é possível mencionar a adoção de mecanismos complementares de segurança do tipo adaptativo que se baseiam no histórico dos usuários (perfil de navegação, geolocalização, perfil de uso de redes sociais etc.).

As assinaturas digitais são realizadas por certificados digitais e permitem não só dar consentimento ao conteúdo de um documento ou mensagem, mas também assegurar sua inviolabilidade e o não repúdio da assinatura.

No setor público da ALC, o grau de desenvolvimento das transações on-line é muito baixo.[13] Portanto, os mecanismos de autenticação digital são limitados e, em geral, se restringem a usuário e senha. Vários países da região têm estabelecido uma regulação de assinatura digital,

---

10 Àqueles aqui detalhados podem-se adicionar a autorização para acessar determinados recursos e os inerentes à gestão (atualizações e remoções do sistema).

11 A credencial digital é um documento, arquivo ou identificador digital que, no mundo digital, equivale a um documento de identidade físico. Similar ao mundo físico, os atributos de identidade contidos na credencial digital variam: podem ou não incluir biometria, assinatura, etc.

12 Um certificado digital é um arquivo digital que, no mundo digital, cumpre funções similares às de um cartão de identidade físico que inclua a assinatura da pessoa. Portanto, o arquivo contém a identificação da pessoa e sua senha pública. Faz parte do mecanismo que o proprietário pode utilizar para assinar pacotes de informações (documentos). Dito de outra forma, o arquivo diz quem é seu proprietário (identificação) e permite comprovar a assinatura digital que essa pessoa utiliza (autenticação). O arquivo é emitido por um certificador autorizado cuja função é garantir a terceiros que a assinatura corresponde à pessoa. O certificado pode estar gravado no disco rígido de um computador, no chip de um documento físico ou na nuvem.

13 Consulte o estudo sobre a qualidade dos trâmites, em Pareja *et al.* (2016).

alguns há mais de 10 anos. Entretanto, o nível de uso ainda é muito incipiente. Dentre os principais fatores causais desse baixo nível de desenvolvimento, podemos mencionar: i) as escassas possibilidades de uso dos certificados, devido à baixa oferta de serviços que aceitam assinaturas digitais e ao relativamente reduzido número de casos de uso onde é necessária uma assinatura digital com certificado; ii) o custo para o usuário (considerável, no começo); iii) o incômodo que representa para o usuário ter que contar com um leitor do dispositivo onde o certificado está armazenado (*smartcard*, *token*-USB ou outro), e iv) vários marcos regulatórios que podem ter sido aprovados mais para emular países avançados, seguindo uma moda, do que levando em conta a situação local ou administrando de modo realista as expectativas de adoção.[14]

Governança dos sistemas de identidade

Existem diversos modelos de governança para os sistemas de identificação. Por um lado, há países em que uma entidade pública central tem as competências exclusivas em termos de registro de nascimentos e inscrição no sistema nacional de identidade (junto à emissão correspondente do documento de identidade físico). Nessa categoria se encontram todos os países da América Hispânica.

Por outro lado, há países onde não existe uma única instituição pública central que inscreva e emita um documento nacional de identidade (por exemplo, Canadá, Estados Unidos, Reino Unido e vários países do Caribe). Nesses casos, costumam existir documentos de identidade funcionais. Por exemplo, carteira de habilitação, comprovante de registro no seguro social, passaporte ou documento eleitoral. Esses documentos de identidade coexistem e cabe a cada agente definir qual será aceito como comprovante de identificação de um indivíduo. Em geral, os ecossistemas com diversos documentos de identidade implicam um maior risco de fraude. Portanto, nesses casos se exige uma sólida coordenação entre os diferentes emissores.

Em alguns países, o número e o documento de identidade são emitidos no momento do nascimento, enquanto em outros são obtidos na hora da abertura de uma conta bancária, do início dos estudos, de empreender uma atividade econômica, ou para dirigir ou votar.

No caso da identidade digital, há países da região onde a instituição administradora do sistema de identidade gerencia a identidade digital, sobretudo para seu uso na relação com o Estado. Em nenhum caso isso envolve um fornecedor exclusivo. Pelo contrário, o mais comum é que cada organismo implemente seu próprio mecanismo de autenticação. Não obstante, alguns países da região, como Chile e Uruguai, estão avançando na implementação de um esquema *single sign-on*[15] para o setor público. Há países em que o principal impulsor da identidade digital única para o setor público é o organismo responsável pelo governo digital.

No âmbito privado, em especial no caso das instituições financeiras, observa-se uma tendência a desenvolver modelos próprios de gestão da identidade digital. Isso se deve à criticidade e aos riscos do processo de autenticação para esse tipo de instituições e implica que há poucas experiências em que uma instituição financeira contrata com outra empresa os serviços de autenticação de usuários.

---

14 Consulte Andrews, Pritchett e Woolcock (2012). Os autores chamam os casos desse tipo de “mimetismo isomórfico” (*isomorphic mimicry*).

15 Com esse esquema, a pessoa se conecta com o mesmo usuário e senha em qualquer site, nesse caso, do governo. Um exemplo que também cabe destacar é a França: https://franceconnect.gouv.fr/.

Custo e financiamento dos sistemas públicos de gestão de identidade

As instituições fornecedoras de serviços de identidade são financiadas com uma combinação de recursos provenientes do orçamento público e da venda de serviços. A proporção de ambas as fontes varia conforme o país.

Alguns serviços costumam ser prestados de forma gratuita (como a emissão da certidão de nascimento), enquanto outros não. Mesmo os serviços que são obrigatórios para os cidadãos (renovação do documento de identidade, por exemplo) são normalmente cobrados. Também costuma-se vender serviços a empresas (especialmente as do setor financeiro), relacionados à verificação da identidade.[16]

Quanto à identidade digital, existe comumente um baixo grau de consciência a respeito dos custos associados (algo que também ocorre no setor privado), sendo muito comum serem incluídos como parte do custo total da gestão das tecnologias da informação e, portanto, não são quantificados. Isso, por sua vez, impede que se considerem alternativas com melhor relação custo-benefício.

Os principais componentes do custo de gestão da identidade digital são os seguintes:

1) Implementação e manutenção do suporte tecnológico, constituído por bases de dados, plataforma PKI (na sigla em inglês, *Public Key Infrastructure*),[17] o software de gestão dos dados de identidade e outras medidas de cibersegurança.
2) Cadastro e renovação de certificados. Dada sua criticidade, em muitos casos é um trâmite presencial, com o consequente alto custo tanto para a instituição como para os cidadãos.
3) Aquisição e manutenção dos dispositivos que armazenam certificados (*tokens*, cartões, leitores, geradores de chaves dinâmicas, etc.)
4) Suporte aos usuários (por exemplo, quando esquecem sua senha).

Na tabela 2, apresentamos, para referência, uma estimativa dos custos operacionais de gestão da identidade por ano e por usuário:

16 Por exemplo, a solicitação dos dados pessoais de uma pessoa a partir de sua impressão digital.

17 Traduzido como “Infraestrutura de senha pública”, é a plataforma de geração, gestão e revogação de certificados digitais, que permite criptografar e descriptografar comunicações e documentos.

Tabela 2. Custos operacionais de gestão da identidade

Tipo de mecanismo	Custo anual por usuário (US$)
Usuário-chave	10 a 100[18]
Chave dinâmica[19]	20 a 36[20]
Assinatura digital	50 a 180[21]

Esses custos. que são inevitáveis para que seja possível realizar transações via web, podem parecer significativos. Entretanto, deve-se compará-los com os correspondentes aos outros canais de atendimento. No caso do canal on-line, o custo operacional total inclui o custo de gestão da identidade digital. Na tabela 3, apresentamos
esses custos.[22]

Tabela 3. Custos operacionais por canal de atendimento (US$)

Canal	Canadá	Reino Unido	Noruega	Austrália
Presencial	7,42	15,32	14,01	19,61
Telefônico	4,57	5,89	7,01	7,66
On-line	0,11	0,44	0,53	0,46

Fonte: Elaboração própria baseada em Kernaghan (2012), Local Government Association (2014) e Deloitte (2015).

Benefícios e impacto da identidade digital

Do ponto de vista econômico, é possível considerar dois tipos de benefícios associados à identidade digital: i) os derivados diretamente da digitalização de processos existentes que antes eram oferecidos somente de forma presencial (por exemplo, a verificação de identidade), e ii) os associados ao surgimento de novos serviços e atividades econômicas como resultado do uso da identidade digital. Na tabela 3, apresentamos a vantagem desse ponto de vista operacional. Para concluir a análise, é preciso considerar a redução de custos transacionais para os usuários do canal on-line, basicamente pela economia de tempo e transferências. Isso gera um impacto ainda maior, embora difícil de determinar. De todo modo, parece razoável estimá-lo em uma hora-homem (correspondente a uma renda média) por transação. Agora, mesmo quando a economia para os cidadãos é claramente positiva, cabe ressaltar que, ao levar os serviços aos canais virtuais, se produz uma externalização dos custos a eles. Isso se manifesta, por exemplo, na necessidade de contar com um dispositivo para se conectar e nos custos dos certificados digitais, no serviço de conectividade e outros.

---

18 Ver, por exemplo, AT&T (2016).
19 As chaves dinâmicas são chamadas *one-time password* (OTP).
20 Ver, por exemplo, Lista de preços da Bitium (2017).
21 Ver, por exemplo, Produtos e preços da DocuSign (2017).
22 No âmbito privado –ou seja, no setor financeiro– observa-se custos semelhantes entre os canais presenciais e remotos.

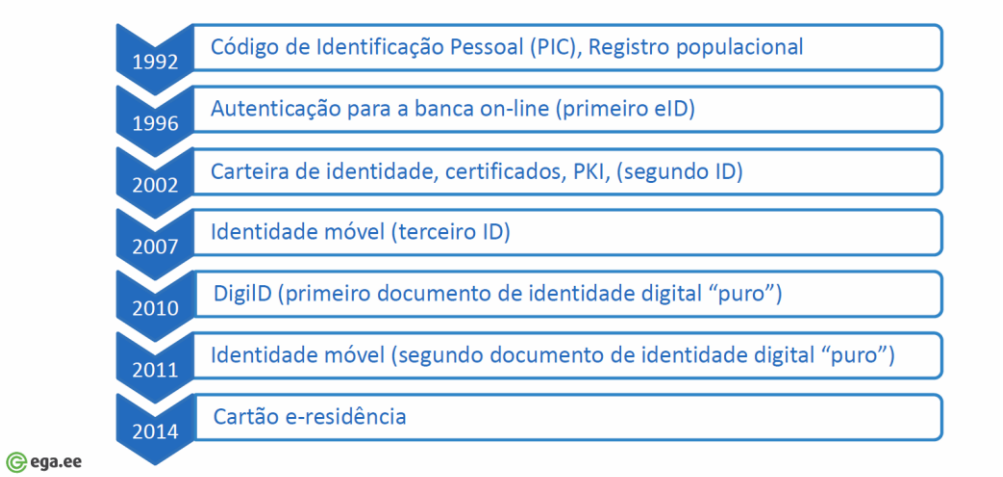
Com relação às atividades econômicas derivadas da gestão da identidade digital, é possível mencionar as seguintes:

1) Cibersegurança: necessária para a proteção contra fraudes, roubo de identidade, etc.
2) Desenvolvimento de software específico para gestão de identidade que inclui as funcionalidades já mencionadas.
3) Serviços privados de autenticação.
4) Gestão de certificados digitais por parte de organismos públicos e empresas emissoras de certificados.
5) Desenvolvimento e produção de dispositivos para autenticação e armazenamento de certificados digitais.
6) Algumas atividades que são reduzidas ou desaparecem, por exemplo, as associadas ao atendimento presencial do público.

Estônia: do registro da população à gestão da identidade digital[23]

A Estônia é um dos países líderes em gestão da identidade digital. Desde o início da década de 1990, alguns componentes essenciais da gestão de identidades foram sendo estabelecidos no marco legislativo (código de identificação pessoal, registro da população etc.) (gráfico 1). Em 1996, foi iniciado o processo de autenticação para bancos on-line. A partir daí, se produziu uma evolução constante e, em 2014, começou a ser emitida a identidade digital para estrangeiros que desejam fazer parte da comunidade de residentes digitais da Estônia (*Estonia e-residents*).[24] Atualmente, 98% dos residentes da Estônia possuem um documento de identidade que funciona como *token* para utilizar a identidade digital.

Gráfico 1. Marcos na gestão da identidade digital na Estônia



Fonte: Elaboração própria.

Identidade

No cerne da política de gestão da identidade estoniana, estão os seguintes princípios: i) o Estado é o único responsável por identificar as pessoas; ii) a gestão é centralizada; iii) cada pessoa deve contar com uma única e exclusiva identidade legal, e iv) o vínculo entre o documento físico e o certificado digital é inequívoco e verificável publicamente através de um elemento fundamental no sistema estoniano: o código de identificação pessoal (PIC, na sigla em inglês), que entrou em vigor em 1992.

Nos tempos em que a identificação da pessoa se limitava ao mundo físico, a presença física da pessoa, em grande medida, compensava a necessidade de contar com um identificador único legal. Embora muitos estados incluíram um código numérico de identificação pessoal nos documentos de identidade, sua ausência não causava nenhuma consequência grave. O desenvolvimento dos serviços eletrônicos mudou completamente a situação: a existência de um identificador único passa a ser um requisito prévio para o estabelecimento de um marco de identificação forte.

---

23 A autora desta seção é Mari Pedak, especialista em identidade digital da Academia do Governo Eletrônico da Estônia (eGA). Ver a declaração no final do resumo executivo.

24 A Estônia tem 12.000 residências digitais outorgadas. Ver https://e-estonia.com/e-residents/about/.

O PIC é um número de 11 dígitos. Contém informações pessoais (gênero e data de nascimento), diferente de outros países, onde o número de identidade é completamente sequencial e, portanto, não contém nenhuma informação pessoal. O PIC é designado quando a pessoa se cadastra no Registro da População.

Em culturas e contextos históricos diversos, a atitude a respeito do número de identificação é diferente. Na Europa há países em que a designação de números a pessoas vai contra sua memória histórica ou social. Alguns países consideram que o número de identificação pessoal ou os dados que contém são confidenciais e, mesmo quando existem, seu uso é muito limitado.

Muitas vezes, as discussões sobre o identificador único se concentram em, precisamente, se o mesmo deve ou não refletir atributos da pessoa, algo bastante irrelevante. O identificador único é necessário para assegurar uma identificação inequívoca e incondicional dos consumidores de serviços eletrônicos em processos de autenticação segura e intercâmbio de dados. Como as tecnologias da informação modernas oferecem novas formas de identificação única, espera-se que essa discussão sobre a forma tomada pelo identificador abra espaço para um debate mais substancial.

O registro da população como base da gestão de identidade

O registro da população da Estônia inclui os eventos abrangidos pelo registro civil e outros, entre os quais figura o registro do domicílio. O registro da população é resultado de um processo contínuo no qual a informação sobre os acontecimentos da vida e o local de residência, originalmente registrados em diferentes sistemas administrativos, são vinculados de forma automática e contínua.

Os distintos sistemas administrativos recebem dados das pessoas e são, ao mesmo tempo, uma fonte de dados. O registro da população é alimentado pelas listas de votação, pelo censo, pelo processo de emissão de documentos de identidade, pelos sistemas de registro civil e pelo registro de residência, ou seja, os dados para o registro da população são recolhidos pelo setor público ao prestar serviços distintos.

Com a difusão dos registros digitais e do intercâmbio automatizado de dados, a relevância dos dados ou, em outras palavras, a qualidade dos dados e sua manutenção tornam-se cruciais. Os dados obsoletos ou imprecisos são transmitidos em tempo real pelo país ou, inclusive, através de fronteiras nacionais, podendo implicar consequências negativas para as pessoas.

Sobre a experiência da Estônia, para garantir a qualidade dos dados, recomenda-se estabelecer uma hierarquia de registros e atribuir a diferentes instituições a “propriedade” de subconjuntos de dados específicos. Sem isso, é provável que se produzam sobreposições desnecessárias de processos e bases de dados, o que resulta em uma duplicação inútil dos gastos em equipamentos e tecnologia. Além disso, as mesmas informações acabarão sendo armazenadas em diferentes formatos e em diferentes registros, causando confusão e dificultando o desenvolvimento do sistema em seu conjunto. O registro civil é uma boa opção para manter o conjunto principal de dados pessoais.

O estabelecimento de tal hierarquia assegura que todos os processadores de dados estejam usando os dados corretos, enviados pela instituição oficialmente proprietária (exclusiva) dos mesmos. E, caso se detecte dados pessoais incorretos, as correções só podem e devem ser realizadas por tal instituição proprietária, depois do qual todos os processadores de dados podem utilizar o conjunto de dados corrigido.

A identidade digital e seus ecossistemas

Os regimes digitais de identidade podem ser classificados em três tipos: i) aqueles com baixo nível de segurança (por exemplo, senhas); ii) aqueles baseados em PKI (por exemplo, documento eletrônico), e iii) os que se baseiam em *blockchain*. A seguir, descrevemos cada um deles e seu uso na Estônia.

Regime de identidade com baixo nível de segurança

Esses sistemas de identidade digital utilizam meios como cartões de senha e calculadoras de PIN.[25] Apesar da insegurança desses regimes, são os que predominam no mundo digital. A autenticação de nome e senha prevalece nas redes sociais. Lamentavelmente, muitos países e grandes prestadores de serviços só oferecem esquemas desse tipo.

Inclusive na Estônia, a sociedade da informação mais avançada, cerca de 25% dos usuários do portal do Estado usam esses mecanismos de autenticação. Os motivos por trás da popularidade, derivados de seu êxito no setor financeiro, incluem: i) início relativamente cedo do banco eletrônico na Estônia (1996), que incluiu o fornecimento de serviços de autenticação para terceiros; ii) nível muito elevado da adoção do banco eletrônico por parte das pessoas (quase 100%); iii) simplicidade de utilização (não é preciso hardware especial, como leitor de *smartcards*, nem a instalação de softwares).

Esquema de identidade baseado em PKI

A segurança dos esquemas de identidade digital baseados em PKI é construída a partir da criptografia assimétrica. Usa-se uma chave criptográfica, que se divide em duas partes: chave pública e chave privada. A chave pública é administrada pelo fornecedor da identidade. Os sistemas diferem nos métodos de armazenamento das chaves privadas.

Os mais comuns são os esquemas em que a chave privada se encontra no chip de um documento de identidade digital ou em um cartão SIM de celular (esses esquemas são os usados na Estônia). Isso assegura a proteção da chave por parte de seu proprietário.

Há países, como a Dinamarca, que não emitem documento nacional de identidade, onde as chaves privadas são administradas centralmente pelo governo, um sistema conhecido como nemID.[26] As chaves privadas armazenadas centralmente também podem ser guardadas com bastante segurança usando medidas de segurança técnicas e organizativas. No entanto, elas não estão sob o controle de seus donos. Tais soluções são possíveis nos países onde as pessoas confiam tanto em seu governo que estão dispostas a acreditar que seja excluído o

---

25 O cartão de senha consiste em um cartão físico com uma série de números e, a cada nova tentativa de iniciar a sessão, o sistema solicita um número diferente desse cartão. A calculadora de PIN gera um novo código aleatório periodicamente (por exemplo, a cada 30 segundos). Originalmente, o usuário consultava um PIN e um token. Mais recentemente, a consulta passou a ser feita por um aplicativo. Ambos os esquemas são implementações do modelo OTP, já que a senha correta é diferente e aleatória a cada tentativa de iniciar a sessão. Isso faz com que o roubo de senhas não tenha sentido.

26 https://www.nemid.nu/dk-en/.

uso indevido de suas chaves privadas. Dado que o uso dos serviços de identidade digital está diretamente relacionado à confiança,[27] é aconselhável dar prioridade aos esquemas nos quais cada uma pessoa gerencia sua própria chave privada.

O documento de identidade estoniano se baseia na tecnologia PKI e incorpora dois certificados: um para a autenticação e outro para as assinaturas eletrônicas. Para usar as chaves privadas, é necessário usar um código PIN. Além disso, o chip contém um arquivo que replica os dados visíveis no cartão. Não há informação biométrica eletronicamente utilizável no documento.

A identidade móvel foi introduzida no mercado estoniano em maio de 2007 pela maior operadora móvel (EMT) em cooperação com o centro de certificação SK. Para obter uma identidade móvel, o usuário deve substituir o cartão SIM por um que seja compatível com PKI. Apesar de o processo de registro estar a cargo da operadora móvel, ele não pode ser considerado suficientemente confiável. Por isso, o usuário deve ativar sua identidade móvel no ambiente web. A identidade móvel não requer que um leitor de smart card seja conectado ao computador nem a instalação de um software específico. Os certificados de identidade móvel contêm as mesmas informações pessoais que os certificados do documento de identidade.

Blockchain

Nos esquemas discutidos anteriormente, sempre há um terceiro que atua como garantia da identidade (por exemplo, o governo). As novas tecnologias permitem que se dispense esse terceiro, ou seja, não há um intermediário. A tecnologia mais conhecida nesse sentido é o *blockchain*, que ganhou grande reputação como um componente central das criptomoedas. Se o *blockchain* for usado, toda a comunidade atuaria como garantia da identidade de uma pessoa, enquanto a chave privada seria administrada pelos próprios indivíduos usando uma carteira digital ou um papel. Já existem serviços baseados em *blockchain* oferecidos no mercado estônio. Por exemplo, a empresa GuardTime oferece serviços de assinatura digital com base em *blockchain*.

Atores envolvidos no ecossistema de identidade digital

As partes interessadas do ecossistema abrangem aquelas relacionadas à produção de portadores de identidade, à atribuição da identidade digital e à habilitação de seu uso.

Na Estônia, há principalmente dois ministérios envolvidos neste tema:

1) O Conselho de Polícia e Guardas Fronteiriços, subordinado ao Ministério do Interior (MI), é diretamente responsável pela emissão e pela manutenção dos documentos de identidade pessoal e pelas identidades eletrônicas dos residentes em geral. O Centro de Informática e Desenvolvimento, também subordinado ao MI, é responsável pela manutenção e pelo desenvolvimento dos sistemas de informática e bases de dados correspondentes do registro da população e dos documentos de identidade.

---

27 Os sistemas de identidade e assinatura digitais, igualmente aos sistemas físicos, exigem que um terceiro garanta às partes que uma pessoa ou máquina é quem diz que é. No mundo físico, para comprovar a identidade, mostra-se um documento de identidade. Quem quiser verificar essa identidade, basta observar a fotografia e outros dados pessoais que aparecem no cartão e comparar com a pessoa que está diante de si. Fica implícito que o verificador confia nos dados do cartão porque confia que o emissor deste fez as verificações correspondentes e que o documento é seguro (difícil de falsificar). No mundo digital, ocorre algo similar (ver a nota 12). Quem recebe um documento assinado compara, com o certificador autorizado que outorgou o certificado ao subscritor, que a assinatura corresponde à pessoa. E confia no que o certificador diz, seja por seu prestígio, ou porque o governo (a autoridade certificadora raiz) assegura que é confiável.

2) A Autoridade Estatal de Sistemas da Informação (RIA), subordinada ao Ministério de Assuntos Econômicos e Comunicações (MEAC), é responsável pela coordenação governamental no campo das TI, pelo uso da identidade digital e pela segurança dos ecossistemas digitais.

A visão na Estônia é que somente os governos podem criar um marco que proporcione o grau de harmonização necessário para a gestão da identidade digital no nível nacional. O setor privado, por sua vez, desempenha um papel significativo no ecossistema estoniano. A fabricação e a personalização dos documentos de identidade são subcontratadas da empresa TRÜB Baltic AG. Os serviços de certificação e validação são proporcionados pela empresa SK. RIA e SK funcionam como um centro de excelência para o uso eletrônico do documento de identidade, proporcionando software para o uso de documentos de identidade eletrônica, inclusive o marco do software de assinaturas digitais, suporte ao usuário final e serviços a prestadores de serviços que usam o documento de identidade. Na realidade, devido a seu pequeno mercado, só há uma autoridade certificadora (emissora de certificados digitais) na Estônia.

Documento de identidade digital

O documento de identidade entrou em vigor na Estônia em 2002 (gráfico 2). A implementação foi considerada concluída em outubro de 2006, quando foi superado o limite de 1 milhão de documentos expedidos. Desde então, o número de documentos ativos se manteve em torno de 1,1 milhão. O documento de identidade é válido por no máximo cinco anos[28] e é obrigatório a partir dos 15 anos de idade. Permite a identificação física, a identificação, autenticação e assinatura digitais, a criptografia e descriptografia de mensagens, e também é válido como documento de viagem dentro da Europa.

Tanto o documento de identidade como os certificados que ele contém não são válidos até que sejam ativados. Isso é produzido quando é entregue ao usuário. Quando o documento é emitido, o receptor pode optar por manter inativos os certificados, ou seja, por não ter uma identidade digital. Nesse caso, o documento só pode ser utilizado como um documento de identidade tradicional. Geralmente, essa opção é muito pouco utilizada.

[28] A ideia de vencimento dos documentos de identidade está associada, principalmente, às variações dos atributos de identidade que ocorrem durante a vida de uma pessoa (as mudanças que ocorrem na fisionomia e em alguns dados pessoais que aparecem no documento, por exemplo, o domicílio) e a necessidade de refletir essas mudanças para que o documento possa ser utilizado para verificar a identidade ou a residência. Por outro lado, a evolução tecnológica, tanto na produção de cartões de identidade, como na de certificados digitais, que tende a oferecer maior segurança a estes e, consequentemente, maior confiança no sistema, também é um fator que leva a recomendar uma duração limitada. Há países, por exemplo, a Estônia, onde os documentos têm uma vigência de cinco anos; em outros, de 10, e, ainda em outros, como o Brasil, que tem duração ilimitada.

Gráfico 2. Documento de identidade da Estônia

Fonte: Elaboração própria.

Em outubro de 2010, iniciou-se a emissão de um cartão de identidade exclusivamente digital (DigiID) (infográfico 1). Ele só possui a funcionalidade digital do documento de identidade principal e, portanto, não pode ser usado para a identificação física de uma pessoa. Cada DigiID está associado a um documento de identidade principal e contém uma segunda identidade digital. O cartão é feito de PVC e não possui características de segurança.

A finalidade do DigiID é permitir que as pessoas diferenciem sua identidade digital entre ações privadas e ações tomadas como membros de uma organização, por exemplo, enquanto funcionários. O DigiID só costuma ser usado no trabalho (professores em escolas, médicos em hospitais, funcionários do governo em seus escritórios etc.), enquanto o documento de identidade principal é portado constantemente.

Infográfico 1. Cartão de identidade digital (DigiID) da Estônia

Fonte: https://www.politsei.ee/et/nouanded/dokumentide-naidised/digi-id/kuni-30112014-valja- antud-digi-id.dot.

O documento de identidade estônio é multifuncional e usado em todas as áreas dos serviços públicos. Assim, por exemplo, na Estônia não existe um cartão de seguro social separado e não é preciso levar uma carteira de habilitação e os documentos do carro, pois a polícia pode consultar as respectivas bases de dados em tempo real a partir da identificação contida no documento de identidade.

O uso da biometria nos documentos de identidade digitais é um tema recorrente, especialmente nos países onde o nível de alfabetização digital é baixo. O chip dos documentos de viagem seguros e modernos contém as características biométricas da pessoa, as quais podem ser comparadas (por exemplo, nas fronteiras) às características físicas da pessoa capturadas no momento (verificação de um para um). O uso da biometria nos documentos de viagem tem oferecido maior segurança no movimento fronteiriço das pessoas.

No entanto, as opções diferem significativamente quando se trata da inclusão da biometria nos documentos de identidade para sua verificação nas bases de dados digitais (verificação de um para muitos). Por exemplo, o chip do documento de identidade da Estônia não contém dados biométricos e, ao mesmo tempo, é usado desde 2002 de forma segura, tanto para a autenticação como para a assinatura digital. A experiência da Estônia demonstra que o uso da biometria não é necessário para criar um ecossistema seguro em um país com alfabetização digital avançada. Quando, no fim de 2014, preparou-se a aquisição para a próxima geração de documentos de identidade e foram realizadas consultas com especialistas em segurança cibernética e proteção de dados, nenhum deles apoiou a introdução da biometria no documento de identidade, já que ela é considerada uma solução insegura. O uso da biometria só foi apoiado para uma solução *match-on-card*, análoga aos documentos de viagem. No entanto, esse exemplo não deve ser superestimado, já que, nos países onde o nível de alfabetização digital é baixo (o que leva a uma maior necessidade de verificações de identidade presenciais), a utilização da biometria na comprovação da identidade pode ser a única opção viável.

Usos da identidade digital

A legislação estônia diferencia entre autenticação e assinatura digital, deixando a autenticação fora do âmbito da aplicação da lei. Isso significa que não há nenhum regulamento relacionado à hierarquia dos diferentes sistemas de autenticação. Os regulamentos que existem geralmente são restritos a aplicações ou áreas específicas. Os métodos de autenticação baseados em PKI são os preferidos no setor público. Existem três métodos de autenticação: pelo documento de identidade, pela identidade móvel ou a identidade bancária.[29] Todos são utilizados amplamente nos serviços que exigem identidade legal, tanto no setor público como no privado. Por exemplo, os estonianos usaram o portal de serviços estatais @eesti.ee mais de 3,5 milhões de vezes em 2015. E 54% foi autenticado com o documento de identidade, 38% com a identidade bancária e 8% com a identidade móvel.

Quanto à assinatura digital, após 15 anos, esse método de uso se transformou no sistema de assinatura digital mais confiável e usado do mundo. Hoje em dia, são geradas na Estônia aproximadamente 7 milhões de assinaturas digitais por mês.[30] Na verdade, uma das principais razões da introdução do documento de identidade era que os estonianos pudessem contar com um meio que lhes permitiria assinar digitalmente. Desde o início, ferramentas gratuitas vêm sendo distribuídas para os usuários finais e integradores de sistemas. Como resultado, os estonianos compartilham uma visão comum sobre o que são os documentos assinados digitalmente, que são amplamente aceitos, inclusive nos tribunais. Esse desenvolvimento deu lugar ao uso massivo das assinaturas digitais, substituindo totalmente as assinaturas manuscritas. Em bancos eletrônicos, são usadas massivamente, já que todas as transações devem estar assinadas digitalmente (sempre que o usuário inicia a sessão com um documento de identidade ou uma identidade móvel).

Embora não devesse, a introdução de novas tecnologias e novos métodos por vezes abre espaço para o questionamento dos ganhos em termos de eficiência. Estima-se que a introdução de uma assinatura digital economiza em média 20 minutos por transação[31] e que, também em média, a cada três dias, uma pessoa realiza uma transação que exige assinatura. Isso equivale a aproximadamente uma semana de trabalho por ano. Por isso, a Estônia economiza anualmente 2% de seu PIB por ser uma sociedade livre de papéis.[32]

A implementação da autenticação digital e da assinatura digital também possibilitou a otimização dos serviços públicos. Alguns serviços específicos tiveram economias de tempo ainda maiores. Por exemplo, o registro de empresas acumulou uma economia de tempo para o empresário que é 17 vezes maior do que a média.

A autenticação e a assinatura digital são serviços de plataforma, que podem ser usados por qualquer serviço eletrônico. Uma variedade importante de serviços de identificação pode ser construída sobre os serviços de plataforma, como o acesso a edifícios, pagamentos eletrônicos, fidelização de clientes, etc. (Electronic Identity, 2015).

---

29 A identidade bancária é um método baseado em certificados digitais providenciados pelos bancos, que assumem, assim, um papel de garantia da identidade das partes de uma transação digital.

30 .http://www.id.ee/?lang=en&id

31 World Development Report 2016: Digital Dividends.

32 https://e-estonia.com/facts/.

Promoção do uso da identidade digital

O papel crítico da confiança no contexto da administração eletrônica não pode ser subestimado. A confiança não se deriva unicamente de uma infraestrutura técnica segura, na qual a maioria dos países se concentrou. É preciso gerar confiança. E os melhores resultados são obtidos quando existe colaboração entre o setor público e o privado. Mas tão importante quanto a confiança é a sensibilização dos cidadãos. Lamentavelmente, esse aspecto se manteve em segundo plano em todos os países pioneiros, inclusive na Estônia.

Ao introduzir a identidade digital, os países enfrentam uma situação clássica de ovo e galinha. Por um lado, os serviços eletrônicos não começam a se desenvolver até que haja um número suficientemente grande de consumidores para que se justifiquem os custos. Ao mesmo tempo, ao receber um documento de identidade digital do governo, obviamente as pessoas desejam usá-lo com entusiasmo. Isso implica que, durante a implementação, há um desajuste entre a demanda e a oferta, o que deve ser gerido para que o projeto não se perca e a confiança não se deteriore. Na Estônia, essa situação durou quatro anos. Os prestadores de serviços começaram a fazer esforços para desenvolver serviços recentemente quando se chegou a 1 milhão de identidades digitais. Nesse sentido, as campanhas de sensibilização são essenciais nesta etapa, para poder manter a população informada quanto ao que esperar da identidade digital, quais serão seus benefícios e quando poderão desfrutar deles.

Na Estônia, as campanhas de formação e sensibilização começaram com o projeto em 2002 e ainda continuam, incluindo: i) cursos de alfabetização digital (especialmente para adultos mais velhos); ii) cursos de comportamento seguro na Internet e uso seguro de dispositivos inteligentes, e iii) apoio e promoção de atividades extracurriculares relacionadas à informática para jovens, com o objetivo de aumentar o número de jovens que decidem estudar ciências ou TI.[33]

Espanha: gestão da identidade e seu impacto na economia digital[34]

A identidade digital, e, muito vinculada a ela, a assinatura digital, estiveram constantemente presentes nas políticas públicas espanholas destinadas ao desenvolvimento da sociedade da informação e do conhecimento como elementos fundamentais para garantir a confiança nas transações on-line. Em sua condição de Estado-membro da União Europeia, essas políticas públicas na Espanha sempre foram enquadradas no contexto mais amplo das políticas da UE, em que a identidade e a assinatura digitais foram consideradas de maneira usual como facilitadores essenciais para a realização do mercado único europeu e para facilitar a mobilidade de cidadãos e empresas. Essas políticas estão consubstanciadas na Agenda Digital Europeia e seu Plano de Ação de Administração Eletrônica (2011-15), no Programa de Trabalho ISA de serviços de interoperabilidade para as Administrações e na Diretiva Europeia sobre Serviços Eletrônicos.

---

33 http://www.vaatamaailma.ee/en/.

34 O autor desta seção é Carlos Gómez Muñoz, Chefe de Informática da Diretoria de Tecnologias da Informação e das Comunicações do Ministério da Fazenda e Função Pública da Espanha. Ver a declaração no final do resumo executivo.

No caso espanhol, o plano España.es (2003-05) contemplava várias medidas para garantir a segurança e a confiança nas redes digitais, entre as quais estava o desenvolvimento do Documento Nacional de Identidade eletrônico (DNI-e) e o estabelecimento de um marco legal para a assinatura digital. Esta preocupação com a segurança e a confiança on-line teve sua continuidade nos planos posteriores Avanza (2006-10) e Avanza 2 (2011-2015), e na atual Agenda Digital para a Espanha, que prevê medidas para facilitar os mecanismos de identificação e autenticação frente à Administração, e para impulsionar os serviços de confiança no mundo digital.

Apesar de que as políticas mencionadas tiveram seu desenvolvimento nos primeiros anos do século XXI, as primeiras medidas para implantar na Espanha os sistemas de identificação e assinatura digital com caráter geral (ou seja, que puderam ser usados em vários serviços eletrônicos de diferentes provedores) datam do final do século XX, com o início do projeto CERES (CERtificação ESpanhola).

Os primórdios da assinatura digital

O projeto CERES foi iniciado em 1996 pela Fábrica Nacional de Moeda e Timbre da Casa Real da Moeda, em um momento em que as primeiras PKI começavam a ser implementadas. O objetivo do projeto era constituir um Prestador de Serviços de Certificação de caráter público, que garantisse a autenticidade, a integridade, a confidencialidade e o não repúdio das transações eletrônicas realizadas pelos cidadãos, pelas empresas e pelas Administrações Públicas. Para fomentar sua adoção, definiu-se um modelo de negócio em que os certificados digitais seriam gratuitos para os cidadãos, financiando-se o sistema com as contribuições dos prestadores de serviços eletrônicos que usavam esse sistema de identificação e assinatura digital.

A primeira experiência de uso generalizado do sistema aconteceu em 1999, quando a Agência Estatal de Administração Tributária permitiu o uso da certificação digital na apresentação telemática do imposto de renda de 1998, quando foram realizadas mais de 20.000 declarações por esse meio. Desde então, o conjunto de serviços públicos que permitem o uso de certificados emitidos pelo CERES foi aumentando, bem como o número de cidadãos e empresas que dispõem de tais certificados, até chegar a cerca de 4 milhões de certificados de pessoa física ativos em 2014.

Também em 1999, foi aprovada a Diretiva europeia sobre a assinatura digital,[35] que tinha como objetivo facilitar o uso da assinatura eletrônica para promover o comércio eletrônico e o mercado único, para o qual foi estabelecido um marco regulatório para o mercado de prestadores de serviços de certificação. Por se tratar de uma Diretiva, seu conteúdo devia ser desenvolvido em nível nacional, o que ocorreu na Espanha com a transposição da Diretiva na Lei da Assinatura Eletrônica.[36] Essa Lei constitui um fundamento básico, pois outorga à assinatura digital plena validade jurídica, reconhecendo a equivalência funcional entre a assinatura digital reconhecida[37] e a manuscrita.

---

35 Diretiva 1999/93/CE do Parlamento Europeu e do Conselho.

36 Lei nº 59/2003.

37 É a realizada com um dispositivo seguro, utilizando certificados eletrônicos emitidos com as máximas garantias previstas.

A introdução do DNI-e

A Lei da Assinatura Eletrônica, além de regulamentar o mercado de prestadores de serviços de identificação na Espanha,[38] previu a existência do DNI-e como meio de identificação e assinatura, em conjunto com o programa España.es.

O DNI-e se tornou realidade em 2006, quando se começou a emitir as primeiras unidades que incorporavam um chip ao tradicional cartão do DNI. O chip, além de conter dados de identificação e biométricos, continha dois certificados eletrônicos, um de autenticação e outro de assinatura. Desde então, os antigos DNI sem chip foram sendo substituídos pelos novos DNI-e, até que hoje em dia praticamente toda a população espanhola está incluída, sendo obrigada a portar um DNI.

Apesar do DNI ser obrigatório para todos os cidadãos espanhóis maiores de 14 anos, não ocorreu o mesmo com seu uso como meio de identificação e assinatura digitais, que é totalmente voluntário. A identidade digital incluída no DNI-e requer a ativação por parte do cidadão para poder ser utilizada. Por outro lado, o usuário deve ter um leitor de cartões. Esses aspectos, somados ao surgimento de problemas de compatibilidade com algumas plataformas e a escassa oferta de serviços que o aceitam no setor privado, têm motivado que o uso real esteja abaixo das expectativas.

Espera-se que o novo DNI-e 3.0, vigente desde janeiro de 2015, ajude a superar as barreiras que impedem o uso, ao incorporar entre suas melhorias a possibilidade de acessar o chip sem a necessidade de um leitor de cartões, por meio da tecnologia NFC[39] presente em muitos smartphones e tablets.

Acesso eletrônico aos serviços públicos

Em 2007, a Lei de acesso eletrônico dos cidadãos aos serviços públicos foi aprovada.[40] Seu objetivo era impulsionar o desenvolvimento da administração eletrônica na Espanha, outorgando aos cidadãos o direito a se relacionar eletronicamente com as Administrações Públicas, que, por sua vez, estavam obrigadas a proporcionar os meios para possibilizar a relação. Como resultado de sua aprovação, desenvolveu-se a maior parte das infraestruturas de administração eletrônica que funcionam atualmente na Espanha.

No que diz respeito à identificação digital, a mencionada lei consolidou um modelo no qual os cidadãos tinham três opções para se identificarem eletronicamente perante a Administração: i) utilizar seu DNI-e, cuja aceitação é universal nos serviços públicos; ii) utilizar um dos certificados eletrônicos admitidos pela Administração em particular com a qual se relaciona, ou iii) utilizar um sistema de identificação não baseado em certificados (por exemplo, usuário e senha) específicos do serviço ao qual se quer acessar.

Devido ao número elevado de prestadores de serviços de certificação existentes na Espanha, o uso de certificados para acessar aos serviços públicos apresentava um problema prático, pois cada Administração devia estabelecer conexões com cada um dos prestadores. Além disso, a variedade de algoritmos e formatos de assinatura existentes multiplicou a

---

38 Este mercado, atualmente, é um dos mais desenvolvidos da Europa, com mais de 50 prestadores, dos quais, 25 estão qualificados.

39 *Near Field Communication* é uma tecnologia que habilita transações e pagamentos de bens e serviços.

40 Lei nº 11/2007.

complexidade da gestão dos documentos assinados. Para solucionar esse problema, foi desenvolvida a plataforma @Firma, que atua como intermediária entre as Administrações e os prestadores. Assim, a plataforma permite a validação das identificações e assinaturas realizadas com qualquer certificado emitido por um prestador reconhecido pelo Ministério da Indústria, Energia e Turismo (entre eles, o DNI-e), simplificando grandemente a implantação de aplicativos de administração eletrônica. @Firma proporciona também aplicativos e componentes para realizar assinaturas (em computadores ou dispositivos móveis) e serviços de selo de tempo para formatos de assinatura duradoura.

Por outro lado, a alternativa que essa lei permitia a cada serviço público para usar seus próprios sistemas de identificação não baseados em certificados fez com que muitas entidades optassem por essa solução, o que resultou em uma situação ineficiente, tanto para os próprios cidadãos, que se viam obrigados a se registrar e a gerenciar suas credenciais de maneira independente em cada serviço, como para as próprias Administrações, que deviam dedicar recursos para o desenvolvimento e a manutenção desses sistemas.

Para corrigir essa situação, em 2014, iniciou-se o projeto Cl@ve, destinado a implantar uma plataforma comum para a identificação, autenticação e assinatura eletrônica por meio do uso de chaves concordadas. O objetivo desse sistema era unificar todas as soluções existentes, habilitando sistemas de identificação não baseados em certificados eletrônicos que podiam ser usados em todos os serviços públicos. Para isso, usavam-se dois sistemas já existentes, um da Agência Tributária, que daria lugar ao sistema Cl@ve PIN (para uso opcional), e outro do Seguro Social, que daria lugar ao sistema Cl@ve Permanente (para uso frequente).

O sistema Cl@ve é complementado pelo Cl@veFirma, uma solução para assinatura digital na qual os certificados eletrônicos residem em um servidor. Com o Cl@veFirma, evita-se os problemas associados à gestão e ao acesso aos certificados no dispositivo do usuário, mantendo todas as vantagens do uso da assinatura digital.[41] Esses certificados de assinatura são emitidos pela Direção Geral da Polícia, igualmente aos do DNI-e. O acesso ao certificado para assinaturas é gerado com a Chave Permanente do usuário, na modalidade de nível de segurança reforçada.

Para poder usar o sistema Cl@ve, é preciso que o cidadão tenha se inscrito e feito uma verificação prévia de sua identidade. Essa inscrição pode ser feita: i) presencialmente; ii) on-line com um certificado eletrônico e iii) on-line sem certificado, mas fornecendo uma informação conhecida somente pelo cidadão e pela Administração (essa última modalidade habilita apenas o acesso aos serviços que exigem um nível de segurança básico).

Embora o alcance inicial do sistema Cl@ve correspondesse ao âmbito da Administração nacional, onde seu uso é obrigatório, desde o início o sistema foi aberto para o restante das Administrações, que podiam utilizá-lo voluntariamente. Não obstante, essa situação mudou recentemente com a vigência da Lei do Procedimento Administrativo Comum das Administrações Públicas,[42] que exige que todas as Administrações Públicas espanholas aceitem os sistemas de identificação usados pela Administração do Estado.

---

41 Comparar com o caso da Estônia.

42 Lei nº 39/2015.

Esta Lei, junto com a Lei do Regime Jurídico do Setor Público,[43] conforma o novo marco legal para a atuação administrativa na Espanha e dá o impulso definitivo à administração eletrônica ao estabelecer que a atividade da Administração, tanto em suas relações internas como externas, deve ser digital.

As principais novidades da lei têm a ver com a clara separação da identificação e da assinatura, simplificando o uso de ambas, e a redução dos atos em que a assinatura se faz necessária. Além disso, a Lei está plenamente alinhada com o Regulamento europeu eIDAS,[44] que define o marco geral para a identificação eletrônica e os serviços de confiança digital na União Europeia, e destina-se a ser uma das referências fundamentais da identificação eletrônica no futuro.

Identificação no marco da União Europeia

O regulamento eIDAS consta de duas partes diferenciadas, sendo uma dedicada à identificação eletrônica transfronteiriça e outra aos serviços de confiança.

No que diz respeito à identificação eletrônica, embora o alcance do regulamento afete unicamente a identificação eletrônica transfronteiriça, seu impacto está sendo observado também em nível nacional, onde os Estados-membros estão alinhando suas estratégias nacionais de identificação eletrônica com as disposições do regulamento. Para tal, estão sendo implantados sistemas de identificação de alcance nacional e categorizando os sistemas de identificação e os serviços que fazem uso deles conforme os níveis de segurança marcados pelo regulamento; por sua vez, está sendo estudado como habilitar o acesso do setor privado a esses sistemas de identificação, já que o regulamento prevê seu uso de maneira opcional.

No que diz respeito aos serviços de confiança, o regulamento busca a criação de um mercado único, de maneira que os serviços de identificação oferecidos por um prestador localizado em qualquer país da União possam ser usados no restante dos países sem qualquer limitação. Dessa forma, pretende-se resolver os problemas causados pela Diretiva de Assinatura, cuja transposição a nível nacional foi realizada de maneira heterogênea, dando origem a uma falta de interoperabilidade dos sistemas de assinatura nacionais. Além da assinatura eletrônica, o regulamento inclui outros serviços que anteriormente não estavam regulados a nível europeu: i) os selos eletrônicos, (meio equivalente à assinatura para pessoas jurídicas); ii) os selos de tempo eletrônicos; iii) a entrega eletrônica certificada e iv) a autenticação de sites da internet. Por sua vez, em consonância com a Diretiva de Assinatura, distingue entre os serviços qualificados (aqueles sujeitos a uma supervisão mais estrita e que fornecem o nível máximo de garantias em sua prestação) e os não qualificados.

Uma menção especial deve ser feita à novidade que introduz o regulamento eIDAS em relação à assinatura no servidor: como a realizada pelo sistema Cl@veFirma, permite que tenha o mesmo valor que a incorporada no dispositivo e que, portanto, possa ser usada para realizar as assinaturas qualificadas. Com isso, busca-se eliminar as barreiras para a adoção generalizada desse tipo de solução, muito mais usáveis.

---

43 Lei nº 40/2015.

44 Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho que derroga a Diretiva 1999/93/CE.

Lições aprendidas

Uma das primeiras lições do caso espanhol é a importância de **separar a identificação e a assinatura eletrônica**. Como as primeiras experiências da implantação das infraestruturas de identificação eletrônica de caráter generalizado foram realizadas por meio de certificados eletrônicos, tende-se a considerar ambas de maneira conjunta. No entanto, embora costumem ocorrer no contexto de uma mesma transação, elas não impõem os mesmos requisitos nem exigem as mesmas tecnologias. Como a identificação e a autenticação são um processo mais simples que a assinatura, faz sentido que eles também se apoiem em mecanismos tecnológicos mais simplificados, sobretudo para o usuário.

Outra das lições que podem ser extraídas é a **importância de um marco legal adequado**, que garanta a validade legal das operações realizadas on-line, outorgue confiança suficiente para as partes que intervêm nas mesmas, impulsione a administração eletrônica e seja consistente com as práticas de identificação existentes no mundo físico, de forma que ambos os mundos, on-line e presencial, estejam alinhados. Por outro lado, deve-se levar em conta a identificação de pessoas jurídicas, que, em muitas ocasiões, são os principais usuários de serviços digitais. Isso implica estabelecer regras para a gestão de poderes e capacidades de representação das pessoas físicas que as representam.

A **neutralidade tecnológica** é outro dos princípios que se deve respeitar na hora de traçar o marco geral para a identificação eletrônica e os serviços de confiança, já que as tecnologias que os sustentam mudam rapidamente com o tempo. É por isso que é muito recomendável adotar um foco baseado nos resultados que se espera alcançar, mais do que nas tecnologias que serão utilizadas. Isso é, por exemplo, o que faz o regulamento eIDAS na hora de especificar os requisitos dos diferentes níveis de segurança na autenticação que prevê (básico, substancial e alto). A adoção de padrões, como a ISO/IEC 29115:2013 sobre o marco para a garantia da autenticação, ou o SAML 2.0, OpenID, Oauth para a federação de identidades, contribui também para minimizar o risco derivado da obsolescência tecnológica.

O **princípio da proporcionalidade** deve levar em conta no desenho de um marco global de identificação. Por via de regra, quanto maior a segurança de um mecanismo de identificação, mais difícil é utilizá-lo. É por isso que se deve buscar um compromisso entre segurança e usabilidade, exigindo um nível de segurança na autenticação que seja adequado à natureza do serviço e à informação em questão, o que implica uma avaliação dos riscos do sistema de informação. O mesmo ocorre com o uso da assinatura eletrônica, cuja complexidade motiva que somente se exija quando é necessário deixar a constância fiel da vontade do usuário.

Outra das lições aprendidas é a existência de diferentes perfis de usuário em função da idade, formação, ocupação profissional, conhecimento em tecnologias da informação e comunicações, frequência de uso dos meios digitais etc. Cada coletivo tem suas preferências em termos de meios de relação, por isso é uma boa prática **deixar o cidadão decidir** se quer se relacionar por meios eletrônicos e quais mecanismos usar. Nesse sentido, é relevante a experiência da Agência Tributária espanhola. Embora fosse possível acessar seus serviços eletrônicos identificando-se com um certificado eletrônico desde 1999, em 2010 observou-se que o patamar máximo foi atingido, de modo que planejou-se a habilitação de um novo mecanismo de acesso mais simples destinado a todos aqueles que não dispunham de certificados. Isso deu lugar aos serviços de confirmação do rascunho da declaração do imposto de renda e ao sistema de identificação Clave PIN, que aumentaram notavelmente o nível de tramitação eletrônica em relação ao que existia anteriormente.

Em relação à variedade de perfis, acaba sendo conveniente planejar também a oportunidade de estabelecer uma obrigação de se relacionar com a administração por meios exclusivamente eletrônicos para os grupos que dispõem de meios suficientes. No caso da Espanha, a lei 39/2015 estabelece essa obrigação para pessoas jurídicas, entidades sem personalidade jurídica, determinados grupos profissionais e funcionários públicos. A Dinamarca foi mais além e ampliou essa obrigação para todo o cidadão, assegurando a possibilidade de que aqueles que não contam com os meios ou conhecimentos para isso possam receber a assistência necessária.

Um aspecto relevante é também o **processo de registro dos usuários e de entrega da credencial**, já que o nível de segurança de um mecanismo de autenticação depende fortemente de tal processo. Nesse sentido, o registro assegura a vinculação entre a identidade física e a identidade digital, de modo que é muito importante a verificação da identidade que tem lugar nesse momento, que será mais segura enquanto forem usados os documentos e dados existentes nos registros oficiais. Geralmente, essa verificação adquire a máxima garantia legal quando realizada por uma entidade administrativa, o que lhe concede um grande valor, tanto para o setor público como para o setor privado. Além de um cenário de uso no qual o setor privado admite credenciais emitidas pelo setor público (como o DNI-e na Espanha), existe a possibilidade de cenários alternativos nos quais as credenciais emitidas pelo setor público são usadas como base de confiança para gerar credenciais próprias do setor privado.

Outro ponto também muito importante é a **definição do modelo de financiamento**, que deve ser sustentável. Para isso, é necessário estabelecer qual é a contribuição de cada ator ao financiamento do sistema. Deve-se levar em conta que, se o custo recair sobre o cidadão, a adoção pode ser prejudicada e, com isso, a demanda pelos serviços digitais também. Por outro lado, se o custo recair sobre o prestador do serviço eletrônico que usa o mecanismo de identificação, os obstáculos afetarão a incorporação deles ao sistema e a oferta de serviços que usam o mecanismo de identificação será freada. Também é possível que o financiamento seja realizado com os orçamentos do Estado. Evidentemente, existe a possibilidade de definir modelos mistos nos quais o sistema é financiado por contribuições de todas as partes.

Por outro lado, é importante considerar os custos não tão visíveis, como a infraestrutura para a distribuição de credenciais ou a integração dos serviços eletrônicos com o sistema de identificação. Por fim, deve-se prestar atenção especial à possível competência estabelecida entre o setor público e o setor privado em termos de provisão dos meios de identificação, já que a participação dos esquemas de identificação de caráter público pode distorcer a lógica de mercado. Nesse sentido, uma possível aproximação pode ser deixar que o setor público se encarregue exclusivamente pela identificação de caráter legal e para o setor privado a prestação de serviços de valor agregado vinculados a essa identificação, como podem ser a certificação de atributos adicionais, a incorporação de garantias adicionais ou a utilização de mecanismos mais convenientes e utilizáveis. No entanto, essa aproximação deve sempre se contrastar com o marco jurídico e a cultura existente em relação aos papéis que ambos os setores devem desempenhar.

Por fim, deve-se ter consciência da importância cada vez maior da **dimensão transfronteiriça da identificação eletrônica**. Com um comércio eletrônico que tem alcance global e com uma ameaça do crime cibernético também de caráter global, a necessidade de oferecer segurança para as transações eletrônicas que se produzem entre cidadãos e empresas de outros países é cada vez mais indispensável. Nesse sentido, a experiência da União Europeia com o regulamento eIDAS acaba sendo paradigmática, embora também seja relevante a iniciativa MobileConnect, um novo padrão de segurança impulsionado pela GSMA – associação internacional que agrupa mais de 800 operadores de telefonia móvel do mundo todo – que permite a autenticação nos serviços on-line somente com um número de celular para onde é enviado um código que o usuário deverá introduzir em seguida. Um marco adequado para a identificação eletrônica transfronteiriça simplifica as relações com os cidadãos e as empresas estrangeiras, aumenta a facilidade para fazer negócios no país e ajuda a atrair o talento de estudantes e trabalhadores.

Referências bibliográficas

Andrews, M., L. Prichett y M. Woolcock. 2012. “Escaping Capability Traps through Problem-Driven Iterative Adaptation (PDIA).” Center for Global Development. Documento de Trabalho nº 299. Disponível em: https://www.cgdev.org/publication/escaping-capability-traps-through-problem- driven-iterative-adaptation-pdia-working-paper.

AT&T. 2010. “AT&T Healthcare Community Online: On-Demand Identity Management.” Disponível em: http://www.corp.att.com/healthcare/docs/hco_identity_management.pdf.

Bitium. 2017. Lista de preços. Disponível em: https://www.bitium.com/site/pricing/.

Deloitte. 2016. “Picture Perfect: A Blueprint for Digital Identity.” Disponível em: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-blueprint-for-digital-identity.pdf.

Deloitte Access Economics. 2015. “Digital Government Transformation.” Deloitte Commissioned by Adobe. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte- au-economics-digital-government-transformation-230715.pdf.

DocuSign. 2017. Produtos e preços. Disponível em: https://www.docusign.com/products- and-pricing.

e-Estonia. Disponível em: https://e-estonia.com/e-residents/about/.

Electronic Identity (eID). 2015. “Application Guide: where, why, how.” Disponível em: https://eid.eesti.ee/index.php/EID_application_guide.

Fórum Econômico Mundial. 2016. A Blueprint for Digital Identity. Disponível em: http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf:

France Connect. s/f. Disponível em: https://franceconnect.gouv.fr/.

Kernaghan, K. 2012. “Transforming Local Public Services Using Technology and Digital Tools and Approaches.” Universidade de Brock.

Local Government Association. 2014. “Transforming Local Public Services.” Disponível em: https://www.local.gov.uk/sites/default/files/documents/transforming-public-servi-2a5.pdf.

Pareja, A., C. Fernández, B. Blanco, K. Theobald y A. Martínez. 2016. Simplificando vidas: qualidade e satisfação com os serviços públicos. Banco Interamericano de Desenvolvimento. Monografia nº 487. Disponível em: https://publications.iadb.org/handle/11319/7975.