PRINCÍPIOS DE IDENTIFICAÇÃO

PARA O DESENVOLVIMENTO SUSTENTÁVEL

PRINCÍPIOS DE IDENTIFICAÇÃO PARA O DESENVOLVIMENTO SUSTENTÁVEL:
RUMO À ERA DIGITAL

ORGANIZAÇÕES ENDOSSANTES

Agência Noroeguesa de Cooperação para o Desenvolvimento (Norad)

Banco Africano de Desenvolvimento

Banco Asiático de Desenvolvimento (ADB)

Centro para o Desenvolvimento Global (CGD)

Comissão Económica das Nações Unidas para África (ECA)

Digital Impact Aliance (DIAL)

Digital Nations

FHI 360

Fundação Bill & Melinda Gates (BMGF)

Fundo das Nações Unidas para a Infância (UNICEF)

Gabinete de Instituições Democráticas e Direitos Humanos da OSCE (ODIHR)

Grupo Banco Mundial

GSMA

ID4Africa

Mastercard

Omidyar Network

Open Identity Exchange Reino Unido/Europa

Organização dos Estados Americanos

Organização Internacional para as Migrações (IOM)

Plan International

Privacy and Consumer Advisory Group to the Government Digital Service e GOV.UK

Programa Alimentar Mundial da ONU

Programa das Nações Unidas para o Desenvolvimento (PNUD)

Smart Africa

Secure Identity Alliance (SIA)

United Nations Capital Development Fund (UNCDF)

UNHCR, A Agência da ONU para os Refugiados

União Internacional de Telecomunicações (UIT)

União Internacional do Notariado

Women in Identity

PRINCÍPIOS

INCLUSÃO

1. **Assegurar o acesso universal dos indivíduos, livre de discriminação.**
2. **Remover barreiras ao acesso e ao uso.**

CONCEÇÃO

3. **Estabelecer uma identidade fiável: única, segura e precisa.**
4. **Criar uma plataforma responsiva e interoperável.**
5. **Utilizar padrões abertos para evitar a dependência de fornecedores e tecnologias.**
6. **Proteger a privacidade e a autonomia pessoal na conceção do sistema.**
7. **Planear para a sustentabilidade financeira e operacional.**

GOVERNAÇÃO

8. **Proteger os dados pessoais, manter a segurança cibernética e proteger os direitos das pessoas por meio de um quadro legal e regulatório abrangente.**
9. **Estabelecer mandatos institucionais e procedimentos de responsabilização claros.**
10. **Assegurar a legalidade e a confiança por meio de mecanismos independentes de supervisão e resolução de reclamações.**

FINALIDADE

Cada pessoa tem o direito de participar plenamente na sua sociedade e economia e de ser reconhecida como uma pessoa perante a lei.[1] No entanto, cerca de mil milhões de pessoas em todo o mundo não têm meios de prova de sua identidade, o que é essencial para protegerem os seus direitos e os permitir terem acesso a serviços e oportunidades.[2] Muitos outros têm formas de identificação que são inseguras ou nas quais os prestadores de serviços não confiam. Alguns vivem em países em que os sistemas de identificação são fracos e inadequados para a era digital. Muitos países, ainda, falham na salvaguarda dos direitos e na proteção dos dados. Solucionar esta "lacuna de identificação", aumentar a cobertura, melhorar a qualidade e a governança dos sistemas de identificação que protegem os direitos e facilitam o acesso aos serviços é fundamental para a agenda do desenvolvimento.

As organizações que endossam estes Princípios estão empenhadas num conjunto de valores partilhados. Elas têm o objetivo de assegurar que os sistemas de identificação sejam inclusivos, protejam os dados e os direitos dos indivíduos, além de serem concebidos para apoiar o desenvolvimento sustentável.

Baseando-se nas normas internacionais existentes,[3] os Princípios foram desenvolvidos e publicados pela primeira vez em 2017 por um grupo de organizações comprometidas com o apoio ao desenvolvimento de sistemas de identificação inclusivos, fiáveis, transparentes, voltados para melhorar a vida das pessoas e a consecução dos Objetivos de Desenvolvimento Sustentável (ODS). Tendo em conta a rápida evolução do sector da identificação, os signatários originais dos Princípios comprometeram-se a revê-los para incorporar novas perspetivas e lições aprendidas. Esta segunda edição reflete as contribuições deste processo e de consultas públicas realizadas.

As organizações signatárias, no âmbito dos seus respectivos mandatos, políticas operacionais e regras, utilizam estes Princípios para promover um entendimento comum de questões chaves e boas práticas. Elas visam melhorar o alinhamento das partes interessadas, orientar decisões de apoio ou financiamento, além de facilitar as discussões a nível nacional, regional e global. Esse trabalho em conjunto pretende apoiar sistemas de identificação que promovam o desenvolvimento económico e social, além de proteger os direitos humanos, sem que ninguém fique para trás. Esperamos que um número cada vez maior de partes interessadas, incluindo governos, organizações intergovernamentais, parceiros de parceiros de desenvolvimento, sociedade civil, organizações não-governamentais e intervenientes do sector privado se juntem a nós no endosso aos Princípios e na sua implementação.

---

1 O direito ao reconhecimento perante a lei está consagrado no Artigo 6 da Declaração Universal dos Direitos Humanos (DUDH) e no Artigo 16 do Pacto Internacional dos Direitos Civis e Políticos (ICCPR). O direito ao registo de nascimento está consagrado em várias convenções internacionais, incluindo o Artigo 7 da Convenção sobre os Direitos da Criança (CDC).

2 As estimativas de 2018 da Base de Dados Global ID4D do Banco Mundial estão disponíveis em: http://id4d.worldbank.org/glo al-dataset

3 Isto inclui, entre outros, os Princípios e recomendações da ONU sobre o Registo Civil e Estatísticas Vitais (CRVS), normas internacionais sobre a proteção de dados (tais como o Regulamento Geral Europeu para a Proteção de Dados e a Convenção 108+ do Conselho da Europa), normas globais e regionais e quadros de confiança para a identificação, e os Princípios para o Desenvolvimento Digital.

Definições e escôpo

Estes Princípios destinam-se a ser aplicados de uma forma ampla à criação e utilização de sistemas de identificação[4] para fazer progredir os objetivos de desenvolvimento. Devido ao seu papel central na realização dos direitos individuais e na melhoria do acesso a serviços e direitos básicos no mundo físico e digital, **o foco dos Princípios está nos sistemas "oficiais" de identificação fornecidos por, em nome de, ou reconhecidos pelos governos.**[5]

Normalmente, cada país tem uma configuração única de seus sistemas de identificação oficiais, que podem variar muito nas suas finalidades, tecnologias, arquiteturas, usos, fornecedores e arranjos de governação. No entanto, esses sistemas podem ser categorizados como sistemas de identificação "legais" ou "funcionais". **Os sistemas de identificação legais** dão reconhecimento perante a lei e meio de prova de identidade legal. O nome e a natureza dos sistemas de identificação legais variam de acordo com a legislação nacional, mas normalmente incluem sistemas de registo civil, sistemas de identificação nacional, registos de população e outros sistemas básicos de identificação.[6] Os **sistemas de identificação funcionais** fornecem provas oficiais de identidade e autorização para fins ou sectores específicos. Incluem normalmente sistemas de identificação que fornecem identificação para eleitores, cartões de racionamento, números da previdência social, cartões de saúde, números de identificação fiscal e muito mais; nalguns casos essas credenciais também podem ser reconhecidas como prova de identidade para outros fins ou sectores.[7]

Dada a esmagadora tendência para a digitalização das economias e das sociedades, os Princípios refletem a natureza cada vez mais digital dos sistemas oficiais de identificação. Por exemplo, muitos fornecem credenciais e serviços digitais oficiais (como IDs móveis, certificados digitais, assinaturas eletrónicas, etc.) que permitem uma autenticação automática e remota para acesso a serviços e direitos, tanto presencialmente, quanto online. Nalguns casos, os governos construíram eles próprios esses sistemas. Noutros casos, os países desenvolveram ecossistemas de fornecedores de identidade digital que contam com sistemas oficiais de identificação existentes para a comprovação da identidade e o registo. Num modelo de ecossistema federado, por exemplo, diversas entidades públicas e/ou privadas operam dentro de um quadro de confiança, podendo emitir credenciais de identidade digital reconhecidas oficialmente. As arquiteturas e normas de identidade descentralizadas emergentes também estão a criar possibilidades de armazenar e verificar credenciais digitais oficiais em dispositivos pessoais.

Para o resto deste documento, o termo "sistema de identificação" é utilizado para se referir tanto as versões analógicas quanto digitais dos sistemas de identificação oficiais acima descritos.

---

4 Em termos mais gerais, os sistemas de identificação recolhem e validam dados de identidade através de um processo de registo, fornecendo em seguida credenciais às pessoas, tais como certificados, cartões ou outros documentos de identidade, que estas podem utilizar para se autenticarem ou verificarem atributos de identidade específicos perante terceiros que necessitem de confiar nas suas reivindicações ou atributos de identidade.

5 Os sistemas de identificação reconhecidos pelos governos são ativados e seguem o quadro legal de um país, e baseiam-se num processo de prova de identidade que envolve a validação do titular através de credenciais emitidas pelo governo e/ou registos de fonte autorizada, como sistemas de registo civil, sistemas de identificação nacional ou registos de população.

6 Os governos mantêm a responsabilidade final pela identificação legal (ver, por exemplo, a Definição Operacional Oficial de Identidade Legal da ONU, Resolução ECOSOC E/CN.3/2020/15). Embora uma prova de identidade legal, especialmente o registo de nascimento e/ou de casamento, seja frequentemente um requisito para adquirir uma nacionalidade, a identificação legal não tem necessariamente de estar ligada à nacionalidade e não deve ser equiparada a um estatuto legal ou nacional. Embora alguns sistemas de identificação legal (por exemplo, sistemas de identificação nacionais) exijam ou constituam uma prova de nacionalidade, o mesmo não acontece com outros.

7 No caso dos solicitantes de asilo e dos refugiados, embora os estados anfitriões sejam os principais responsáveis por fornecer provas de identidade legal aos refugiados que não tenham documentos de viagem válidos, as credenciais emitidas pela Agência das Nações Unidas para os Refugiados sob seu mandato em nome do estado anfitrião podem ser reconhecidas como prova de identidade legal ou oficial (Convenção sobre o Estatuto dos Refugiados de 1951, Artigos 25 e 27); Estatuto do Alto Comissariado das Nações Unidas para os Refugiados de 1950).

Por que a identificação é importante para o desenvolvimento

Para as pessoas, a identificação é um direito, um instrumento de proteção e uma porta de acesso a serviços, benefícios e oportunidades.

A importância da identificação para os direitos das pessoas e para o desenvolvimento foi reconhecida pela comunidade internacional com a adoção do Objetivo de Desenvolvimento Sustentável (ODS) 16.9: "até 2030, fornecer uma identidade legal para todos, incluindo o registo de nascimento." O direito a uma identidade desde a nascença, como garantido no Artigo 7 e 8 da Convenção sobre os Direitos da Criança (CDC), e a ser reconhecido como uma pessoa perante a lei são os primeiros passos fundamentais para assegurar a proteção ao longo da vida, sendo um direito que garante outros direitos. Uma identidade legal é a base sobre a qual as crianças ganham uma nacionalidade, evitam o risco de serem apátridas e são protegidas contra a violência e a exploração. Por exemplo, a prova de idade é necessária para ajudar a evitar o trabalho infantil, o casamento infantil e o recrutamento de menores de idade em conflitos armados.

Além disso, ter uma forma oficial de provar a própria identidade pode ser exigido para muitas interações formais, transações e serviços em todo o sector público e privado. Por exemplo, a verificação da identidade de uma pessoa com base numa credencial ou registo oficial é frequentemente exigida para abrir uma conta bancária, votar numa eleição, obter um emprego formal, adquirir uma nacionalidade, matricular-se na escola, inscrever-se num seguro de saúde, receber uma transferência social, comprar um cartão SIM, registar bens, atravessar fronteiras, ou procurar uma reparação legal. A aceleração para os serviços online e a transformação digital entre governos e empresas significa que as pessoas também precisam cada vez mais de um meio seguro e acessível para provarem a sua identidade na Internet.[8]

É fundamental que os governos, intervenientes do sector privado e outras partes interessadas sejam capazes de identificar pessoas de uma forma fiável ou verificar certos atributos para poderem fornecer programas e serviços de forma eficiente, eficaz e responsável.

A capacidade de saber quem as pessoas são é essencial para diversas atividades governamentais, entre elas a implementação de programas sociais, garantindo que os benefícios sejam recebidos pelas pessoas corretas; a resposta em situações de emergência, desastres naturais e epidemias, situações que exigem respostas rápidas; cobrar impostos; reduzir fraudes nos salários dos funcionários públicos; a gestão de migrantes de forma segura e organizada; além disso, no caso do registo civil, a produção de estatísticas vitais para o planeamento e monitorização do desenvolvimento. Para certas entidades privadas é necessário verificar a identidade dos clientes

8 Por estas razões, a identificação é um fator chave para a identificação de diversas metas dos Objetivos de Desenvolvimento Sustentável, para além da 16.9, incluindo a 1.3 (implementar sistemas de proteção social), 1.4 (assegurar que os pobres e vulneráveis tenham controlo sobre a terra, a propriedade e os ativos financeiros), 5a (dar às mulheres pobres igualdade de acesso aos recursos económicos, incluindo as finanças), 5b (melhorar a utilização da tecnologia, incluindo as TIC para promover a capacitação das mulheres), 8.10 (acesso universal à banca, seguros e serviços financeiros), 10.7 (migração e mobilidade segura e responsável), 10c (reduzir o custo das transferências de remessas), 12c (eliminar gradualmente os subsídios aos combustíveis nocivos), 16a (reforçar a capacidade de combater o terrorismo e o crime), 16.5 (reduzir a corrupção) e muitas outras.

com segurança para acesso à alguns serviços, tais como a abertura ou autorização de acesso a uma conta. Desta forma, é possível mitigar riscos, proteger os clientes contra fraudes, roubo de identidade, além de cumprir a "due diligence" do cliente (CDD), os requisitos do Know Your Customer (KYC) e outros regulamentos. Quando os sistemas de identificação fornecem mecanismos digitais para os indivíduos se autenticarem on-line, estes são também fatores importantes que contribuem para uma economia digital inclusiva e sustentam as plataformas digitais, serviços eletrônicos e sistemas de pagamento digitais.[9]

Quando concebidos e utilizados adequadamente, os sistemas de identificação têm o potencial de ajudar os países a acelerar o desenvolvimento inclusivo.

Isto inclui melhorar a governação e a prestação de serviços, aumentar a inclusão financeira, reduzir as desigualdades de género através da capacitação das mulheres e raparigas e aumentar o acesso aos serviços de saúde e redes de segurança social para as pessoas que vivem na pobreza. Em comparação com os registos em papel, a adoção de tecnologias digitais tem o potencial de aumentar a precisão e a fiabilidade dos dados e credenciais de identidade, automatizar processos para economizar recursos, aumentar a conveniência e fornecer novas plataformas para inovações na prestação de serviços. Embora existam riscos, a digitalização também apresenta a oportunidade de projetar intencionalmente sistemas de identificação para que sejam mais inclusivo, intuitivos e protejam os dados das pessoas. Isso pode ser alcançado com a elaboração de novas normas, adoção de modelos e ferramentas que permitam a supervisão pelos indivíduos sobre como os seus dados estão sendo utilizados.

---

9 Ver, por exemplo, FATF. 2020. Guidance on Digital Identity. Financial Action Task Force (FATF), Paris; Banco Mundial. 2018. "Private Sector Economic Impacts from Identification Systems." Washington, DC; Gelb, A., e Metz, A. 2018. *Identification Revolution: Can Digital ID Be Harnessed for Development?* Washington, DC. Center for Global Development; Gelb, A., e Clark, J. 2013. "Identification for Development: The Biometrics Revolution," *Center for Global Development Working Paper 315*.

Por que desenvolver "bons" sistemas de identificação é essencial para mitigar os riscos

Apesar das oportunidades que surgem com a melhoria da identificação, sistemas de identificação mal implementados ou utilizados de forma inadequada podem criar diversos riscos que afetam principalmente grupos desfavorecidos e que as tecnologias digitais podem ampliar.

Os principais riscos estão relacionados com a exclusão ou discriminação, a proteção da privacidade e dos dados pessoais, além de sistemas mal concebidos ou que funcionam de forma deficiente e oferencem poucos benefícios. Os grupos vulneráveis e marginalizados são muitas vezes os menos propensos a ter provas da sua identidade, mas também os que mais necessitam de proteção e dos serviços associados à identificação.[10] As pessoas que não conseguem obter ou utilizar a identificação estão sujeitas, portanto, a um risco maior de ficarem para trás quando é necessário satisfazer requisitos de identificação rigorosos para ter acesso aos serviços. Sem medidas de mitigação proactivas, novos sistemas de identificação podem reforçar ou perpetuar desigualdades, práticas discriminatórias e preconceitos estruturais existentes. Tal como acontece com outros sistemas que processam dados pessoais, os sistemas de identificação também podem prejudicar os direitos de privacidade e proteção de dados pessoais quando não existem de leis e regulamentos, supervisão e controlos e salvaguardas técnicas adequados. Violações de dados, vigilância e tratamento de dados não autorizados, fraudes relacionadas com a identidade e o desvio de finalidade podem acarretar em sérios riscos para as pessoas, especialmente para os grupos mais vulneráveis. Além disso, os sistemas de identificação são frequentemente construídos com uma abordagem "top-down" e com pouca transparência. Juntamente com más práticas de aquisição e escolhas de conceção que inflacionam os custos e criam dependência de fornecedores ou tecnologias, isso pode resultar em sistemas que são operacional ou financeiramente insustentáveis e que não servem as necessidades das pessoas ou os objetivos de desenvolvimento.

Embora estejam presentes em qualquer sistema de identificação, esses riscos podem ser ampliados pela digitalização. Com as tecnologias digitais, a escala e os potenciais danos da má gestão ou da utilização indevida de dados pessoais são muito maiores do que com os sistemas baseados em papel. Do mesmo modo, a adoção de tecnologias que dependem da conectividade à Internet e de dispositivos caros tem o potencial de ampliar a exclusão digital e criar novos obstáculos para que grupos já marginalizados obtenham ou utilizem a identificação de uma forma fiável. A velocidade da inovação também pode criar incentivos para que haja a tendência de obter a mais recente tecnologia, em vez de construir sistemas que sejam adequados para os fins atuais e com a flexibilidade necessária para a adaptação as necessidades futuras. Além disso, mesmo se os sistemas de identificação forem automatizados com sucesso, é improvável que atinjam o seu potencial sem uma digitalização completa, transformando e repensando processos para o meio digital, e investimentos complementares em conectividade à Internet, serviços online, plataformas de pagamento e outros sistemas digitais.

---

10 Os grupos específicos em maior risco de serem excluídos pelos sistemas de identificação variam de acordo com o contexto, mas incluem frequentemente pessoas que vivem na pobreza, mulheres e crianças, populações migrantes, refugiados e solicitantes de asilo, residentes remotos e rurais, minorias étnicas, linguísticas ou religiosas, minorias sexuais e de género, pessoas com deficiência, deslocados internos, apátridas, pessoas afetadas por conflitos, trabalhadores do sector informal e outros grupos marginalizados ou minoritários. Ver, por exemplo, Banco Mundial. 2019. *Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Findex Survey*, Washington, DC: Grupo Banco Mundial.

Para aproveitar os benefícios dos sistemas de identificação na era digital, esses riscos devem ser abordados de forma proactiva, abrangente e contínua pelas partes interessadas.

A construção de um sistema de identificação que satisfaça as metas de desenvolvimento exige uma abordagem multifacetada na qual intervenham múltiplas partes interessadas. Para isto é necessário definir claramente os objetivos e os usos autorizados para o sistema; a adoção de quadros legais e regulatórios adequados, que proporcionem as salvaguardas e supervisão; a implementação de políticas e práticas inclusivas para a adoção e utilização dos sistemas de identificação; aplicar a conceção e avaliação de riscos, com um enfoque centrado nas pessoas e que proteja a privacidade e os dados pessoais; escolher tecnologias adequadas ao contexto, equitativas e acessíveis que assegurem a qualidade, a segurança e a utilidade do sistema no momento atual e no futuro. O envolvimento contínuo e transparente com o público e um conjunto diversificado de partes interessadas ao longo destes processos é essencial para fomentar a confiança e a responsabilização, e assegurar que os sistemas de identificação sejam construídos para serem úteis às pessoas e para apoiar os resultados do desenvolvimento sustentável.

Principais partes interessadas e seus papéis

Na prática, a aplicação dos Princípios exige um esforço coordenado e sustentado de múltiplas partes interessadas que desempenham papéis essenciais no fornecimento, utilização, supervisão e financiamento de sistemas de identificação:

- **Indivíduos.** As pessoas são o centro dos sistemas de identificação, tanto como os titulares dos dados desses sistemas, quanto como os seus utilizadores finais, que dependem da identificação para protegerem e reivindicarem os seus direitos e para acederem aos serviços. Eles têm o direito de conhecer e exercer uma supervisão e controlo adequados sobre como, e com que finalidade, os seus dados pessoais são recolhidos, utilizados, armazenados, partilhados e qualquer outra forma tratamento realizado por entidades públicas e privadas. É essencial compreender e atender às necessidades e preocupações das pesssoas em relação aos sistemas de identificação, proteger seus dados pessoais e sua privacidade, além de assegurar a sua participação na conceção e implementação dos sistemas de identificação que afetam suas vidas.

- **Governos.** As agências governamentais nacionais e locais são normalmente os fornecedores de identidade para sistemas de identificação legal, por exemplo, registo civil e estatísticas vitais (RCEV), sistemas de identificação nacional, registos de população, credenciais de identificação básicas, etc., assim como muitos sistemas funcionais, tais como identificação de eleitores, identificadores fiscais e cartas de condução. Outras agências governamentais e prestadores de serviços confiam frequentemente nestes sistemas e os utilizam para identificar ou autenticar as pessoas com quem interagem ou que servem. As instituições governamentais, incluindo os órgãos legislativos e órgãos de supervisão, também desempenham um papel fundamental na criação e aplicação de quadros legais e regulatórios que permitam e salvaguardem os sistemas de identificação fornecidos tanto pelo sector público como pelo privado. Finalmente, as agências governamentais estão normalmente envolvidas no estabelecimento de normas e no desenvolvimento e supervisão de quadros de confiança e garantia para os fornecedores de serviços de identidade, as partes que neles confiam e outras partes interessadas em ecossistemas de identidade digital centralizados, federados ou descentralizados.

- **Sector privado.** As empresas privadas são desenvolvedores, inovadores e fornecedores de componentes e infraestruturas de sistemas de identificação, também podem ser provedores de serviços de verificação e autenticação de identidade. Muitas empresas privadas também dependem de sistemas de identificação legais ou outros para verificar ou autenticar a identidade dos seus clientes (por exemplo, para abrir contas bancárias ou de dinheiro para dispositivos móveis). Nalguns casos, entidades do sector privado são provedores de identidade dentro de um ecossistema federado ou descentralizado que utiliza credenciais emitidas pelo governo e registos de fontes autorizadas (por exemplo, registos civis e sistemas nacionais de identificação) para criar credenciais digitais ou serviços de autenticação que são aceites para serviços online do governo (e do sector privado).

- **Organizações não-governamentais, comunitárias e da sociedade civil.** Organizações não-governamentais (ONGs), a sociedade civil e organizações comunitárias (OSC e OBC) podem desempenhar um papel vital na conceção e implementação de sistemas de identificação, inclusive por meio de assistência jurídica, conscientização, realização de consultas públicas e capacitação das pessoas para que tenham acesso a meios de identificação ou reparação de denúncias, exigindo que os provedores de serviços de identidade prestem contas de suas atividades.

- **Organizações internacionais, órgãos regionais e parceiros de desenvolvimento.** Órgãos intergovernamentais internacionais, agências de desenvolvimento e humanitárias, fundações e outros doadores apoiam financeiramente, provêem assistência técnica ou o estabelecimento de marcos regulatórios para sistemas de identificação. Outros organismos internacionais e regionais também estão envolvidos no estabelecimento de normas relacionadas com a identificação, incluindo as relativas à interoperabilidade transfronteiriça e ao reconhecimento mútuo de credenciais. Em certos casos, os intervenientes no desenvolvimento humanitário também podem ser fornecedores de identidade ou administrar sistemas de identificação para programas ou atividades específicas. No caso dos refugiados e solicitantes de asilo, o Alto Comissariado das Nações Unidas para Refugiados pode fornecer provas de identidade legal ou oficial em nome do estado anfitrião sob o seu mandato.

PRINCÍPIOS

INCLUSÃO

1 Assegurar o acesso universal dos indivíduos, livre de discriminação.

- *Identidade legal para todos.* Todos devem ser capazes de provar a sua identidade legal. Os países devem cumprir as suas obrigações e compromissos para fornecer identificação legal a todos os seus residentes,[11] não apenas aos seus cidadãos,[12] desde o nascimento até à sua morte, conforme refletido nas leis internacionais e nacionais.[13] Isto inclui a obrigação do registo de nascimento universal para todas as crianças,[14] o que é essencial para a prova da identidade legal desde o nascimento, e o registo atempado de outros eventos vitais, tais como casamentos e morte. Além disso, deve-se respeitar as obrigações e compromissos de fornecer uma prova de identidade legal aos refugiados, apátridas e migrantes que não tenham uma credencial válida ou não possam provar a sua identidade legal de outro modo.

- *Não discriminação.* Todos os sistemas de identificação devem estar livres de discriminação nas suas políticas, nas práticas e desde a sua conceção. Isto inclui assegurar que os quadros legais, os requisitos e procedimentos para registar, obter ou utilizar a identificação, e os dados recolhidos ou apresentados nas credenciais não permitem ou reforçam a discriminação contra determinados grupos, tais como aqueles que enfrentam maiores riscos de exclusão por razões culturais, políticas, económicas ou outras. Entre esses grupos, incluem-se pessoas que vivem na pobreza, mulheres, crianças, populações rurais, minorias raciais, étnicas, linguísticas, religiosas, pessoas com deficiência, minorias sexuais e de género, migrantes, solicitantes de asilo, refugiados, deslocados à força, apátridas, entre outros. Além disso, os sistemas e os dados de identificação nunca devem ser utilizados como um instrumento de discriminação ou para infringir ou negar direitos individuais ou coletivos.

---

11 Embora os estados tenham o direito soberano de determinar a elegibilidade para a cidadania e emitir as provas de cidadania de acordo com o direito internacional, também têm a obrigação de fornecer provas de identidade legal, ou reconhecer a identificação legal emitida por outro estado ou organização internacional, a todas as pessoas residentes no seu território, incluindo o registo de nascimento. Por exemplo, a Convenção sobre o Estatuto dos Refugiados de 1951, Artigo 27 estabelece que os estados "emitirão documentos de identidade a qualquer refugiado no seu território que não possua um documento de viagem válido", e uma disposição semelhante para apátridas está contida na Convenção sobre o Estatuto dos Apátridas de 1954, Artigo 27. Fornecer a todos uma prova de identidade legal é fundamental para a evitar a situação de apátrida (ver www.unhcr.org/ibelong).

12 Os estados devem fornecer uma prova de cidadania a todas as pessoas que a ela tenham direito, sem qualquer tipo de discriminação.

13 A obrigação dos estados de fornecerem uma prova de identidade legal não significa necessariamente que a inscrição nos sistemas de identificação deva ser legalmente obrigatória.

14 Por exemplo, o Artigo 7 da Convenção sobre os Direitos da Criança (CDC) estabelece: "A criança deve ser registada imediatamente após o nascimento e tem direito, desde o nascimento, a um nome, ao direito de adquirir uma nacionalidade e, na medida do possível, o direito de conhecer e ser cuidada pelos seus pais". A CDC foi ratificada por todos os Estados Membros da ONU, com exceção dos Estados Unidos, que assinaram mas não ratificaram o tratado. Na prática, porém, praticamente todos os nascimentos nos Estados Unidos são devidamente registados.

2 Remover barreiras ao acesso e ao uso.

- *Custos diretos e indiretos.* Os custos para o indivíduo nunca devem ser uma barreira para obter as credenciais de identidade necessárias para cumprir direitos ou aceder aos serviços ou usufruir de direitos básicos. Por exemplo, o registo civil e a emissão inicial de certidões de nascimento e de óbito, assim como outras credenciais de identidade legal devem ser gratuitos para o indivíduo. Se forem cobradas taxas por certos serviços adicionais (tais como a reemissão de credenciais perdidas), as taxas devem ser razoáveis, proporcionais aos custos incorridos e devem ser transparentes para o público. Os custos indiretos da obtenção de identificação, incluindo as taxas para documentos de apoio, custos de viagem e procedimentos administrativos complicados, também devem ser minimizados.

- *Assimetrias da informação.* As partes interessadas devem trabalhar para reduzir as barreiras e as disparidades das informações e do conhecimento que possam impedir que indivíduos, tais como minorias linguísticas, pessoas com baixos níveis de alfabetização, pessoas com deficiência e outras, acedam ou utilizem a identificação e promovam uma cultura de confiança e responsabilização, aumentando a alfabetização e a sensibilização em torno do sistema. As campanhas de informação e educação e outros materiais devem ser inclusivas e acessíveis para garantir que todos tenham o conhecimento, as capacidades e as ferramentas necessárias para participar do sistema de identificação e exercer os seus direitos de supervisão e controlo.

- *Lacunas na tecnologia.* Embora a tecnologia seja um habilitador chave dos sistemas de identificação, a ninguém deve ser negada a identificação ou serviços e direitos associados por falta de conectividade móvel ou à Internet, dispositivos eletrónicos, alfabetização digital ou competências digitais, o conforto ou a capacidade de utilizar determinada tecnologia, ou devido a preconceitos ou falhas tecnológicas. As partes interessadas devem, por isso, trabalhar em conjunto para garantir que os serviços de identificação e de autenticação estejam disponíveis para todos, independentemente dos recursos, competências e conectividade digital. Além disso, são necessários mecanismos acessíveis de processamento de exceções e de reparação de reclamações para evitar a recusa de serviços ou direitos e em caso de dificuldades técnicas.

- *Inclusão desde a conceção.* Os sistemas de identificação devem dar prioridade às necessidades e abordar as preocupações dos grupos marginalizados e vulneráveis que estão em maior risco de exclusão e que mais necessitam das proteções e benefícios que a identificação pode oferecer. Isso exige trabalhar com as comunidades para identificar proactivamente as barreiras legais, processuais, sociais e económicas enfrentadas por grupos específicos, riscos e impactos específicos a esses grupos, e adotar tecnologias e medidas de mitigação adequadas para garantir que os sistemas de identificação novos ou atualizados não reforcem ou aprofundem as desigualdades existentes.

CONCEÇÃO

3 Estabelecer uma identidade fiável: única, segura e precisa.

- *Unicidade.* Um sistema de identificação fornece um mecanismo para estabelecer e autenticar uma identidade única quando, dentro desse sistema, cada pessoa tem apenas uma identidade e não há duas pessoas com a mesma identidade. A exclusividade é particularmente importante dentro dos sistemas legais de identificação e outros que suportam casos de utilização que exigem altos níveis de segurança,[15] tais como nas eleições e nos sistemas de pagamento de benefícios governo para pessoas (G2P). Mais importante, a exclusividade *dentro* de um dado sistema *não* implica que apenas deve existir um único fornecedor ou sistema de identidade ou um identificador único e permanente (por exemplo, um número de ID exclusivo) utilizado para todas a finalidades num país ou jurisdição.

- *Segurança.* Os sistemas de identificação devem ter salvaguardas adequadas e eficazes contra o acesso não autorizado, adulteração (alteração ou outras modificações não autorizadas dos dados ou credenciais), roubo de identidade, utilização indevida de dados, crimes cibernéticos e outras ameaças que possam ocorrer ao longo do ciclo de vida da identificação. Os dados devem ser protegidos quando armazenados e em trânsito, inclusive quando as pessoas utilizam as suas credenciais ou dispositivos pessoais. As medidas de segurança devem incluir sistemas de sensibilização para a utilização segura do sistema e para notificar as pessoas em caso de violação de dados, assim como possibilidades de recurso para identidades que tenham sido roubadas ou comprometidas e que necessitem serem reemitidas.

- *Precisão.* Garantir que os dados de identidade sejam exatos e atualizados é um dos princípios centrais da proteção de dados e um direito das pessoas, também é essencial para a fiabilidade do sistema. Os sistemas de identificação devem ser concebidos de modo a garantirem uma recolha de dados exata e devem ter procedimentos fáceis de utilizar para que as pessoas possam ver e atualizar os seus dados e corrigir erros para garantir a sua precisão ao longo do tempo.

---

15 De um modo geral, um "nível de garantia" (LOA) representa o grau de confiança que um determinado sistema de identificação ou credencial fornece a um terceiro de que uma identidade reivindicada por uma pessoa ou entidade é realmente a sua identidade "verdadeira". Isso é função de múltiplos fatores, incluindo a força do processo de prova de identidade quando as pessoas estão inscritas num sistema de identificação e recebem credenciais (o nível de garantia de identidade ou IAL), a força do processo e da tecnologia de autenticação (nível de garantia de autenticação ou AAL) e, se for utilizado um modelo federado, protocolo de asserção utilizado pela federação para comunicar a autenticação e atribuir informações (nível de garantia da federação ou FAL) (adaptado de NIST 800-63:2017).

4 Criar uma plataforma responsiva e interoperável.

- *Necessidades dos utilizadores.* Os serviços de identificação e autenticação devem ser concebidos para satisfazer as necessidades e preocupações reais das pessoas. Além disso, devem ser flexíveis, escaláveis e úteis para as entidades públicas e do sector privado que confiam neles para identificação ou autenticação. Isto exige uma ampla consulta às partes interessadas e uma aprovação participativa e centrada nas pessoas, incluindo a sociedade civil, o público em geral, os prestadores de serviços e outras partes interessadas, começando com o processo de conceção e continuando durante toda a implementação.

- *Interoperabilidade.* Sujeito às leis e regulamentos sobre partilha de dados e salvaguardas técnicas apropriadas, incluindo os princípios de "privacidade desde a conceção", a capacidade dos sistemas de identificação de comunicarem com outros sistemas (por exemplo, sistemas de registo civil e prestadores de serviços) e trocar dados ou informações facilita os serviços como verificação ou atestados de identidade, eKYC, outras formas de partilha de dados autorizadas e o reconhecimento mútuo de sistemas de identificação estrangeiros.[16]

5 Utilizar padrões abertos para evitar a dependência de fornecedores e tecnologias.

- *Padrões abertos.* As conceções baseados em padrões abertos permitem a livre concorrência e inovação.[17] Os padrões abertos são essenciais para uma maior eficiência, melhor funcionalidade e adaptabilidade dos sistemas de identificação, tanto dentro dos países como além-fronteiras.

- *Evitar a dependência de fornecedores e tecnologias.* Bons processos de aquisição facilitam a concorrência, promovem a inovação e impedem o "bloqueio" por tecnologias e fornecedores, o que pode aumentar os custos e reduzir a flexibilidade para aceitar as alterações necessárias ao longo do tempo. Os processos de aquisição devem realçar a relação custo-benefício, economia, integridade, adequação à finalidade, eficiência, transparência e justiça. Uma gestão eficaz dos contratos assegurará que estes benefícios sejam sustentados ao longo da implementação.

16 A interoperabilidade com sistemas estrangeiros pode facilitar a migração e o comércio, mas devem ser implementados controlos para proteger a segurança de grupos vulneráveis, como refugiados, cujos dados pessoais devem muitas vezes ser protegidos do seu país de origem.

17 Por exemplo, a ISO/IEC desenvolveu normas que cobrem muitos aspetos dos sistemas de identificação. Para mais detalhes, ver Banco Mundial. 2016. "Technical Standards for Digital Identity Systems: Formulating a Strategic Approach."

6 Proteger a privacidade e a autonomia pessoal na conceção do sistema.

- *Uma perspectiva da privacidade desde a conceção.* Os sistemas de identificação devem ser concebidos para dar prioridade para a proteção dos dados e a privacidade como a configuração standard sem exigir qualquer ação especial adicional por parte de qualquer indivíduo. Os dados pessoais, incluindo quaisquer dados que estejam ligados ou possam ser ligados a um indivíduo, devem ser protegidos contra uma utilização indevida de forma proactiva e por falha, por meio de um quadro legal e regulatório robusto, da conceção do próprio sistema e adoção de normas técnicas e controlos operacionais.[18]

- *Princípios para a proteção de dados na prática.* A conceção, as políticas e as tecnologias utilizadas pelos sistemas de identificação devem estar em conformidade com as normas globais de proteção de dados, incluindo a minimização da recolha dos dados, a proporcionalidade da sua utilização, especificação da sua finalidade, processamento legal, limites estritos de retenção dos dados, exatidão, segurança, responsabilidade e transparência, entre outros.[19] Por exemplo, os sistemas de identificação devem limitar a recolha e exposição dos dados, especialmente de informações pessoais sensíveis,[20] incluindo nas credenciais e na estrutura dos números de identificação. Os protocolos de autenticação devem revelar apenas os dados mínimos necessários para garantir níveis de garantia adequados e reter os dados apenas durante o tempo necessário para as finalidades para as quais os dados podem ser utilizados legalmente, ou para as quais foi dado o consentimento. Esses níveis e o método de autenticação devem refletir uma avaliação do nível de risco nas transações e devem, de preferência, basear-se em normas internacionais reconhecidas.[21] As regras e políticas para os dados devem ser transparentes e disponibilizadas às pessoas num formato de fácil utilização para lhes facilitar o conhecimento dos seus direitos e dos processos disponíveis para exercer o controlo ou supervisão dos seus dados.

---

18 Para saber mais sobre a abordagem à "privacidade através da conceção", ver, por exemplo, Cavoukian, A. 2011. "Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices." https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

19 Os exemplos de normas mais normalmente mencionadas incluem as Práticas de Informação Justas (FIP), as Diretrizes de privacidade da OCDE, o Regulamento geral de proteção de dados da UE, os Princípios da ONU sobre privacidade e proteção de dados e a Convenção 108+, entre outros.

20 O conceito de "Informações pessoais confidenciais" pode variar de acordo com o contexto, mas geralmente estas incluem dados que podem ser utilizados para criar identidades fraudulentas e/ou para criar perfis ou visar indivíduos. Estão incluídos dados biométricos e números de identificação, como números de identidade permanentes ou exclusivos (UIN), assim como atributos como religião, etnia, casta, afiliação política e assim por diante. A divulgação de informações de identificação pode envolver riscos particularmente graves para certas pessoas, por exemplo, solicitantes de asilo e refugiados. Assim, são aplicáveis considerações específicas aos sistemas de identificação utilizados principalmente ou exclusivamente para fins humanitários, particularmente em ambientes afetados por conflito, violência e fragilidades. Ver, por exemplo, "Política para o Processamento de Dados Biométricos pelo CICV" do Comité Internacional da Cruz Vermelha". 2019. Disponível em: https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf, e o ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action, 2ª Edição, 2020.

21 Essas avaliações de impacto do risco devem ser feitas pela entidade responsável que cria, recolhe, partilha ou utiliza dados para fins de autenticação e identificação ligados ao caso de utilização específico. Exemplos de normas existentes para níveis de garantia para comprovação da identidade incluem a ISO/IEC 29115 e as emitidas pelo eIDAS, o Gabinete do Governo do Reino Unido, o Instituto Nacional de Normas e Tecnologia dos EUA (NIST) e outros.

7 Planear para a sustentabilidade financeira e operacional.

- *Sustentabilidade.* Os sistemas de identificação devem ser concebidos para terem uma sustentabilidade fiscal e operacional a longo prazo. Isto exige uma abordagem transparente e baseada em resultados para assegurar que o sistema seja adequado à finalidade e fazer escolhas técnicas e de gestão sustentáveis, e a adoção de modelos de negócio que garantam a longevidade do sistema sem comprometer outros Princípios. As taxas aplicadas pela utilização dos serviços de identificação podem criar barreiras ao acesso, à inclusão para indivíduos e a sua adoção por prestadores de serviços Os esforços para recuperar os custos através de ganhos de eficiência e redução de fraudes também devem ponderar as metas de economia fiscal em relação ao potencial de aumento dos erros de exclusão. Os sistemas de identificação devem ser projetados para incentivar elevados padrões de desempenho para todas as partes envolvidas.

GOVERNAÇÃO

8 Proteger os dados pessoais, manter a segurança cibernética e proteger os direitos das pessoas por meio de um quadro legal e regulatório abrangente.

- *Quadro legal e regulatório.* Os sistemas de identificação devem ser sustentados por quadros legais e regulatórios legitimados, abrangentes e baseados em políticas que promovam a confiança no sistema, garantam a proteção e a privacidade dos dados (incluindo a segurança informática), limitem os abusos como a vigilância não autorizada em violação do devido processo legal, estejam livres de discriminação e promovam a inclusão, particularmente para grupos vulneráveis ou marginalizados, além de assegurar a responsabilização. Os quadros legais devem ser claros na definição de responsabilidade e recursos disponíveis para os indivíduos e devem ser supervisionados por entidades reguladoras independentes com poderes apropriados e um financiamento consistente. Devem também proteger as pessoas contra o acesso e utilização inadequada dos seus dados para vigilância indevida ou estabelecimento ilegal de perfis. Os quadros exigem que haja um equilíbrio entre modelos regulatórios e autorregulatórios que não sufoque a concorrência, a inovação ou o investimento. São também necessários quadros legais e regulatórios adequados para a interoperabilidade transfronteiriça ou o reconhecimento mútuo.[22]

- *Direitos dos titulares dos dados.* Os serviços de identificação devem proporcionar às pessoas uma escolha genuína e um controlo sobre a recolha e utilização dos seus dados, incluindo a capacidade de revelar seletivamente apenas os atributos necessários para uma determinada transação. As pessoas devem contar com meios simples para corrigir gratuitamente dados errados e obter uma cópia de seus dados. Os dados pessoais não devem ser utilizados para outras finalidades, sem o consentimento da pessoa, a não ser que tal seja exigido ou autorizado por lei (por exemplo, como necessário e proporcional).[23] Os fornecedores de serviços de identidade e outras partes interessadas devem ser transparentes na gestão da identidade, desenvolver recursos apropriados para aumentar a consciência das pessoas sobre como os seus dados serão utilizados, e fornecer-lhes ferramentas acessíveis e fáceis de utilizar para gerirem os seus dados, dar um consentimento livre e esclarecido e processar reclamações. Os fornecedores de serviços de identidade devem garantir que o processo inicial para corrigir erros seja administrativo e não judicial, a fim de aumentar a velocidade de resolução e reduzir os custos. Os acordos de partilha de dados também devem ser transparentes e totalmente documentados.

---

22 Por exemplo, deve ser dada uma consideração especial a solicitantes de asilo e refugiados; ver *Advisory Opinion on the Rules of Confidentiality Regarding Asylum Information* da UNHCR em https://www.refworld.org/docid/42b9190e4.html

23 Ver, por exemplo, Convenção 108+, Artigos 5, 10, e 11.

9 Estabelecer mandatos institucionais e procedimentos de responsabilização claros.

- *Responsabilidades institucionais.* A legislação, os regulamentos e o quadro de confiança devem estabelecer e regular acordos de governação abrangentes para sistemas e fornecedores de serviços identificação a nível interno e, se aplicável, a nível internacional. Isso deve incluir a especificação dos termos e condições que regem as relações institucionais entre as partes participantes, para que os direitos e responsabilidades de cada um sejam claros para todos.
- *Responsabilização.* Deve haver uma clara responsabilização e transparência em torno dos papéis e responsabilidades de todas as entidades envolvidas na construção, operação, gestão e supervisão dos sistemas de identificação.

10 Assegurar a legalidade e a confiança por meio de mecanismos independentes de supervisão e resolução de reclamações.

- *Supervisão.* A utilização de sistemas de identificação deve ser monitorizada (quanto à sua eficiência, transparência, exclusão, utilização indevida, etc.) para assegurar que todas as partes interessadas cumpram as leis aplicáveis, utilizem adequadamente os sistemas de identificação para cumprir os seus objetivos, monitorizam e respondem a potenciais violações de dados, e recebem queixas ou preocupações dos indivíduos relativamente ao processamento dos dados pessoais. Os reguladores devem dispor de recursos e poderes suficientes para cumprirem as suas responsabilidades estatutárias.

- *Adjudicação.* Os litígios relativos à identificação e utilização de dados pessoais, como por exemplo, a recusa de registar uma pessoa ou de corrigir dados, ou uma determinação desfavorável do estatuto jurídico de uma pessoa, que não sejam resolvidos de forma satisfatória pelos provedores de identidade devem ser objeto de uma análise rápida e com custos reduzidos por parte de autoridades administrativas e judiciais independentes com autoridade para proporcionar uma reparação adequada sem acrescentar barreiras para o indivíduo.

Crédito das fotografias | Capa Superior: UN Women/Fatma Elzahraa Yassin, Meio: iStock.com/hadynyah, Inferior: iStock.com/borchee; Página 7: UNICEF/BANA2012-02020/Jannatul Mawa; Página 9: iStock.com/ Bartosz Hadyniak; Página 11: Sébastien Rieussec/Safran; Página 15: UN MediaJashim Salam.

REPUBLIQUE DE COTE D'IVOIRE

ETAT CIVIL

CIRCONSCRIPTION D'ETAT CIVIL

de TEAPLEU

CENTRE

de BEALE

N° du Registre 24 DU 18/2/2001

NAISSANCE DE

DIOMANDE

NOEL

BEROLE

/

EXTRAIT

du Registre des actes de l'Etat Civil
pour l'année 2001

Le QUATORZE FEVRIER DEUX MIL UN /.

est né DIOMANDE NOEL BEROLE /.

à BOPLEU

Fils de DIOMANDE NIHOUA GERARD /.

Nationalité

et de DIOMANDE OLINSE CHANTAL /.

Nationalité

MENTIONS (éventuellement) : NEANT

Marié le à /

Avec

Mariage dissous par décision de divorce en date du à /

Décédé le /

Certifié le présent extrait conforme aux indications portées au registre

Délivré à TEAPLEU le 23 NOVEMBRE 2009

L'officier de l'Etat Civil

D 05 957 551

OCMOE ESSON
Administrateur Civil

ORGANIZAÇÕES ENDOSSANTES

Empowered lives.
Resilient nations.

Convidamos outras organizações a também endossarem estes Princípios

Fevereiro de 2021