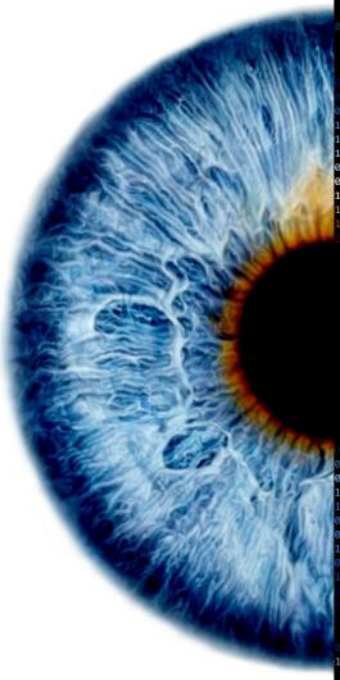
PRIVACIDADE BRASIL



Políticas de identidade e dados pessoais

Índia | Brasil
México | Quênia
Estônia | **Reino Unido**

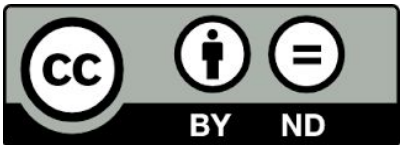
Políticas de Identidade e Dados Pessoais.

Índia, México, Estônia, Quênia, Reino Unido e Brasil

Julho - 2017

Autoras: Margareth Kang e Maria Luciano

Ilustração: Rafael Viana



01 de julho de 2017.

Sumário

Sumário Executivo

O presente relatório pretende analisar as políticas de identificação única e as razões do aparente aumento dessas no mundo. Para isso, foram selecionados países de diferentes continentes, sendo eles: Brasil, Índia, Reino Unido, Estônia, México e Quênia. A escolha desses países também buscou uma variedade quanto aos modelos criticados e aplaudidos, e modelos implementados ou não.

Diante da vasta gama de análises possíveis, foi adotada a perspectiva da privacidade e da proteção de dados pessoais, no intuito de averiguar como essa temática se relaciona às políticas de identificação única, e como os países abordam esse direito na implementação de suas políticas de identidade.

INTRODUÇÃO

O problema da identificação tornou-se particularmente desafiador com o avanço das novas tecnologias de comunicação na sociedade de informação. *Online,* as preocupações em torno da identificação, segurança e acesso à rede são crescentes. Dentre elas, destacamos o uso indevido de informações pessoais por atores mal-intencionados; a ausência de mecanismos eficientes para garantir segurança e confiança nas relações online; e o potencial de vigilância provenientes do acesso a esses dados.

As políticas de identidade são fonte essencial de informação na formulação e implementação de políticas públicas, complementando o censo[1] e outros instrumentos convencionais de coleta de informações pessoais e demográficas. A

[1] A respeito da necessidade de complementação do censo, é interessante apontar suas várias dificuldades. Primeiramente, eles são caros. Em segundo lugar, em parte por seu custo, os censos tendem a ser tomados com pouca frequência. Assim, no momento em que um censo subsequente é realizado, os dados do censo mais antigo estarão muito desatualizados e podem até estar desatualizados quando forem lançados pela primeira vez após o processamento. Além disso, o censo pode nem sempre fazer as perguntas que são mais importantes para a formulação de políticas.

identificação para o indivíduo é indispensável para assegurar o acesso a oportunidades educacionais, serviços financeiros, benefícios de saúde e de assistência social, desenvolvimento econômico, bem como a participação eleitoral. Nesse sentido, é evidente o interesse dos governos em políticas de identidade que os munam com dados específicos de cada um dos seus cidadãos.

1. IDENTIDADE E POLÍTICAS PÚBLICAS

"Identidade" é um conceito subjetivo e nebuloso. Cada um de nós reúne características pessoais e psicológicas, traços físicos, experiências de vida e preferências próprias. Essas identidades desempenham papéis fundamentais em nossa sociedade. Algumas delas - como nacionalidade, gênero e renda - são relevantes para o desenvolvimento socioeconômico de um país.

A identificação legal é um direito humano[2] do qual 1,5 bilhão de pessoas no mundo não usufruem[3]. Sem ela, o indivíduo está vulnerável a exploração e abusos, não tem acesso a serviços essenciais, pode ser marginalizado e ficar tecnologicamente invisível. Assim, a identificação legal confere uma identidade civil ao cidadão, tornando-o titular de direitos e deveres. A certificação da identidade de uma pessoa é mais que uma conveniência: é requisito para participar plenamente da sociedade e exercer seus direitos.

A identificação nacional trata das relações do indivíduo para além da Administração Pública, no ambiente entre-Estados, ao passo que o registro civil trata das relações do indivíduo com a Administração Pública, empresas e outras pessoas. Assim, o registro civil constitui uma forma de autenticação[4] da identidade legal. No

[2] Art. 15º da Declaração Universal de Direitos Humanos. Nesse documento, "cidadania" e "nacionalidade" são usados indistintamente.
[3] WORLD BANK. Identification for Development – Strategic Framework. Washington, DC: World Bank, 2016. Disponível em < http://pubdocs.worldbank.org/en/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf>.
[4] "A identificação é um processo pelo qual a identidade de alguém é revelada ("Este é João"), enquanto a autenticação é um processo que resulta em uma pessoa sendo aceita como autorizada a participar ou realizar alguma atividade ('Eu estou autorizado a retirar dinheiro desta conta bancária', ou 'Sou velho o suficiente para comprar álcool')".WHITLEY, Edgar A., HOSEIN, Gus. *Global Challenges for Identity Policies*. Palgrave Macmillan, UK, 2010, p.02.

Brasil, o registro civil de pessoas naturais configura um repositório de atos e fatos que impactam a vida civil dos cidadãos, quais sejam nascimentos, casamentos, óbitos, emancipações, interdições, sentenças declaratórias de ausência, opções de nacionalidade e as sentenças que deferem a legitimação adotiva[5]. O foco principal do registro civil tem sido fornecer a cada cidadão uma identidade legal. Embora esta seja uma atividade crucial para o setor público e um direito fundamental dos cidadãos, as estatísticas agregadas que podem emergir desses eventos individuais são úteis para entender mudanças sociais, bem como diferenças entre as diversas áreas de um mesmo país. Nesse sentido, essas informações podem ser extremamente úteis para a formulação de políticas públicas.

A gestão da identidade (*identity management*) também é importante para facilitar a mobilidade internacional. Os governos recolhem quantidades consideráveis de informações pessoais de cidadãos e visitantes e emitem documentos de identificação para facilitar viagens, com base em normas e tecnologias internacionalmente acordadas.

Contudo, a coleta e agregação de dados sobre os indivíduos merece atenção. De um lado, há o risco de uso indevido dessas informações - notadamente sua comercialização, um mercado crescente[6]. De outro lado, essas informações conferem ao Estado maior capacidade de investigação, expandindo o instrumental de vigilância estatal, com implicações na privacidade dos cidadãos. Por essas razões, regimes robustos de proteção à privacidade e dados pessoais são condição à implementação de políticas de identidade.

2. IDENTIDADES E NOVAS TECNOLOGIAS

No universo das novas tecnologias, parece que observamos uma aproximação entre a pessoa e seus dados identificadores. Foto e assinatura não

[5] BRASIL. Lei Nº 6.015 / 1973. Art. 29.
[6] El País. Seus dados são vendidos por 7,5 centavos de dólar. Disponível em <http://brasil.elpais.com/brasil/2017/05/03/tecnologia/1493835469_309268.html>.

bastam, a prova da identificação e a credibilidade dessa se apoiam com mais frequência e intensidade em dados biométricos únicos. Assim, impressão digital, reconhecimento facial e leitor de íris são algumas das tecnologias que têm ganhado cada vez mais espaço no dia a dia dos cidadãos.

Por dados biométricos entende-se aqueles capazes de identificar uma pessoa, incluindo: dados morfológicos (impressão digital, íris, face, voz, formato das mãos etc), biológicos (sangue e DNA), e comportamentais (postura, modo de andar, velocidade e intensidade na escrita e digitação, etc).

Se por um lado essa variada gama de dados biométricos sempre existiu, os limites tecnológicos não permitiam a utilização dos mesmos em larga escala. Atualmente, no entanto, a identificação por meio da biometria está presente com naturalidade nos diversos espaços da vida de um indivíduo, como por exemplo: para acessar as funcionalidades do telefone celular, realizar transações bancárias, entrar em estabelecimentos, entre outros.

Verifica-se, entretanto, que essas tecnologias necessitam de aprimoramento. Recentemente, um grupo hacker alemão (Chaos computer club) conseguiu, em menos de um mês do lançamento do Galaxy S8 da Samsung, enganar o dispositivo de reconhecimento de íris através de um olho artificial[7]. Lembrando que o mesmo Galaxy S8 teve sua funcionalidade de reconhecimento facial hackeada antes mesmo do lançamento. Mas essa divulgação de vulnerabilidade é apenas uma das muitas outras que já foram anunciadas na mídia, como: o caso da Ministra de Defesa da Alemanha Úrsula Von Der Leyen, que teve as suas digitais copiadas a partir de fotos divulgadas inclusive pela imprensa oficial[8]; e o acesso ao Iphone 5 a partir de uma

[7] Esse olho teria sido fabricado a partir de uma impressora e uma lente de contato, com informações disponíveis na foto de perfil da rede social de uma pessoa. The Guardian. Samsung Galaxy S8 iris scanner fooled by German hackers. 2017. Disponível em: < https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security>.

[8] The Guardian. Hackers fakes German Minister´s fingerprints using fotos of her hands. 2014. Disponível em: < https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands >.

impressão digital copiada[9].

A utilização de dados biométricos como alternativa para o reconhecimento pessoal não é passível de crítica por si só - aliás, como já delineado, mesmo em menor escala, elas existem há muito tempo. No entanto, os avanços tecnológicos permitem hoje maior capacidade e eficiência na agregação, armazenamento e gerenciamento dos dados pessoais, inclusive os biométricos. Atualmente, um telefone celular tem o potencial de reconhecer seu proprietário pela face, íris e digital, além de conhecer todas as localizações por onde passou, e armazenar outras informações, que se combinadas e mal utilizadas, podem ser extremamente lesivas ao indivíduo.

A. Biometria - Tecnologia Neutra ou Discriminatória?

O sistema de biometria opera com frações aceitáveis ou não de incompatibilidades, ou seja, por probabilidade, auferindo resultados através de cálculos estatísticos. Por esse motivo, um indivíduo de óculos de sol pode ser identificado através da face, por exemplo. Ressalta-se que ao desenvolvedor do sistema cabe estabelecer e implementar as taxas de erro do seu sistema, o que resulta em uma diferença na precisão entre os sistemas de reconhecimento biométrico. Assim, por utilizar os critérios de análise, e fazer uso de uma base de dados selecionada, à discricionariedade de cada desenvolvedor, fica evidente que a concepção do reconhecimento biométrico como uma tecnologia completamente neutra não é uma verdade por completo.

Sendo assim, os algorítmos implantados nesses sistemas podem estar enviesados inclusive inconscientemente por dados que estão na sua base ou por critérios nele implantados, daí a possibilidade de discriminação. Ao falarmos de reconhecimento facial, por exemplo, a história do filme em cores nos indica a construção de um modelo centrado no homem branco. Apesar dos avanços consideráveis nessa área, verifica-se que a discriminação proveniente da construção

[9] The Guardian. Iphone 5S fingerprint sensor hacked by Germany´s Chaos Computer Club. 2013. Disponível em: < https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked >.

e evolução tecnológica ainda existe.[10]

No Quênia, por exemplo, a existência de uma determinada política de identidade favoreceu a discriminação. Com a "segunda geração" de carteiras de identidade em 1995, implementou-se um processo de solicitação do documento que favorece a discriminação de membros de comunidades marginalizadas. Esse exame de admissibilidade ("*vetting*") consiste em um processo formal de entrevistas e comitês de avaliação em que agentes públicos solicitam, arbitrariamente, quaisquer outros documentos para a concessão da carteira[11]. As diversas fases desse procedimento facilitam atrasos, corrupção e arbitrariedades, culminando com a não concessão do documento a membros de algumas comunidades.

B. Dos Documentos de Identificação

Os documentos de identificação são largamente utilizados para identificar e autenticar o indivíduo. "Tradicionalmente, a ligação entre um documento de identidade e seu usuário era assegurada por um selo, assinatura feita à mão, e uma foto padrão".[12]

Mas a pressão para a criação de novos sistemas de identificação foi intensificada no final do século XX, pautados por três razões principais: a) a justificativa de eficiência administrativa; b) a demanda de setores não governamentais, como o comércio e os bancos, por sistemas confiáveis de identificação dos indivíduos; e c) pelos imperativos da segurança nacional presente nos Estados-Nação contemporâneos, e intensificados após o ataque de 11 de setembro de 2001.[13] Ademais, em termos administrativos, com a crescente digitalização da burocracia governamental, os documentos de identidade eletrônicos de e-government (e-IDs) ganham espaço como um "importante facilitador para o

[10] VOX. Color film was built for white people. Here's what it did to dark skin.The unfortunate history of racial bias in photography. 18 de setembro de 2015. Disponível em: < https://www.youtube.com/watch?v=d16LNHIEJzs>

[11] Oppenheim, Ben; Powell, Brenna Marea. *Legal Identity in the 2030 Agenda for Sustainable Development: Lessons from Kibera, Kenya*. Open Society Foundations, 2015.

[12] MEINTS, Martin. Gasson, Mark. The Future of Identity in the Information Society. Challenges and Opportunities. Springer. 2009. p. 177.

[13] LYON, David. BENNET, Colin J. Playing the ID card. Understanding the Significance of Identity Card Systems. Routledge 2008. New York. p. 10.

governo eletrônico”[14] na autenticação e identificação dos indivíduos.

Nem toda identificação única pressupõe a implantação de um documento, já que a adoção de um número único e de um cartão de identificação carrega em si um atributo cultural. Enquanto para alguns países portar mandatoriamente documentos de identificação é parte da interação diária nas relações do indivíduo com a sociedade, como é o caso do Brasil; para outros, não é um padrão cultural fazê-lo.

C. Da Centralização dos Dados Pessoais

A política de identificação única pressupõe a unificação das informações em um banco de dados único ou na inter-relação dos bancos de dados de diversos órgãos e setores através de um número único. Se por um lado esse cenário pode trazer maior eficiência na gestão da administração pública, por outro expõe a privacidade e os dados pessoais do indivíduo a maiores riscos. Lembrando que os bancos de dados espalhados pelos diversos órgãos da administração pública atraem interesses não só do setor privado como também dos próprios órgãos governamentais.

No setor público, o erro na identificação de um indivíduo pode acarretar cerceamento de direitos, e garantias como: o não recebimento de uma assistência social devida, a limitação da participação política, a imposição de penalidades de forma errônea, entre outros.

No que tange ao armazenamento desses dados, cabe uma reflexão sobre como os dados biométricos são armazenados no setor privado e, principalmente, no setor público. Diferentemente de uma senha, que pode ser guardada em segredo, e, se corrompida, pode-se criar uma nova, os dados biométricos são públicos, estando em constante exposição, além de serem de difícil alteração. Afinal, mudar a face, os olhos, ou as mãos, de um indivíduo não é tão banal.

Mas parece que a utilização dos dados biométricos é um caminho sem volta,

[14] MEINTS, Martin. Gasson, Mark. The Future of Identity in the Information Society. Challenges and Opportunities. Springer. 2009. pg. 176.

e está presente com cada vez mais naturalidade na sociedade. Por exemplo, um dos equipamentos mais frequentemente utilizados na captação de dados biométricos são as câmeras de segurança (CCTV). O aumento da utilização desses equipamentos tem várias razões, como: o barateamento de equipamentos e sistemas, combate à criminalidade, defesa de ataques terroristas, controle de ambientes, entre outros.

O uso disseminado dessa ferramenta já denota a naturalidade do convívio entre câmeras de segurança e indivíduo, assim como tem ocorrido com os leitores biométricos atualmente. Alguns países, como a Coréia do Sul, reconhecendo a ameaça que a indevida utilização desses sistemas pode trazer às pessoas, trazem disposição especial em matéria de utilização das câmeras de segurança e as imagens por elas coletadas[15]. Tal regulamentação da limitação do uso do CCTV nos indica que a coleta e utilização de dados biométricos por outros meios também pode ser regulada, auxiliando a garantia da privacidade dos indivíduos e aumentando o controle e segurança das tecnologias utilizadas.

Por essas razões, limites são necessários quanto: à agregação dos dados em uma única base, ao relacionamento das diversas bases através de um número único, ao acesso e alteração do banco de dados, entre outros. Políticas públicas que se apoiam em uma identidade única, com uso da biometria como certificação, precisam considerar os efeitos que a tecnologia pode trazer na vida de uma pessoa, e da sociedade como um todo. Para isso, os princípios de proteção de dados pessoais, como legalidade, finalidade, necessidade, transparência, segurança, coleta mínima e acesso, devem ser usados como instrumento de medida na construção, implementação e gerência da identificação única.

[15] A Lei de proteção de dados da Coreia do Sul - PIPA (Personal Information Protection Act - 2011) trata em especial sobre as câmeras de segurança, incluindo as imagens dela provenientes, no rol de dados pessoais. Ademais, possui regulamentações específicas que estabelecem limites para as instalações desses câmeras em ambientes privados, não permitindo sua instalação por mera liberalidade do proprietário do estabelecimento.

3. ANÁLISE DE PAÍSES

A. Índia

Em 2009 foi criada a Autoridade de Identificação Única da Índia (UIDAI)[16], com a atribuição de implementar um esquema de identificação único (UID), bem como operar e manter sua base de dados[17]. Para tanto, a UIDAI lançou o Aadhaar, um programa de identificação indiano em que os residentes acima de 5 anos de idade recebem um número único de identificação de 12 dígitos (UID), ao qual são associadas informações biométricas - digitais, scan facial e de íris[18]. Seu objetivo é fornecer um UID que possa ser autenticado e verificado online[19] – o Repositório Central de Informações de Identificação (Central Identification Data Repository) é armazenado em nuvem. Inicialmente, o programa era destinado à identificação de pessoas de baixa renda, visando combater fraudes em programas de assistência social e tornando-os mais eficientes. Mais tarde, foi expandido de forma a cobrir toda a população[20].

O Aadhaar foi lançado por um decreto executivo em 2009[21], e desde então tem sido implementado sem uma estrutura normativa. Em 2010 foi proposto o *Aadhaar Bill 2010*, mas este fora rejeitado pelo Parlamento por não endereçar

[16] A UIDAI é um gabinete que integra a Comissão de Planejamento (Planning Commission), criada em 1950 e encarregada da formulação, execução e acompanhamento dos planos quinquenais.
[17] Notificação No. A.03011/02/2009-Adm. I, publicada na Parte I, Seção II do The Gazette of India. Disponível em <https://uidai.gov.in/images/notification_28_jan_2009.pdf>.
[18] International Telecomunication Union. Review of National Identity Programs, 2016, p. 23.
[19] Existem 246 Agências de Autenticação de Usuários na Índia, tanto públicas como privadas. Ao realizar suas atividades, essas Agências auxiliam na certificação da identidade do indivíduo, por exemplo, quando algum órgão ou empresa realiza um pedido de autenticação antes de conceder um empréstimo ou benefício. The Centre of Internet & Society. Why experts worry about Aadhaar-based authentication, 2016. Disponível em < http://cis-india.org/internet-governance/news/bangalore-citizen-matters-august-2-2016-akshatha-why-experts-are-worried-about-aadhaar-based-authentication >.
[20] Quando a UIDAI foi criada já havia outro programa de identificação denominado Registro Nacional da População (National Population Register - NPR), conduzido pelo Ministério de Home Affairs. Esse programa tinha a segurança nacional e o estabelecimento da cidadania como motivações. Em 2011, decidiu-se que tanto o Aadhaar como o NPR iriam coletar dados biométricos, mas o fariam em estados diferentes. Em 2014, contudo, a coleta dos dados biométricos passou a ser exercida exclusivamente pelo Aadhaar – ao NPR caberia colher dados não biométricos e relacioná-los ao UID correspondente.
[21]Notificação No. A.03011/02/2009-Adm. I, publicada na Parte I, Seção II do The Gazette of India. Disponível em <https://uidai.gov.in/images/notification_28_jan_2009.pdf>.

questões como segurança e privacidade de dados. Em 2016, um novo projeto de lei, o *Aadhaar Bill 2016*, foi aprovado, culminando no *Aadhaar Act 2016*[22]. Este último, contudo, não traz em seu texto a data de início de sua vigência, motivo pelo qual o Aadhaar Act segue inaplicável, sendo o decreto executivo a regulação principal sobre o tema.

A obrigatoriedade do UID é ponto controverso no debate sobre o Aadhaar. Há alguns anos órgãos públicos têm utilizado o UID como condição, dentre outros, à concessão de auxílios socioeconômicos, ao pagamento de salários, à abertura de contas bancárias e ao registro de imóveis. Diante disso, em 2013, a Suprema Corte emitiu uma ordem (Order of Sept. 23, 2013[23]) em que dispunha sobre o caráter facultativo do Aadhaar, argumentando que "ninguém deve sofrer por não ter o cartão Aadhaar, ainda que alguma autoridade tenha expedido circular tornando-o obrigatório". Contudo, o Aadhaar Act 2016 parece contrariar essa ordem. Em sua seção 7, o documento dispõe que "um indivíduo deve ser autenticado ou comprovar seu número Aadhaar para estabelecer sua identidade" "como condição para o recebimento de subsídio, benefício ou serviço"[24].

Outro ponto bastante discutido sobre o Aadhaar é seu regime de proteção de dados pessoais. Na legislação indiana a definição de "privacidade" se faz presente

[22] O Aadhaar Act 2016 foi aprovado como uma money bill ("lei financeira"), o que tem gerado críticas. De acordo com o art. 110 (1) da Constituição da Índia, uma money bill deve endereçar apenas os seguintes temas: taxas, obrigações financeiras do Governo da Índia ou transações financeiras que envolvam o Fundo Consolidado da Índia. Argumenta-se que o Aadhaar Act faz referência a benefícios e serviços financiados pelo Fundo Consolidado da Índia – cuja maior eficiência é a motivação central do programa. Contudo, o objetivo principal do Act é garantir a obtenção de um número de identificação único, de modo que o Act não configuraria hipótese de money bill. Outra crítica deve-se ao fato de que uma money bill só pode ser apresentada na Lok Sabha (câmara baixa do Parlamento), deixando a Rajya Sabha (câmara alta do Parlamento) à margem de sua tramitação. É dizer, o Aadhaar Act 2016, em razão do seu formato de "money bill", teve um trâmite mais simples, tendo sido discutido e aprovado somente da câmara baixa do Parlamento

[23] Disponível em <http://judis.nic.in/temp/494201232392013p.txt>.

[24] "7. The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment: Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service". A Lei do Aadhaar, contudo, não estabelece as hipóteses em que o número não será concedido - parece haver, nesse ponto, uma atuação demasiadamente discricionária do UIDAI.

na Constituição da Índia 1949: “nenhuma pessoa deve ser privada de sua vida ou liberdade pessoal” exceto por procedimento previsto em lei (art. 21). A partir disso a jurisprudência da Suprema Corte vem delineando e estabelecendo os casos em que esse conceito de “privacidade” se aplica.

Na Índia, a lei que regula a proteção de dados pessoais é o Information Technology Act 2000. A definição de dados pessoais no sistema jurídico indiano é estabelecida pela Notificação G.S.R. 313(E) do Ministério das Comunicações e Tecnologia da Informação de 2011: dados pessoais são informações sobre uma pessoa natural que, direta ou indiretamente, juntamente com outras informações disponíveis, são capazes de identificar tal pessoa (2,(1), (i)). Dados sensíveis, por sua vez, referem-se a senhas; informações financeiras; condições de saúde física, mental e psicológica; orientação sexual; histórico médico e informações biométricas (seção 3 da mesma Notificação). Essas definições são utilizadas no Aadhaar Act[25].

O Information Technology Act 2000 define “sistema seguro” como hardware, software e procedimentos que sejam razoavelmente protegidos de mau uso e acesso indesejado, confiáveis e apropriados para as funções que devem desempenhar, e que tenham aderido a procedimentos de segurança amplamente aceitos.

De acordo com a cláusula 3(2) do Aadhaar Act, à época da solicitação do UID, deve-se informar ao cidadão a maneira como seus dados serão utilizados, a natureza daqueles que terão acesso a seus dados durante a autenticação, e informações procedimentais para pedido de acesso a esses dados pelo próprio cidadão. Nos termos da cláusula 29, nenhum dado biométrico poderá ser compartilhado nem utilizado para outros fins (que não a geração de números Aadhaar ou sua autenticação). Contudo, a cláusula 33 prevê a possibilidade de compartilhamento de dados pessoais mediante ordem judicial ou tendo em vista “interesse de segurança nacional”, expressão não definida. Ainda, não existe previsão de notificação dos cidadãos em caso de vazamento dos dados, de

[25] Para comparação das redações do Aadhaar Bill 2010 e do Aadhaar Act (antigo Aadhaar Bill 2016), ver “The Centre of Internet & Society. A comparison of the 2016 Aadhaar Bill, and the 2010 NIDAI Bill” disponível em < http://cis-india.org/internet-governance/blog/a-comparison-of-the-2016-aadhaar-bill-and-the-2010-nidai-bill>.

compartilhamento com terceiros[26] ou de mudança no uso dos dados fornecidos, e a alteração dos dados pelo próprio cidadão depende de autorização da UIDAI (cláusula 31 (1)).

Assim, verificou-se que o Aadhar Act, apesar de aprovado, não se encontra em vigência, dado a inexistência da data de implementação da lei. Por conta disso, o Aadhaar tem obedecido aos termos do Decreto executivo de 2009, e às decisões da Suprema Corte Indiana. A temática da privacidade e proteção de dados pessoais: a) foi motivo de rejeição do projeto de lei do Aadhaar, versão 2010, b) não constou no decreto executivo de 2009, e c) esteve presente na lei do Aadhaar 2016, em consonância com a lei de proteção de dados pessoais da Índia (Information Technology Act 2000). Assim, no que tange à privacidade e proteção de dados pessoais, os dados sobre o Aadhaar obedecem a regulação da lei de proteção de dados.

Ademais, ressalta-se que o Aadhaar possui uma complexa estrutura de gerenciamento de dados pessoais. Da coleta, ao armazenamento final dos dados, as informações passam por diversas entidades públicas e privadas que conjuntamente formam a estrutura de gerenciamento do Aadhaar. Desse modo, sua base de dados pode ser acessada por diversos atores, cuja permissão de acesso reside apenas na discricionariedade do UIDAI.

B. Reino Unido

A ideia de uma política nacional de identidade voltou a debate no Reino Unido após os ataques terroristas de 11 de setembro de 2001[27]. O Partido Trabalhista

[26] Em ordem de 2014 (Order of 24th March, 2014), a Suprema Corte negou a concessão de dados de um indivíduo, pela UIDAI, a autoridades de Goa para facilitar investigação criminal sem seu consentimento escrito.

[27] Esse debate não era novo no Reino Unido. Cartões de identidade nacional foram adotados durante a Segunda Guerra Mundial como parte da segurança nacional, para encontrar inimigos e espiões. Em 1952 seu uso foi suspenso – era desnecessário em tempos de paz. Conf. SULLIVAN, Claire. The United Kingdom Identity Cards Act 2006 – Proving Identity? e LONDON SCHOOL OF ECONOMICS. The Identity Project: an Assessment of the UK Identity Cards Bill and its Implications. Há quem indique, ainda, outra experiência do tipo, o primeiro registro nacional entre 1915-1919. Conf. AGAR, Jon. Identity cards in Britain: past experience and policy implications disponível em

apresentou a iniciativa como mecanismo de combate ao terrorismo, à fraude em benefícios sociais e ao trabalho ilegal[28]. Em consulta pública realizada entre 2002 e 2003, das 7.000 respostas 5.000 foram contra a implementação desse tipo de política[29]. Apesar disso, com a aprovação do Identity Cards Act 2006, instituiu-se "um esquema nacional para registro de indivíduos e emissão de cartões capaz de identificar indivíduos registrados", o Esquema de Identidade Nacional (National Identity Scheme - NIS).

O núcleo do NIS não era o cartão de identidade nacional, mas o Registro de Identidade Nacional (National Identity Register - NIR), um banco de dados centralizado da população com dados de residentes do Reino Unido maiores de 16 anos[30]. Um cartão de identidade só seria emitido depois que os dados fossem inseridos no NIR. O acesso a esses dados se daria através de um número único atribuído a cada indivíduo, o Número de Registro de Identidade Nacional (National Identity Registration Number). A construção e manutenção do NIR eram competências do Secretário de Estado (Seção 1 (1) do Act). Tanto o Número como o Registro seriam usados por uma variedade de órgãos e organizações públicos e privados.

O processo de inscrição no NIR era composto de duas etapas. A primeira etapa era a verificação biográfica, na qual informações sobre a vida do indivíduo eram comparadas com informações que os setores público e privado tivessem registradas sobre ele por meio de entrevistas. A segunda etapa era a verificação biométrica, na qual os dados biométricos do indivíduo eram comparados com os

<http://www.historyandpolicy.org/policy-papers/papers/identity-cards-in-britain-past-experience-and-policy-implications>.

[28] Essas motivações ficam evidentes na definição de *interesse público* adotada no Identity Card Act: "Seção 1(4) - For the purposes of this Act something is necessary in the public interest if, and only if, it is (a) in the interests of national security; (b) for the purposes of the prevention or detection of crime; (c) for the purposes of the enforcement of immigration controls; (d) for the purposes of the enforcement of prohibitions on unauthorized working or employment; or (e) for the purpose of securing the efficient and effective provision of public services".

[29] BBC. Timeline: ID Cards. 2010. Disponível em < http://www.bbc.com/news/10164331>.

[30] A implementação se daria da seguinte forma: a partir de 2008/9 os residentes do Reino Unido maiores de 16 anos poderiam registrar-se no NIR; até 2010 qualquer pessoa que solicitasse um passaporte teria seus dados inseridos no NIR, mas o cartão de identidade seria facultativo. A abordagem que seria adotada a partir de 2010 não era clara, mas sua obrigatoriedade era iminente – o site oficial do programa afirmava que o objetivo final era que "todos os residentes maiores de 16 anos deveriam ter um cartão".

dados biométricos já contidos no NIR.

O Identity Cards Act adotava a definição de dados sensíveis do Data Protection Act de 1998, segundo o qual dados sensíveis compreenderiam informações sobre origem racial ou étnica, posição política, crenças religiosas, eventual associação a sindicatos, condição de saúde física ou mental, vida sexual, e acusação ou condenação criminal. De acordo com a seção 1 (6), dados sensíveis não seriam registráveis no NIR, ou seja, dados biométricos não estavam no rol dos dados sensíveis.

As seções 17-21 do Act permitiam que o Secretário de Estado fornecesse dados do NIR a autoridades públicas e terceiros sem o consentimento do indivíduo, sob a justificativa de preservar a segurança nacional, prevenir e apurar crimes, investigar e verificar questões relacionadas à tributação e à alfândega, e "por quaisquer outros motivos mediante ordem do Secretário de Estado". Quando não estivesse dentro dessas hipóteses, o consentimento do indivíduo era necessário para fornecer dados "a uma pessoa" ("a person", Seção 12). Ademais, solicitações para alterar dados no NIR estavam sob o poder discricionário do Secretário de Estado (seção 10 (4)).

O Act especificava diversas categorias de informações a serem inseridas no NIR, dentre as quais 10 digitais, scan facial e de íris e todos os locais onde o indivíduo já residira ao longo de sua vida – dentro e fora do Reino Unido. O volume de dados e informações contidas no NIR gerou críticas do ponto de vista da privacidade dos cidadãos.

Em 2010, com a ascensão da coalizão Conservador-Liberal Democrata ao governo, o Identity Cards Act foi revogado e o NIS, suspenso. A medida, argumentou-se, representaria uma economia de £86 milhões em 4 anos e de £800m em 10 anos, ante os altos custos de manutenção e implementação do NIS. À época, o Home Office, responsável pelo controle de fronteiras do Reino Unido, declarou que a suspensão do programa era "o primeiro de muitos passos para reduzir o controle do Estado sob pessoas decentes e seguidoras da lei, e dar-lhes poder"[31]. Os dados

[31] The Gardian. ID cards scheme to be scrapped within 100 days. 2010. Disponível em www.privacidadebr.org

até então coletados foram destruídos.

A revogação do Identity Cards Act parece, assim, ter tido resultado de três preocupações: (i) os altos custos de sua implementação; (ii) a preocupação com privacidade e proteção de dados pessoais diante de um banco de dados unificado e, por isso, altamente vulnerável; e (iii) a preocupação com a vigilância estatal sob os cidadãos diante da coleta e processamento de uma quantidade considerável de dados pessoais.

Recentemente, contudo, essas preocupações parecem assumir um lugar secundário. Com a intensificação dos movimentos migratórios na Europa (notadamente a imigração ilegal) e a maior ocorrência de atentados terroristas, o debate acerca da implementação de uma política nacional de identidade no Reino Unido tem retomado fôlego[32].

C. Estônia

Após tornar-se independente da União Soviética em 1991, a Estônia se deparou com a impossibilidade de fisicamente servir a uma população pequena espalhada por um vasto território. Diante desse cenário, os setores público e privado engajaram-se em desenvolver soluções digitais de governança e e-services[33]. O e-ID, lançado em 2002 e regulado pelo Digital Signature Act 2000 e pelo Identity Documents Act 2000, é parte desses esforços.

O e-ID é um cartão emitido pela Polícia e Conselho de Guarda de Fronteiras, válido para identificação física e digital, e obrigatório para cidadãos e residentes permanentes a partir de 15 anos de idade. É o único documento obrigatório,

<https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards>.

[32] A esse respeito: BBC. Calais and the UK's lack of ID cards. 2015. Disponível em <http://www.bbc.com/news/uk-politics-33756783>. The Telegraph. It's time to bring back national ID cards. 2016. Disponíve em <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12109626/Its-time-to-bring-back-national-ID-cards.html>.

[33] KOTKA, Taavi. Country as a Service: Estonia's New Model. 2016. Disponível em <https://e-estonia.com/country-as-a-service-estonias-new-model/>.

podendo, assim, substituir outros documentos de identificação – em países da União Europeia ele substitui o passaporte.

Esse cartão de identidade tem um chip eletrônico com dois códigos PIN. O primeiro é utilizado para autenticação, permitindo o acesso a *e-services* como verificação da validade do seguro do carro, visualização da lista de candidatos em uma eleição ou de registros médicos individuais. Já o segundo código refere-se à assinatura digital, e é utilizado para validar transações online como, por exemplo, aquisição de apólice de seguros, envio da declaração de imposto de renda ou a realização de um voto em uma eleição.

Em 2010, duas novas derivações do e-ID foram lançadas: a digi-ID (documento digital estatal para identificação pessoal em plataformas eletrônicas e emissão de assinatura digital) e a Mobile-ID (que permite o uso de telefones celulares como forma de identificação digital para acessar e-services e emitir assinatura digital). Por fim, em 2014 foi lançado o e-residency identity card, que confere a estrangeiros uma identidade digital e um cartão de identidade digital com base nas credenciais de identificação de seu próprio país[34].

Por lei, nenhum sistema está autorizado a armazenar a mesma informação em mais de um lugar. Os dados de cada pessoa estão no banco de dados da população, não podendo estar em outros bancos de dados – apenas o identificador exclusivo de cada cidadão pode ser usado nas outras bases de dados. A rede X-Road é a maneira de se compartilhar dados entre as diferentes bases de dados de maneira segura. Nela, cada usuário determina quais informações estão disponíveis e quem tem acesso a elas por meio de padrões de desenvolvimento de software[35].

O direito à privacidade consiste, segundo a Constituição estoniana, na inviolabilidade da vida privada e familiar, excetuando os casos previstos em lei (art. 26 da Constituição da República da Estônia 1992 e §1 (1) do Personal Data Protection Act 2008). A interoperacionalidade do sistema estoniano junto com o

[34] Conf. site oficial do governo da Estônia <https://www.politsei.ee/en/teenused/isikut-toendavad-dokumendid/e-residendi-digi-id/>.
[35] Programa Cidades Sustentáveis. Estônia: uma democracia digital. 2016. Disponível em <http://www.cidadessustentaveis.org.br/noticias/estonia-uma-democracia-digital>.

sistema legal de proteção de dados do país possibilitam assim um cenário que garante ao cidadão o controle do acesso a seus dados pessoais. Mesmo em situações em que os cidadãos não podem barrar o acesso do Estado – como um policial acessando um terminal em tempo real, por exemplo –, eles podem solicitar informações como quem acessou seus dados pessoais e quando. Quando esses acessos não forem justificados, os cidadãos podem registrar queixa[36].

Os dados pessoais (quaisquer dados a respeito de uma pessoa natural identificada ou identificável, § 4, (1)) são regulados pelo Personal Data Protection Act 2008, cujo regime tem o consentimento como elemento central (§ 10, (1)). Esse consentimento deve ser expresso (silêncio e inatividade não são assim considerados) com a possibilidade de ser parcial e condicional (§12.1). Ainda sobre o processamento dos dados pessoais, o Personal Data Protection Act 2008 define "medidas de segurança" como aquelas organizacionais, físicas e de tecnologia da informação com vistas a proteger o processamento, divulgação e destruição acidental ou não autorizado de dados pessoais (§ 6, 6 e § 25, 1).

O caso estoniano de implementação do registro de identificação único através do e-ID é tido como modelo de sucesso, inspirando diversos países a adotarem políticas similares. Através do e-ID verificamos que é possível a implementação de uma identificação única que priorize a privacidade e a proteção de dados do indivíduo, dando inclusive ferramentas para que esse possa ter controle sobre seus dados.

Nesse sentido, a eficiência e a redução de custos de uma política de identificação centralizada não precisa desconsiderar o direito da pessoa de ter controle como sobre o uso de seus dados pessoais, e receber uma "prestação de contas" na utilização indevida, inclusive do setor público. Políticas públicas por si só não justificam o descaso com o direito à privacidade e a proteção de dados pessoais.

Porém, observa-se que a Estônia é, de fato, um país de proporções pequenas,

[36]Secure Identity Alliance. E-Services in Estonia: a success story. 2014. Disponível em < https://secureidentityalliance.org/public-resources/11-14-06-02-sia-estonia-visit-report/file>.

com cerca de 1 milhão e trezentos mil habitantes, em contraste com o Brasil de mais de 200 milhões de habitantes, o que pode facilitar a implantação e gerência desse tipo de política.

D. México

A Constituição Política dos Estados Unidos Mexicanos 1917, em seu art. 36, I, estabelece que é obrigação de todo cidadão mexicano "se inscrever no Registro Nacional de Cidadãos". Para regulamentar essa disposição, os artigos 85 e 86 da Lei Geral de População 1974 atribuem à Secretaria de Governo o registro e irrefutável autenticação dos residentes do país e de mexicanos que residam no exterior, e a definição de regras, métodos e procedimentos técnicos necessários ao Registro Nacional da População (Registro Nacional de Población – RENAPO). O RENAPO compreende os cidadãos inscritos no Registro Nacional de Cidadãos, no Registro de Menores de Idade e no Catálogo de Estrangeiros residentes no México (art. 87 da Lei Geral de População 1974).

Além de realizar os registros, o RENAPO emite a Chave Única de Registro de População (Clave Única de Registro de Población – CURP), instrumento para registrar cidadãos e residentes individualmente (artigo 91 da Lei Geral de População 1974). A adoção dessa Chave visa garantir a transparência na atuação da administração pública, a eficiência na distribuição de benefícios sociais e o combate à fraude. A CURP consta no passaporte e é vinculada à certidão de nascimento, mas não contém informações biométricas nem fotografia – não sendo útil para identificação no dia-a-dia da população[37].

Em 2009[38], por meio de emendas à Lei Geral da População 1974, o governo de Felipe Calderón anunciou a criação do Registro Nacional de Cidadãos, no qual seriam registrados cidadãos e residentes maiores de 18 anos, e a expedição da

[37] Por esse motivo, no caso de pessoas maiores de 18 anos, o título de eleitor com fotografia expedido pelo Instituto Nacional Eleitoral (Instituto Nacional Electoral – INE) é o documento comumente utilizado para identificação.

[38] El Universal. Calderón instituye cédula de identificación biométrica. 2009. Disponível em <http://archivo.eluniversal.com.mx/nacion/170191.html>.

Cédula de Identidade Cidadã[39], documento oficial de identificação que forneceria prova plena dos dados do seu titular ante todas as autoridades mexicanas (artigos 104 e 105 da Lei Geral de População 1974). Tanto o Registro como a Cédula são serviços de interesse público prestados pelo Estado nos termos do art. 97 da Lei Geral de População 1974. A inscrição no Registro é obrigatória (art. 98), mas não cabe sanção (art.106). A iniciativa criaria um sistema de identificação único com uma base de dados nacional, composta pela identidade legal de cada indivíduo e seus dados biométricos.

O atraso na implementação do programa[40] e o crescente número de casos de crianças desaparecidas demandaram sua reestruturação: o registro de menores de idade passou a ser priorizado. Para efeito de identificação de mexicanos menores de 18 anos, seria expedida a Cédula de Identidade Pessoal (CEDI). Esta deveria conter: nome; sexo; local e data de nascimento; nome dos pais; Chave Única de Registro de População; fotografia; imagem da íris; data e local de expedição. A CEDI seria solicitada pelos pais, tutor do menor ou pelo próprio a partir de 14 anos; teria vigência de 6 anos e seria renovada a critério dos pais e tutores ou quando as mudanças físicas do menor fizessem com que ele não correspondesse à fotografia (artigos 53-58 do Regulamento da Lei Geral de População 2000). Ao completar 18 anos, esses jovens deveriam solicitar seu registro junto ao Registro Nacional de Cidadãos.

O programa foi bastante criticado por não endereçar questões de privacidade e

[39] A Cédula conterá: nome dos pais, Chave Única de Registro de População, fotografia, data e local de nascimento, e assinatura e impressões digitais. Com a reforma de 2011 (DOF 19-01-2011), o Regulamento dispõe que a Cédula conterá (art. 47): nome; sexo; local e data de nascimento; data e local de inscrição no Registro Nacional de Cidadãos; nome e nacionalidade dos pais; dados de localização de nascimento no registo civil, ou certificado de nacionalidade ou naturalização; nacionalidade de origem em caso de naturalização; Chave Única de Registro de População; fotografia; impressões digitais; imagem da íris e assinatura do cidadão. Outros dados poderão ser determinados pelo Registro Nacional de População (regulamento, art. 49).

[40] No Legislativo, "a Comissão Permanente pediu, na quarta-feira, para o Executivo a suspender o projeto pelo menos até que os legisladores tenham informação suficiente para estudar o documento, que conteria dados biométricos de cada pessoa e que, segundo as autoridades, serviria para simplificar os procedimentos como inscrição em escolas ou instituições de saúde". Expansion. EL CONGRESO MEXICANO PIDE AL GOBIERNO FRENAR LA CÉDULA DE IDENTIDAD. 2011. Disponível em < http://expansion.mx/nacional/201/101/19/el-congreso-mexicano-pide-al-gobierno-frenar-la-cedula-de-identidad>.

transparência. Argumentou-se também que usar scan das duas íris, além das 10 digitais, não seria proporcional aos objetivos do programa. Além disso, apontou-se os altos custos do programa, a falta de transparência e debate público na elaboração do programa[41].

O direito à privacidade é estabelecido na Constituição Política dos Estados Unidos Mexicanos 1917 (arts. 6, A, II e 16), que prevê a proteção, acesso, cancelamento e retificação de dados pessoais, bem como a inviolabilidade da pessoa, sua família, seu lar, documentos e bens – exceto por ordem escrita e fundamentada de autoridade competente. Quanto a medidas de segurança, a Lei Geral de Proteção de Dados Pessoais em Posse de Sujeitos Obrigados 2017 impõe aos responsáveis pelo tratamento de dados a adoção de medidas de segurança "que permitam proteger os dados pessoais contra dano, perda, alteração, destruição ou uso, acesso e tratamento não autorizado, assim como garantir sua confidencialidade, integridade e disponibilidade" (art. 31). Essa mesma Lei prevê que o tratamento de dados pessoais deverá ser justificado por "finalidades concretas, lícitas, explícitas e legítimas", e o uso desses dados para finalidades distintas só poderá ocorrer mediante consentimento do titular (art. 18). Ainda, o titular dos dados pessoais poderá solicitar acesso, retificação, cancelamento ou oposição ao tratamento realizado (art. 43), e essa solicitação só poderá ser indeferida nas hipóteses previstas no art. 55 (dentre as quais obstrução de justiça, impedimento legal, lesão de direitos de terceiro, para dar cumprmento a obrigações jurídicas assumidas pelo titular).

Em 2015, o governo de Henrique Peña Nieto anunciou o cancelamento definitivo da Cédula de Identidade Cidadã. A Secretaria de Governo afirmou à época que não retomaria o projeto lançado em 2009 e que sua prioridade[42] seria a implementação de uma chave única, um código alfanumérico ligado a dados

[41] Manuli, Gabriela. Despite Privacy Concerns, Mexico Continues Scanning Youth Irises for ID Cards. 2012. Disponível em <https://www.eff.org/pt-br/deeplinks/2012/08/despite-privacy-concerns-mexico-continues-scanning-youth-irises-id-cards>.

[42] Em 2013, o presidente Peña Nieto e os dirigentes dos principais partidos políticos do país firmaram o Pacto pelo México estabelecendo 95 compromissos que seriam vitais para o desenvolvimento do país. Dentre esses compromissos está a criação de uma Cédula de Identidade Cidadã, que permitiria "garantir o direito à identidade cidadã" sem viés político ou eleitoral.

biométricos – diferindo, portanto, do CURP. A decisão tem suscitado críticas pois os custos despendidos na implementação do projeto de Felipe Calderón foram demasiado altos e a nova proposta de Peña Nieto pouco difere da anterior[43].

Diante desse cenário, é possível notar que o registro único no México tem enfrentado diversos obstáculos para a sua implementação. Entre eles, destaca-se a notável influência do cenário político, que diante da mudança de governo decide, por exemplo, cancelar a Cédula de Identidade Cidadã, para criar outro documento com as mesmas funções de características.

Ademais, ao analisar o cenário mexicano, remonta-se no cenário brasileiro o caso do RIC, que após extinto, encontra seu paralelo através da ICN. Apesar das razões de extinção do RIC[44] (Brasil) e da Cédula de Identidade Cidadã (México) não serem as mesmas, é notável que ambos buscam ainda a unificação dos dados pessoais através da implantação de uma identidade única.

E. Quênia

Políticas nacionais de identidade no Quênia remontam a 1915, quando o país ainda estava sob domínio do Reino Unido. Neste ano tornou-se compulsório a todos os homens a partir de 16 anos carregar seu certificado de registro e suas digitais em um "crachá" de metal pendurado em seu pescoço – "corrente Kipande".

O Kipande era o instrumento de controle laboral no regime colonial. Em 1947, a corrente foi substituída por um livreto de identidade. Em 1980, juntamente com a inclusão das mulheres no registro, o livreto deu lugar a cartões de identidade de papel ("Primeira Geração"). Em 1995 passou-se a expedir cartões de identidade de papel do tamanho de cartões de crédito ("Segunda Geração"), e em 2011 começaram a ser expedidos cartões de plástico, mas sem mudanças nos dados

[43]E-consulta.com. Desecha Peña cédula de identidad impulsada por Calderón. 2015. Disponível em <http://nfh3.e-consulta.com/nota/2015-10-02/nacion/desecha-pena-cedula-de-identidad-impulsada-por-calderon>.

[44] O RIC, foi aprovado em 1997 através da lei 9547. DONEDA, Danilo Cesar Maganhoto; KANG, Margareth; SANTOS, Maike Wille. Políticas de identidade na era digital e o registro civil nacional. *Em Debate*. Belo Horizonte, v.8, n.6, p.41-64, 2016. Disponível em: <http://opiniaopublica.ufmg.br/site/files/artigo/4-Margareth-Kang.pdf>

coletados ou recadastramento da população[45].

O cartão de identidade queniano inclui informações biográficas, fotografia, uma impressão digital coletada manualmente em tinta, assinatura e um número de identidade de 8 dígitos[46], e é expedido pelo Escritório de Registro Nacional (National Registration Bureau), do Ministério do Interior[47]. O documento é obrigatório para cidadãos a partir de 18 anos – a não solicitação do documento constitui infração e está sujeita a multa, prisão ou ambas (14, 1, a do Registration of Persons Act 1949).

No Quênia, a cidadania é adquirida por nascimento ou por registro (13, 2 da Constituição do Quênia 2010). A cidadania é adquirida por nascimento se, no dia do nascimento, a mãe ou o pai forem cidadãos (14,1 da Constituição do Quênia 2010). Desde 2008 as certidões de nascimento contêm os nomes e os números de identidade dos pais, o que facilita a comprovação de cidadania no ato de solicitação do cartão de identidade para os indivíduos nascidos a partir desse ano.

A dificuldade de se comprovar cidadania quando não há a identidade dos pais na certidão de nascimento levou à criação de um procedimento sofisticado para concessão do cartão de identidade, o veto ("vetting"). Após a submissão do pedido de uma carteira de identidade, realiza-se o veto, um procedimento por meio do qual um comitê busca averiguar se o indivíduo é ou não queniano. O veto pode incluir entrevistas do indivíduo, seus familiares e referências, e documentos adicionais. Contudo, essa prática tem sido utilizada como instrumento para negar identidade a

[45] Constituição do Quênia, 2010. "12. (1) Every citizen is entitled to a) the rights, privileges and benefits of citizenship, subject to the limits provided or permitted by this Constitution; and b) a Kenyan passport and any document of registration or identification issued by the State to citizens". Kenya Citizenship and Immigration Act, 2011. "22. (1) Every citizen is entitled to the rights, privileges and benefits and is subject to the limitations provided for or permitted by the Constitution or any other written law including (…) (g) the entitlement to any document of registration or identification issued by the State to citizens including (…) (iv) a national identification card".

[46] Programas de transferência de renda e o alistamento eleitoral nacional possuem sistemas próprios de biometria que envolvem cadastramentos separados. Contudo, ambos exigem a apresentação do cartão de identidade para deferir solicitações de cadastro.

[47] O Ministério do Interior também é responsável pelos Registros Civis (nascimento, morte e casamento), Passaportes e Vistos, e Registro de Refugiados. Essas bases de dados, juntamente com o Registro de Cartões de Identidade, estão sendo unificadas em uma base de dados central, o Registro da População Nacional. A iniciativa visa possibilitar que órgãos públicos e privados façam autenticação de documentos de identificação – notadamente, do documento de identidade –, e se insere nos esforços do Quênia implementar e-governance. A implementação dessa base de dados centralizada tem sido regida pelo National Registration and Identification Bill 2012, ainda em discussão e não aprovado.

determinadas raças e etnias. O veto tem sido aplicado de forma seletiva, tornando-se mais complexo e trabalhoso para determinados grupos de indivíduos. Além disso, a prática, por possuir diversas fases, tem estimulado corrupção e arbitrariedades por parte dos oficiais públicos[48].

Uma das principais críticas à política de identificação queniana é sua falta de interoperacionalidade. De um lado, a coleta manual de impressões digitais faz com que a autenticação dos cidadãos no dia-a-dia seja feita com base nas informações biográficas – as digitais são armazenadas em formato de imagem, e sujeitas a um controle manual de qualidade. De outro lado, há pouca integração entre os registros civis e o registro de identidades – por exemplo, no caso dos registros de nascimento, os documentos são majoritariamente físicos, assim como nos registros de óbito, e a transmissão desses fato ao banco de dados é demorada.

Com a implementação de uma base de dados central em curso, o Registro da População Nacional 2012, crescem as preocupações acerca da proteção desses bancos de dados. Contudo, o Quênia não possui uma lei geral de proteção de dados pessoais – o Data Protection Bill 2012 ainda está em discussão. O direito à privacidade é estabelecido pela Constituição e inclui o direito do indivíduo de não ter (i) sua pessoa, lar ou propriedade revistados, (ii) seus bens apreendidos, (iii) informações privadas ou sobre sua família desnecessariamente solicitadas ou reveladas, e (iv) a privacidade de suas comunicações violada (art. 31).

Portanto, em matéria de proteção de dados pessoais, o Quênia, apesar de possuir um projeto de lei em andamento, enfrenta dificuldades técnicas que podem, mesmo com a aprovação da lei, dificultar a implementação da mesma.

O cenário queniano demonstra como as particularidades de cada país pode influenciar a construção e implementação das políticas de identidade. Assim, além da dificuldade do registro do indivíduo com base nos dados biográficos de seus ancestrais, que pode nunca ter se registrado em uma repartição pública, ainda existe a barreira da discriminação de algumas tribos (“vetting”).

[48] COMMISSION ON ADMINISTRATIVE JUSTICE OFFICE OF THE OMBUDSMAN, 2015.

F. Brasil

Atualmente, brasileiros ou estrangeiros residentes no país possuem cerca de vinte documentos que podem ser utilizados para fins de identificação, dentre os quais a certidão de nascimento, o Cadastro de Pessoa Física, a Carteira Nacional de Habilitação e a carteira de identidade ou Registro Geral (R.G.)[49].

Os primeiros esforços para promover uma política nacional de identificação única no Brasil remontam a 1997, com a criação do Registro de Identificação Civil (RIC)[50]. O RIC foi criado com o objetivo de combater fraudes, promover a cidadania e modernizar o registro civil. Nele convergiriam diversos documentos como o RG, CNH e CPF. Sua regulamentação ocorreu somente em 2010 e, a partir daí, ficou a cargo do Instituto Nacional de Identificação do Departamento de Polícia Federal estudar a forma de sua implementação. No entanto, os altos custos parecem ter corroborado com a lenta implementação da iniciativa.

Em 2012 a implementação do projeto passou para o Ministério da Justiça, que no ano seguinte firmou acordo de cooperação com a Universidade de Brasília para desenvolver a infraestrutura tecnológica necessária à implantação do RIC. Os estudos foram suspensos em 2015, em virtude da apresentação, pelo Poder Executivo e pelo Tribunal Superior Eleitoral, do Projeto de Lei 1.775 / 2015, o qual propunha a criação do Registro Civil Nacional – RCN, a ser implementado pelo Tribunal Superior Eleitoral[51].

Inicialmente o PL 1775 dispunha sobre a criação do RCN, e revogava a lei que criara o RIC. Após a realização de audiências públicas e parecer do relator do projeto na Câmara dos Deputados, o nome da iniciativa deixou de ser RCN e passou a ser Identificação Civil Nacional – ICN. Em 11 de abril de 2017, a ICN foi aprovada no

[49] O RG é um documento de validade nacional emitido pelos estados. Pelo fato de não haver uma interoperabilidade entre a base de dados de emissão dos RGs entre os Estados, ele é passível de fraudes, permitindo que o cidadão tenha um documento para cada uma das 27 unidades da federação.
[50] BRASIL. Lei Nº 9.454 / 1997.
[51] Ministério da Justiça e Segurança Pública do Governo Federal < http://justica.gov.br/Acesso/governanca/ric>.

Senado Federal. Finalmente, em 11 de maio do mesmo ano o projeto foi sancionado pela Presidência da República, tornando-se a Lei 13.444/2017.

A ICN foi criada com o objetivo de unificar informações de identificação do cidadão, na busca pela maior eficiência da gestão pública e combate a fraudes. Assim, será criada uma base dados gerida pelo Tribunal Superior Eleitoral, composta pelas bases de dados da Justiça Eleitoral, do Sistema Nacional de Informações do Registro Civil, dos Institutos de Identificação e de outros órgãos, conforme definido pelo Comitê Gestor. Ao cidadão será emitido o Documento Nacional de Identidade (DNI), o qual deverá ser pago pelos cidadãos desde a primeira emissão. Os documentos emitidos por entidades de classe têm um prazo de dois anos para atenderem aos requisitos de biometria e fotografia estabelecidos para o DNI.

Uma análise mais aprofundada da ICN foi feita pelo Privacidade Brasil na Nota Técnica do PL 19/2017 e no Aditivo I - Nota Técnica.

4. CONSIDERAÇÕES FINAIS

A tendência dos países em implementarem uma identificação única merece reflexão em diversos aspectos, entre eles da privacidade e proteção de dados pessoais. A análise dos países acima procurou demonstrar que o avanço da tecnologia tem incentivado países ao redor do mundo à buscarem políticas de identidade única de seus cidadãos, com excessivo apoio no reconhecimento biométrico e de gerenciamento de dados.

É verdade que as tecnologias evoluíram, permitindo um melhor gerenciamento de dados pessoais pelo setor público. Ressalta-se, no entanto, que as inovações e avanços tecnológicos disponíveis aos governos também podem ser acessadas por toda sociedade, o que aumenta a vulnerabilidade das políticas públicas apoiadas nos potenciais tecnológicos.

Não obstante o direito à privacidade ser ameaçado, ressalta-se que a privacidade está diretamente relacionada com outros direitos fundamentais, como a

liberdade de expressão, a liberdade de associação, o direito à informação; que também podem ser mitigados como consequência da não garantia do direito à privacidade.

Outro efeito da identificação única é a vigilância. Uma vez adotada a identidade única, políticas de segurança e auditoria precisam também ser estabelecidas. Já que o excesso por parte dos setor público no gerenciamento e uso dos dados pessoais não pode ser descartado, um dos motivos pelos quais os cidadãos da Reino Unido decidiram por revogar o Identity Card Act. Nesse balizar, discursos de defesa frente ao terrorismo, eficiência da gestão pública, diminuição da violência, não podem servir de justificativas para uma vigilância em massa.

As políticas de identidade envolvem a adaptação na coleta de dados assim como o compartilhamento entre os bancos de dados já existentes. Nesse sentido, o desenho desse tipo de política demanda escolhas das tecnologias envolvidas na implementação dos processos, das finalidades da política e dos interesses políticos que as norteiam, de questões técnicas de interoperabilidade do sistema, e de questões jurídicas de convergência e coerência[52]

Especificamente quanto aos interesses políticos que norteiam as políticas de identidade, é possível perceber que eles variam em diferentes lugares e momentos. Dentre os principais interesses políticos apreendidos na elaboração deste relatório, podemos apontar:

(1) O combate ao terrorismo e a gestão das fronteiras (especialmente após os eventos de 11 de setembro de 2001, a exemplo do Reino Unido);
(2) O combate à fraude a serviços e programas governamentais (Estônia, Índia, Reino Unido, México, Brasil);
(3) Necessidade de apoiar o setor privado com um regime adequado de identificação (Estônia e Quênia);
(4) Necessidade de auxiliar no desenvolvimento de serviços de governo eletrônico (como o e-voting, a exemplo da Estônia e do Quênia);

[52] WHITLEY, Edgar A., HOSEIN, Gus. *Global Challenges for Identity Policies*. Palgrave Macmillan, UK, 2010, p. 07.

(5) Necessidade de gerenciar populações específicas (Quênia);

Assim, em razão da existência de diversos argumentos que sustentam a implantação das políticas de identificação única, estabelecer limites na coleta e gerenciamento dos dados pessoais pode parecer entrar em confronto na busca pela eficiência e combate à fraude. No entanto, grifa-se que a melhora na gestão tem como finalidade principal a sociedade na qual o indivíduo é parte. Por essa razão, não é cabível a construção de uma política que ignore os princípios estabelecidos nas Constituições, como a proteção da dignidade da pessoa humana.

Por isso, estabelecer os direitos fundamentais, a exemplo da privacidade, como princípio na construção de políticas de identificação única, caminha juntamente, e não em conflito, com a busca da administração pública pela melhoria na sua gestão. Nesse compasso, a identificação única deve ser norteada por finalidades específicas, e nunca amplas, previamente aceitas e consentidas pelos indivíduos, no tratamento de seus dados pessoais.

Além das finalidades definidas, o estabelecimento dos meios utilizados, com vistas à proteção da privacidade e dos dados pessoais, também é essencial. Nessa lógica, a adoção de tecnologias pró-privacidade (ex. PET- Privacy Enhacement Technologies) faz-se necessária.

BIBLIOGRAFIA

- ARTHUR, Charles. Iphone 5S fingerprint sensor hacked by Germany´s Chaos Computer Club. The Guardian, 23 de setembro de 2013. Disponível em: < https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked >
- BANERJEE, Shweta. World Development Report 2016 Digital Dividends: Aadhaar – Digital Inclusion and Public Services in India. Washington, DC: World Bank. Disponível em < http://pubdocs.worldbank.org/en/655801461250682317/WDR16-BP-Aadhaar-Paper-Banerjee.pdf>.
- COMMISSION ON ADMINISTRATIVE JUSTICE OFFICE OF THE OMBUDSMAN, August 2015. Stateless in Kenya: An Investigative Report on the Crisis of Acquiring Identification Documents in Kenya. Disponível em <http://www.ombudsman.go.ke/wp-content/uploads/2016/04/Investigation-report-on-the-crisis-of-acquiring-identification-documents-in-Kenya.pdf>.
- DAHAN, Mariana; GELB, Alan. The Role of Identification in The Post-2015 Development Agenda. Washington, DC: World Bank, 2015. Disponível em < http://pubdocs.worldbank.org/en/149911436913670164/World-Bank-Working-Paper-Center-for-Global-Development-Dahan-Gelb-July2015.pdf>.
- DOMÍNGUEZ, Karla Cantoral. El derecho a la identidad del menor: el caso de México. Revista boliviana de derecho. Santa Cruz: Revista boliviana de derecho, n. 20, p. 56-75, 2015. Disponível em < http://www.scielo.org.bo/pdf/rbd/n20/n20_a03.pdf>.
- FROOMKIN, A. Michael. Identity Cards and Identity Romanticism. Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, New York: Oxford University Press, 2009; University of Miami Legal Studies Research Paper No. 2008-41. Disponível em SSRN:< https://ssrn.com/abstract=1309222>
- GELB, Alan; CLARK, Julia. Identification for Development: The Biometrics Revolution. CGD Working Paper 315. Washington, DC: Center for Global Development. Disponível em <http://www.cgdev.org/content/publications/detail/1426862>.
- GREWAL, Japreet; RAKESH, Vanya; CHATTAPADHYAY, Sumandro; HICKOK, Elonnai. Report on Understanding Aadhaar and its New Challenges. The Centre for Internet and Society. Disponível em < https://cis-india.org/internet-governance/blog/report-on-understanding-aadhaar-and-its-new-challenges >.
- HARBITZ, Mia; AXT, Iván Arcos. Identification and Governance Policies: The

Legal, Technical, and Institutional Foundations that Influence the Relations and Interactions of the Citizen with the Government and Society. Inter-American Development Bank. Washington, DC: The Inter-American Development Bank Technical Notes, 2011. Disponível em <http://www.iadb.org/wmsfiles/products/publications/documents/36400828.pdf>.

- HERN, Alex. Samsung Galaxy S8 iris scanner fooled by German hackers. 23 de maio de 2017. Disponével em: < https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security>
- HERN, Alex. Hackers fakes German Minister´s fingerprints using fotos of her hands. The Guardian, 30 de dezembro de 2014. Disponível em: < https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands >
- INTERNATIONAL TELECOMMUNICATION UNION. Review of National Identity Programs. Genebra: International Telecommunication Union, 2016. Disponível em < https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/Review%20of%20National%20Identity%20Programs.pdf>.
- KOHN, Sebastian. Out in the Cold: Vetting for Nationality in Kenya. Disponível em < https://www.opensocietyfoundations.org/voices/out-cold-vetting-nationality-kenya>.
- LYON, David. BENNET, Colin J. Playing the ID card. Understanding the Significance of Identity Card Systems. Routledge 2008. New York.
- MARTIN, Aaron K. National Identity Infrastructures: Lessons from the United Kingdom. International Federation for Information Processing (IFIP). Advances in Information and Communication Technology, AICT-386, p. 44-55, 2012. Disponível em < http://personal.lse.ac.uk/martinak/ifip.pdf>.
- MEINTS, Martin. Gasson, Mark. The Future of Identity in the Information Society. Challenges and Opportunities. Springer. 2009.
- OPPENHEIM, Ben; POWELL, Brenna Marea. Legal Identity in the 2030 Agenda for Sustainable Development: Lessons from Kibera, Kenya. Nova York: Open Society Foundations, 2015. Disponível em < https://www.opensocietyfoundations.org/sites/default/files/legal-identity-2030-agenda-lessons-kibera-kenya-2051216.pdf>.
- < https://ssrn.com/abstract=2379246>.
- PETERS, Guy B. Civil Registration and Vital Statistics as a Tool to Improve Public Management. Washington, DC: Inter-American Development Bank, 2016. Disponível em < https://publications.iadb.org/bitstream/handle/11319/7815/Civil-Registration-and-Vital-Statistics-as-a-Tool-to-Improve-Public-Management.pdf?sequence=

1>.
- PRIVACY INTERNATIONAL. Biometrics. disponível em: < https://www.privacyinternational.org/node/70>; e Facial Recognition, disponíevl em: < https://www.privacyinternational.org/de/757> . Acessados em junho de 2017.
- SULLIVAN, Clare. The United Kingdom Identity Cards Act 2006 – Proving Identity?. Macquarie Journal of Business Law, Vol. 3, 259-287, 2006. Disponível em < https://ssrn.com/abstract=2379246>.
- VASSIL, Kristjan. World Development Report 2016 Digital Dividends: Estonian e-Government Ecosystem: Foundation, Applications, Outcomes. Washington, DC: World Bank. Disponível em < http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf>.
- VÉLEZ, Alejandro. Insecure Identities: The Approval of a Biometric ID Card in Mexico. Surveillance & Society, Vol. 10, n 1, p. 42-50, 2012. Disponível em < https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/Mexico_ID>.
- VOX. Color film was built for white people. Here's what it did to dark skin.The unfortunate history of racial bias in photography. 18 de setembro de 2015. Disponível em: < https://www.youtube.com/watch?v=d16LNHIEJzs>
- WHITLEY, Edgar A.; HOSEIN, Gus. *Global Challenges for Identity Policies*. Basingstoke: Palgrave Macmillan, 2010.
- WORLD BANK. The State of Identification Systems in Africa – A Synthesis of Country Assessments. Washington, DC: World Bank, 2017. Disponível em < https://openknowledge.worldbank.org/handle/10986/26504>.
- WORLD BANK. Identification Systems Analysis – Country Assessment Kenya. Washington, DC: World Bank, 2016. Disponível em < http://documents.worldbank.org/curated/en/575001469771718036/pdf/107277-WP-P156810-PUBLIC.pdf>.
- WORLD BANK. Identification for Development – Strategic Framework. Washington, DC: World Bank, 2016. Disponível em < http://pubdocs.worldbank.org/en/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf>.

	Estônia	Reino Unido	Índia	México	Quênia	Brasil
Data de Implementação	2002	2006	2009	2010	2011	2017
Vigente?	Sim	Não	Sim	Não	Sim	Não
Normativo	Identity Documents Act (1999) e Digital Signatures Act (2000)	Identity Cards Act (2006)	Notificação No. A.03011/02/2009-Adm. I (Decreto Executivo)	Reglamento de la Ley General de Población (2000) e Ley General de Población (1974)	Registration of Persons Act Chapter 107 (1949)	Lei 13.444/2017
Quem utiliza?	Cidadãos e residentes permanentes a partir de 15 anos.	Residentes a partir de 16 anos; Todo indivíduo de uma determinada descrição (“prescribed description”) que tivesse residido e desejasse entrar no Reino Unido.	Residentes a partir de 5 anos.	Residentes e cidadãos.	Cidadãos a partir de 18 anos.	Todos os cidadãos.
Dados de Certificação	Digitais e Íris	Digitais	Digitais e Íris	Digitais e Íris	Digitais	Digitais
Dados Coletados	Nome; Data e local de nascimento; Identificador numérico pessoal; Fotografia; Gênero; Nacionalidade; Digitais; Assinatura; Scan da íris; Cor do cabelo; Outros dados pessoais exigidos por tratado, lei ou outra legislação.	Nome completo; Gênero; Data e local de Nascimento; Endereços de residência à época, no Reino Unido e no Mundo; Todos os endereços de residência ao longo da vida, no Reino Unido e no Mundo; Todos os números de identificação do indivíduo e seus respectivos documentos; Características externas úteis à identificação (ex. cor do cabelo); 10 digitais.	Fotografia; 10 digitais; Scan das duas íris; Nome; Data de nascimento; Gênero; Endereço; Número de telefone celular e e-mail opcionais.	Nome; Filiação; Chave Única de Registro de População; Fotografia; Local e data de nascimento; Digitais; Scan de íris.	Número de registro; Nome complete; Gênero; Tribo ou raça; Data (ou idade aparente) e local de nascimento; Ocupação, profissão, sindicato ou emprego; Local de residência e endereço postal; Digitais das mãos (quando não houver, digitais da palma ou do hálux); Data de registro; Outros dados eventualmente solicitados.	Foto; Dados biográficos; Digitais da base de dados da Justiça Eleitoral, do Sistema Nacional de Informações de Registro Civil, da Central Nacional de Informações do Registro Civil, dos Institutos de Identificação e de outros órgãos conforme definido pelo Comitê Gestor da ICN.
Definição de dados sensiveis	Opiniões políticas; Crenças religiosas e filosóficas; Raça ou etnia; Estado de saúde ou deficiência; Informação genética; Dados biométricos; Vida sexual; Filiação sindical; Informações sobre o cometimento ou o sofrimento de uma infração ou crime antes de audiência pública, uma decisão interlocutória importante ou decisão transitada em julgado.	Raça ou etnia; Opiniões políticas; Crenças religiosas ou de natureza similar; Existência vínculo sindical; Saúde física e psicológica; Vida sexual; Cometimento ou alegado cometimento de crime ou infração; Ritos processuais e sentenças acerca dos crimes e infrações cometidas ou alegadamente cometidas.	Senhas; Informações financeiras; Saúde física, mental e psicológica; Orientação sexual; Histórico médico; Dados biométricos.	Raça ou etnia; Estado de saúde presente ou futuro; Informação genética; Crenças religiosas, filosóficas ou morais; Filiação sindical; Opiniões políticas; Orientação sexual.	Não há.	Não há.

Órgão Competente	Polícia e o Conselho de Guarda de Fronteiras, a agência governamental responsável pela emissão de documentos de identificação pessoal; Data Protection Inspectorate, responsável por garantir a inviolabilidade da privacidade e a transparência da administração pública.	Secretário de Estado	Unique Identification Authority of India - UIDAI	Secretaria de Governo	National Registration Bureau	Tribunal Superior Eleitoral
Propósito da Política	Eficiência e Transparência da Administração Pública; Facilitar o uso de e-services; Segurança nacional; Combate à fraude.	Combate ao terrorismo; Combate à fraude; Facilitar o acesso a benefícios sociais; Combate ao trabalho ilegal.	Combate à fraude; Facilitar o acesso a benefícios sociais; Transparência da Administração Pública.	Eficiência e transparência da Administração Pública; Facilitar acesso a benefícios sociais; Combate à fraude; Segurança nacional.	Facilitar o uso de serviços públicos e privados.	Eficiência da Administração Pública; Combate à fraude.
Principais Críticas	Algumas funcionalidades, como o envio de documentos assinados pelo sistema, só são possíveis entre portadores do cartão, o que limita sua utilização.	Alto custo de implementação; Vulnerabilidade de um banco de dados unificado; Vigilância estatal; Pouco debate sobre o tema com os cidadãos.	Regime de proteção de dados pessoais; Ausência de mecanismos de segurança do banco de dados; Condição ao recebimento de benefícios sociais; Pouco debate sobre o tema com os cidadãos.	Experiências anteriores de má administração de bancos de dados pelo Poder Público; Pouco debate sobre o tema com os cidadãos.	Falta de interoperacionalidade; Autenticação só pode ser feita pelas informações biográficas e não biométricas; Dificuldade de se comprovar cidadania; Pouco debate sobre o tema com os cidadãos.	Alto custo de implementação; Regime de proteção de dados pessoais; Ausência de mecanismos de segurança do banco de dados; Não gratuidade da primeira emissão; Competência técnica e de gestão do órgão responsável; Pouco debate sobre o tema com os cidadãos.
Previsão de sanção para uso indevido de dados?	A Identity document Act (2000), impõe a multa como sua medida de sanção. Esta pode variar entre 300 fine units até 32.000 euros. As penas mais altas são estabelecidas se a viloação for cometida por pessoa jurídica. ex: Violar os requerimentos e medidas de segurança para a proteção de dados pessoais.	O Act estabelecia que um código com as penas civis e respectivas penas deveria ser expedido pelo Secretário do Estado.	O Aadhaar Act impõe penas como multa, e/ou prisão de até 3 anos, para os casos previstos em lei. Ex:Fornecimento de dados pessoais à terceiro sem prévio consentimento.	A Lei de Registro Nacional de Cidadãos estabeleceu a Multa, como pena para os casos de infração na lei. Assim, a pena, varia entre 100 a 320.000 dias de salário mínimo, podendo dobrar em casos de reincidência. Entre as infrações mais graves, cita-se a criação de base de dados sensíveis sem consentimento expresso e por escrito dos titutlares (200 a 320.000 disas de salário mínimo)	Registration of persons act, Chapter 107 (1949) estabelece que aquele que acessar, alterar ou apagar ilegalmente cartões de identidade ou qualquer documento de registro será punido por multa de até 200.000 shillings, prisão de até 18 meses ou ambos.	O Código Penal 1940 estabelece pena de multa ou detenção de 6 meses a 2 anos para o responsável que realizar ou permitir o acesso de pessoas não autorizadas a bancos de dados da Administração Pública (art. 325 §1º).