ENTRE A VISIBILIDADE E A EXCLUSÃO:

UM MAPEAMENTO DOS RISCOS DA IDENTIFICAÇÃO CIVIL NACIONAL E DO USO DE SUA BASE DE DADOS PARA A PLATAFORMA GOV.BR

DataPrivacyBR
Research

Ficha Técnica

A Associação Data Privacy Brasil de Pesquisa é uma organização da sociedade civil, sem fins lucrativos, que promove a proteção de dados pessoais e outros direitos fundamentais diante da emergência de novas tecnologias, desigualdades sociais e assimetrias de poder. Conta com uma equipe multidisciplinar de diferentes regiões brasileiras que desenvolve pesquisas de interesse público, notas técnicas, textos de análise sobre assuntos emergentes, formações com agentes decisórios e com a sociedade de um modo geral.
A Associação acredita que a proteção de dados pessoais é um dos fundamentos da democracia e que precisa ser vista a partir da perspectiva da justiça social e assimetrias de poder. Assim, trabalha para a promoção de uma cultura de proteção de dados e para que os direitos digitais sejam direitos fundamentais de todas e todos, conduzindo pesquisas abertas ao público, orientadas por um forte compromisso social e com financiamento ético.
Para mais informações sobre a organização, impacto de seus projetos e como pesquisas são apoiadas, visite www.dataprivacybr.org.

Imprensa

Para esclarecimentos sobre o documento e entrevistas, entrar em contato com a Associação pelo e-mail imprensa@dataprivacybr.org

Diretores

Bruno Bioni e Rafael Zanatta

Coordenadoras gerais de projetos

Mariana Rielli e Marina Meira

Líder de Projeto

Johanna Monagreda

Pesquisadores

Eduardo Mendonça, Gabriela Vergili, Hana Mesquita, Helena Secaf, Jaqueline Pigatto, Júlia Mendonça, Marina Garrote, Mikael Servilha, Nathan Paschoalini, Pedro Saliba e Thaís Aguiar

Analista de Incidência

Vinícius Silva

Administrativo e Comunicação

Eduardo Barros, Elisa Bayón, Erika Jardim, Horrara Moreira, Júlio Araújo, Layanne Gayofato, Rafael Guimarães, Roberto Júnior, João Paulo Vicente, Matheus Arcanjo e Willian Oliveira

Como citar esse documento

BIONI, Bruno; GARROTE, Marina; MEIRA, Marina; PASCHOALINI, Nathan. Entre a visibilidade e a exclusão: um mapeamento dos riscos da Identificação Civil Nacional e do uso de sua base de dados para a plataforma gov.br. Associação Data Privacy Brasil de Pesquisa, 2022.

Autoria

Bruno Bioni, Marina Garrote, Marina Meira e Nathan Paschoalini

Revisão

Thaís Aguiar

Sumário

Sumário Executivo

O presente *policy paper* busca analisar a Identificação Civil Nacional (ICN), estabelecida pela Lei nº 13.444/2017, principal iniciativa de unificação do sistema brasileiro de identificação civil, assim como o uso da Base de Dados da ICN (BDICN) para autenticação de usuários na plataforma gov.br, portal do governo federal, no acesso a serviços públicos.

Este relatório parte de um cenário de mais de duas décadas de esforços empreendidos nacionalmente para a implementação de um sistema unificado de identificação, que perpassou diferentes governos. Ao longo desse período, sobressaíram-se duas iniciativas legislativas: o Registro de Identidade Civil (RIC), estabelecido pela Lei nº 9.454/1997, mas que nunca foi efetivamente implementado, e a Identificação Civil Nacional (ICN), cujas discussões iniciaram no ano de 2015, culminando na aprovação da Lei nº 13.444, em 2017. Ambas baseiam-se em arquiteturas informacionais semelhantes, que implicam na centralização de bancos de dados do Estado. No caso da Base de Dados da ICN (BDICN), sua estrutura se dá a partir da junção da base de dados biométricos do TSE com bases de dados do Sistema Nacional de Informações de Registro Civil, da Central Nacional de Informações do Registro Civil, dos Institutos de Identificação dos Estados e do Distrito Federal e do Instituto Nacional de Identificação.

Além de analisar historicamente a política estatal de unificação do sistema de identificação civil no Brasil, o objeto de estudo deste documento abrange o uso dessa identificação para o acesso a serviços públicos digitalizados, hoje realizado por meio do gov.br. Trata-se, o gov.br, de um projeto do governo federal de centralização de seus canais digitais, o qual reúne serviços e informações sobre a atuação de todas as áreas do governo. A criação do gov.br, nesse sentido, se insere em um movimento mundial de plataformização de serviços públicos. Segundo Poell, Nieborg e van Dijck (2021), a plataformização da sociedade pode ser definida como a penetração de infraestruturas, processos econômicos e estruturas de governança de plataformas digitais em diferentes setores socioeconômicos, que resulta na reorganização de práticas culturais e do imaginário social sobre essas plataformas.

Atualmente, a autenticação do cidadão no acesso ao gov.br é o principal uso da BDICN[1]. Para que se possa utilizar o gov.br, é necessário que o usuário utilize um *login* único, formado por seu número de Cadastro de Pessoa Física (CPF) e uma senha pessoal. A Base

1 Em fevereiro de 2022 o TSE anunciou a nova fase de implementação da Identificação Civil Nacional, a emissão do Documento Nacional de Identidade de forma faseada, de início para servidores públicos, após no Estado de Minas Gerais, e a partir de Fevereiro de 2023, disponível para toda população (TSE, 2022a).

de Dados da ICN passou a ser utilizada para autenticação dos usuários na plataforma gov.br no acesso a serviços públicos com a assinatura do Acordo de Cooperação Técnica firmado em 15 de março de 2021 entre Secretaria Geral da Presidência, Ministério da Economia e Tribunal Superior Eleitoral.

Diante de um contexto brasileiro marcado por profundas desigualdades socioeconômicas e regionais, a formulação de políticas públicas que tenham por objetivo a universalização do registro civil e a ampliação do acesso a serviços públicos - ou, em outras palavras, que tornem todos os cidadãos visíveis ao Estado -, é essencial. Ao mesmo tempo, se exacerbada, tal visibilidade pode recair em práticas vigilantistas e potencialmente discriminatórias. E não apenas: experiências internacionais mostram que iniciativas de centralização de sistemas de identificação civil, atreladas à plataformização de serviços públicos, ao contrário do que se propõem, podem aprofundar a exclusão de pessoas e grupos já vulnerabilizados.

Proposto de modo a contribuir com este debate e com o desenvolvimento e aprimoramento das políticas públicas relacionadas à identificação civil digital e digitalização de serviços públicos atualmente em curso no Brasil, este *policy paper* trabalha, justamente, o binômio visibilidade-exclusão. A partir da literatura internacional e nacional, o relatório busca identificar os potenciais riscos aos direitos fundamentais e liberdades civis dos cidadãos - ou titulares de dados - que podem emergir da implementação da Identificação Civil Nacional e do uso de sua Base de Dados no gov.br levando em consideração a realidade socioeconômica brasileira. Os riscos identificados foram divididos em dois grupos: (i) riscos de abuso no tratamento de dados pessoais, relacionados à arquitetura informacional e de governança da ICN; e (ii) riscos de exclusão de cidadãos do acesso a políticas públicas. Abaixo, estão dispostos os riscos identificados, em formato de tabela:

GRUPO 1
Riscos de abuso no tratamento de dados pessoais, relacionados à arquitetura informacional e de governança da ICN

Fonte do risco identificado	Motivo	Direitos fundamentais e liberdades civis potencialmente violados pelos riscos identificados
Ausência de pluralidade de visões no processo de governança de uma política pública complexa	Uma composição não multissetorial de um órgão de governança, como o Comitê Gestor da ICN e a Câmara-Executiva Federal de Identificação do Cidadão (CEFIC) – esta última estabelecida pelo Decreto nº 10.900/2021 -, tem o potencial de não comtemplar a pluralidade de visões necessárias ao adequado processo de governança de uma política pública tão complexa quanto a ICN e o gov.br.	Potencialmente todos - não é possível delimitar; afinal são as escolhas de governança que determinarão quais direitos e liberdades serão afetados. Nesse sentido, a limitação da participação da sociedade tem o potencial de afetar o regime democrático do Estado brasileiro.
Usos secundários e/ou compartilhados abusivos dos dados pessoais constantes na Base de Dados da ICN, em contraste ao princípio da finalidade (art. 6º, I, LGPD)	Existe um risco de usos secundários abusivos de dados pessoais na política da ICN, visível, sobretudo, em quatro momentos: **(i)** Na constituição da BDICN, que se deu a partir da junção de bases de dados de outras esferas públicas, cuja finalidade não é necessariamente compatível com a política da ICN; **(ii)** Na utilização da BDICN para autenticação de usuários na plataforma gov.br, que poderia significar uma desvirtuação da finalidade original das atividades de tratamento de dados da ICN; **(iii)** Utilização da BDICN para o cruzamento de dados de cidadãos com intuito de verificar o cumprimento de requisitos necessários ao acesso a benefícios sociais;	**(i)** Violação da autodeterminação informativa, compreendida como um desdobramento do direito fundamental à proteção de dados pessoais, disposto no art. 5º, LXXIX da Constituição Federal. **(ii)** Violação da dignidade da pessoa humana, estabelecida como um dos fundamentos da República Federativa do Brasil, conforme art. 1º, III da Constituição Federal. **(iii)** Violação do princípio da não discriminação, estabelecido como um dos fundamentos da República brasileira, no art. 3º, IV, e da dignidade da pessoa humana, definido no art. 1º, III, ambos da Constituição Federal.

	(iv) Possibilidade de acesso à BDICN pelos poderes Executivo e Legislativo de qualquer nível federativo sem procedimento para verificação de finalidade.	**(iv)** Violação da autodeterminação informacional, compreendida como um desdobramento do direito fundamental à proteção de dados pessoais, disposto no art. 5º, LXXIX da Constituição Federal.
Tratamento discriminatório aos cidadãos e práticas autoritárias	Além de possuir uma arquitetura informacional centralizada, a Base de Dados da ICN dispõe de uma diversidade enorme de dados, inclusive de dados biométricos, o que pode potencializar: **(i)** práticas vigilantistas por parte do Estado; **(ii)** a exclusão ilegal de cidadãos ao acesso a benefícios de assistência social com base em tratamento discriminatório desses dados, fundamentado no art. 11 da LICN.	**(i)** Vigilância em massa cria *"chilling effect"*, reduzindo a participação nos espaços públicos de cidadãos por receio de estarem sendo vigiados pelo governo, ameaçando assim a liberdade de expressão e manifestação, garantidas no art. 5º, IV, IX e XVI[2]. **(ii)** O tratamento discriminatório ameaça a igualdade garantida pela Constituição em seu art. 5º, caput, inciso I. O mesmo art. 5º também estabelece, como alvo de punição da lei qualquer prática discriminatória prejudicial aos direitos e liberdades fundamentais (art. 5º, inciso XLI) e a inafiançabilidade e imprescritibilidade do crime de racismo (art. 5º, inciso XLII).
Violação do princípio da qualidade dos dados (art. 6º, V, LGPD)	Segundo o TSE existem algumas inconsistências na base de dados biométricos: **(i)** Em 2018, 9 milhões de eleitores tiveram algum problema na identificação biométrica imediata durante as eleições. **(ii)** Desde 2014, foram identificados cerca de 52 mil casos relacionados à duplicidade ou pluralidade de biometrias.	**(i)** Impossibilidade do acesso à serviços públicos via plataforma gov.br, cuja prestação é garantida pelo art. 175 da Constituição. **(ii)** Dificuldades na identificação do eleitor para o exercício do direito ao sufrágio, estabelecido no art. 14 da Constituição Federal.
Incidentes de segurança envolvendo a Base de Dados da ICN	Considerando o fato de que a BDICN possui dados biométricos (sensíveis) de mais de 110 milhões	Violação da dignidade da pessoa humana, estabelecida como um dos fundamentos da República

2 Ver mais em Article 19 (2021).

	milhões de brasileiros, o que configura um tratamento de dados em larga escala, a escolha por uma arquitetura informacional centralizada torna-se mais propensa a ser alvo de incidentes de segurança severos, uma vez que um único episódio poderia dar acesso a uma grande quantidade e diversidade de dados pessoais dos cidadãos, inclusive dados sensíveis, como os dados biométricos. Além disso, os incidentes de segurança envolvendo dados biométricos revelam um potencial lesivo ainda maior, uma vez que são dados diretamente relacionados ao corpo do titular e, consequentemente, não podem ser alterados.	Federativa do Brasil, conforme art. 1º, III da Constituição Federal. Segundo Informe do Alto Comissariado das Nações Unidas para os Direitos Humanos, de agosto de 2018 (A/HRC/39/29), "roubo de identidade baseado em dados biométricos é extremamente difícil de remediar e pode afetar severamente os direitos de um indivíduo."
Inviabilização do exercício dos direitos dos titulares previstos na LGPD pelos cidadãos	A plataforma gov.br, que utiliza a Base de Dados da ICN para autenticação de seus usuários, até onde se tem visibilidade de sua interface e política de privacidade, não possui um canal de comunicação direto e adequado para que os cidadãos possam solicitar a confirmação da existência do tratamento de dados, o acesso aos seus dados tratados e a retificação de dados incorretos ou desatualizados.	Violação da autodeterminação informativa, compreendida como um desdobramento do direito fundamental à proteção de dados pessoais, disposto no art. 5º, LXXIX da Constituição Federal.

GRUPO 2
Riscos de exclusão de cidadãos do acesso a políticas públicas

Fonte do risco identificado	Motivo	Direitos fundamentais e liberdades civis potencialmente violados pelos riscos identificados
Exclusão do acesso a serviços públicos de pessoas que não possuem qualquer documento de identidade	A plataforma gov.br utiliza a BDICN para a autenticação de seus usuários a partir de um *login* único, de modo que, a fim de ter acesso aos serviços públicos digitalizados via gov.br, os cidadãos precisam ter seus dados pessoais catalogados na BDICN. Para tanto, é necessário que estes tenham algum documento de identificação, o que depende da emissão de uma certidão de nascimento - o "documento fundacional" brasileiro. Ficam excluídos do gov.br, portanto, aqueles que não possuem esse documento, sendo essa fatia da população mais numerosa nas regiões Norte e Nordeste.	Exclusão de acesso a direitos e políticas públicas, como por exemplo os direitos sociais relativos ao trabalho e à seguridade social, como a impossibilidade de emitir a Carteira de Trabalho e Previdência Social (CTPS) e realizar a prova de vida junto ao Instituto Nacional do Seguro Social (INSS), ambos estabelecidos constitucionalmente como direitos sociais no art. 6º.
Exclusão do acesso a serviços públicos de pessoas que possuam algum tipo de inadequação em seus documentos de identidade	A inadequação de documentos de identidade de pessoas trans tem o potencial de exclusão dessa população do acesso ao gov.br e, consequentemente, dos serviços públicos por meio da plataforma acessados. Tal risco decorre da possibilidade de os dados que constituem a BDICN não corresponderem à identidade de gênero da pessoa, seja porque ela ainda não procedeu com a retificação ou porque as bases de dados que compõem a BDICN ainda não foram atualizadas com as informações devidamente retificadas. Além disso, o risco de exclusão pode, também, se manifestar a	Exclusão de acesso a direitos e políticas públicas, como por exemplo os direitos sociais relativos ao trabalho e à seguridade social, como a impossibilidade de emitir a Carteira de Trabalho e Previdência Social (CTPS) e realizar a prova de vida junto ao Instituto Nacional do Seguro Social (INSS), ambos estabelecidos constitucionalmente como direitos sociais no art. 6º.

	partir de conflitos entre os dados retificados em certidões de nascimento, mas que ainda não foram retificados no banco de dados da justiça eleitoral.	
Exclusão do acesso a serviços públicos de sujeitos hipervulneráveis, como crianças, adolescentes, idosos e pessoas com deficiência	Crianças e adolescentes: **(i)** Em razão da idade, os seus dados não compõem as bases de dados da Justiça Eleitoral e dos Departamentos Estaduais de Trânsito (DETRAN). **(ii)** Por não possuírem dados biométricos registrados na BDICN, podem ser impossibilitados de alcançar o nível máximo de autenticação, que é concedido por meio de validação biométrica dos dados da Justiça Eleitoral e pela validação de dados em certificados digitais. Pessoas idosas: **(i)** A exclusão está associada a dificuldades de uso de computadores, celulares e Internet, decorrentes de analfabetismo e analfabetismo funcional. Pessoas com Deficiência: **(i)** As ferramentas de autenticação disponíveis na plataforma gov.br não são acessíveis e inclusivas a todas as pessoas com deficiência.	Crianças e adolescentes: **(i)** Dificuldade ou inviabilidade de exercer direitos e gozar de políticas e serviços públicos digitais, violando o art. 3º do Estatuto da Criança e do Adolescente. Pessoas idosas: **(i)** Inviabilidade do exercício de direitos sociais relacionados à pessoas idosas, como o acesso à previdência social, estabelecido pelo art. 6º da Constituição Federal. Pessoas com Deficiência: **(i)** Dificuldade ou impossibilidade de acessar serviços públicos digitais, em razão da falta de acessibilidade, violando o art. 4º do Estatuto da Pessoa com Deficiência.
Exclusão do acesso a serviços públicos de pessoas em razão da falta de acesso pleno à Internet	Nessa hipótese, a exclusão se dá em razão da impossibilidade de o cidadão utilizar a plataforma gov.br, seja pela ausência total de acesso à Internet ou pela ausência de um acesso pleno à Internet.	Exclusão de acesso a direitos e políticas públicas, como por exemplo os direitos sociais relativos ao trabalho e à seguridade social, como a impossibilidade de emitir a Carteira de Trabalho e Previdência Social (CTPS) e realizar a prova de vida junto ao

	Segundo dados recentes, a ausência de acesso pleno à Internet ocorre, mais frequentemente, entre as pessoas de classes sociais mais vulneráveis, que inclusive deixam de acessar serviços públicos por falta de conexão.	Instituto Nacional do Seguro Social (INSS), ambos estabelecidos constitucionalmente como direitos sociais no art. 6º.

A partir do mapeamento dos riscos decorrentes da implementação da ICN e da utilização de sua base de dados para autenticação de usuários na plataforma gov.br, este estudo conclui pela necessidade de realização de um relatório de impacto à proteção de dados pessoais (RIPD), previsto pela Lei Geral de Proteção de Dados (LGPD). A recomendação para elaboração do RIPD está ancorada na constatação de que as atividades de tratamento de dados conduzidas no âmbito da ICN e na utilização da BDICN para autenticação de usuários na plataforma gov.br são operações que geram elevado risco aos titulares, considerando que há o tratamento de um grande volume de dados pessoais, inclusive dados sensíveis, como os dados biométricos. Isso, portanto, resulta na obrigatoriedade de elaboração do RIPD para as duas políticas públicas em análise neste *policy paper*: a Identificação Civil Nacional e a utilização da Base de Dados da ICN para a autenticação de usuários na plataforma gov.br.

No âmbito nacional, o RIPD ainda está em processo de regulamentação pela Autoridade Nacional de Proteção de Dados (ANPD), previsto para o biênio 2021-2022. Entretanto, os documentos oficiais elaborados pela Autoridade acerca do assunto já apontam critérios que ensejam alto risco para determinada atividade de tratamento de dados e, consequentemente, tornam a condução de um RIPD obrigatória. É o caso da Resolução CD/ANPD nº 2 de janeiro de 2022, que indica o tratamento de dados em larga escala e a utilização de dados pessoais sensíveis, característicos de ambas as políticas públicas, como gatilhos para constatação de alto risco. Em paralelo, o "Guia Orientativo: aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral", elaborado pela ANPD em conjunto com o Tribunal Superior Eleitoral (TSE), em 2021, (TSE, 2021a) afirma ser obrigatória a condução do RIPD em contextos que ofereçam alto risco ao titular de dados pessoais, além de indicar que a elaboração do RIPD seria altamente recomendada nos cenários em que haveria o tratamento de dados sensíveis e em larga escala.

Além da condução de um RIPD, a análise conduzida neste *policy paper* conclui pela obrigatoriedade de sua publicização. Isso porque o RIPD não é um documento voltado para verificação de conformidade de determinada atividade de tratamento de dados, mas

um documento vivo cujo foco está no titular de dados. Trata-se, por essência, de instrumento voltado à garantia dos direitos fundamentais e liberdades civis dos cidadãos. Nesse sentido, o dever de tornar público o RIPD decorre tanto da finalidade do próprio documento quanto, em operações de tratamento de dados realizadas pelo poder público, dos princípios constitucionais da própria Administração Pública, especialmente o princípio da publicidade, que determina que seus atos sejam públicos e acessíveis ao cidadão.

1. Introdução

1.1. A Associação Data Privacy Brasil de Pesquisa e o projeto *Accountability* e Identidade Civil Digital

O Data Privacy Brasil é um espaço de intersecção entre a escola Data Privacy Ensino e a Associação Data Privacy Brasil de Pesquisa. A Associação Data Privacy Brasil de Pesquisa é uma entidade civil sem fins lucrativos sediada em São Paulo. A organização dedica-se à promoção da proteção de dados pessoais e outros direitos fundamentais diante da emergência de novas tecnologias, desigualdades sociais e assimetrias de poder. Conta com uma equipe multidisciplinar de diferentes regiões brasileiras que desenvolve pesquisas de interesse público, notas técnicas, textos de análise sobre assuntos emergentes, formações com agentes decisórios e com a sociedade de um modo geral.

A Associação acredita na proteção de dados pessoais como um dos fundamentos da democracia e que precisa ser vista a partir da perspectiva da justiça social e assimetrias de poder. Trabalha, assim, para a promoção de uma cultura de proteção de dados e para que os direitos digitais sejam direitos fundamentais de todas e todos, conduzindo pesquisas abertas ao público, orientadas por um forte compromisso social e com financiamento ético.

Este relatório, produzido exclusivamente pela Associação, apresenta os resultados da pesquisa realizada no âmbito do projeto *Accountability* e Identidade Civil Digital (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, s.d a), financiado pela Open Society Foundations. Iniciado em junho de 2021, o projeto tem por objetivo compreender e mapear os sistemas de identidade civil digital que estão sendo desenvolvidos e implementados no contexto brasileiro A partir disso, o projeto tem o intuito de colaborar com a construção de uma sólida cultura de proteção de dados, com enfoque específico em medidas de governança e *accountability*, em especial as avaliações de impacto e risco, considerando que tais mecanismos são imprescindíveis para a garantia de direitos e liberdades fundamentais dos titulares de dados.

Em outras palavras, partindo de um conjunto de preocupações acerca das desigualdades e assimetrias existentes entre Estado e indivíduos e considerando os riscos-benefícios inerentes aos processos de datificação, o projeto busca avançar na reflexão sobre como melhor modelar a política pública de implementação de uma identidade civil digital, tão importante para o exercício da cidadania. Para além de pautar e compreender, respectivamente, a obrigatoriedade e a função de relatórios de impacto à proteção de dados pessoais na implementação de sistemas de identificação civil, este estudo faz uma análise descri-

tiva e avaliativa sobre como essa política de Estado se desenvolveu ao longo da última década no Brasil. O fio condutor do projeto, nesse sentido, é o enquadramento da proteção de dados pessoais como um eixo central na construção de uma relação de confiança e de redução de assimetria informacional entre Estado e cidadãos.

A partir do objetivo do projeto, a Associação tem conduzido diversas atividades, dentre as quais destacam-se a participação, na condição de expositores, na Turing Trustworthy Digital Identity Conference (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, s.d b), organizada pelo Instituto Alan Turing, do Reino Unido, e a condução de um workshop sobre relatório de impacto à proteção de dados pessoais e poder público durante a edição de 2021 da Semana de Inovação da Escola Superior de Administração Pública (ENAP) (DATA PRIVACY BRASIL, 2022).

A equipe da Associação também realizou, no âmbito do projeto, uma oficina fechada (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, s.d c) direcionada a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), Tribunal Superior Eleitoral (TSE) e Secretaria de Governo Digital (SGD), os principais atores envolvidos tanto na regulamentação do relatório de impacto à proteção de dados pessoais quanto na implementação do principal sistema de identidade digital no Brasil. O objetivo desse espaço de interação, que contou com a presença de especialistas nacionais[3] e internacionais, do Norte e Sul Global[4], foi o de fomentar o debate acerca desse importante instrumento estabelecido pela Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente sobre a obrigatoriedade de elaboração de relatórios de impacto e a sua respectiva metodologia em vista da singularidade das operações de dados no contexto de iniciativas de identidade civil digital.

1.2. Entre a visibilidade e a exclusão: um mapeamento dos riscos da Identificação Civil Nacional e do uso de sua base de dados para a plataforma gov.br

Como apontado anteriormente, o intuito deste *policy paper* é apresentar os resultados da pesquisa desenvolvida durante o primeiro ano do projeto *Accountability* e Identidade Civil Digital. Nesse sentido, o documento analisa, em primeiro lugar, a Identificação Civil

3 A oficina contou com a participação da Coordenadora Geral de Normatização da ANPD, Isabela Maiolino, e com a participação da professora do Data Privacy Brasil, Maria Cecília Oliveira Gomes, sobre o Relatório de Impacto no cenário e na legislação brasileira.

4 Para além de especialistas nacionais, a oficina contou com a participação de: Dariusz Kloza e Nikolaos Ioannidis, membros do d.pia.lab, centro de pesquisa vinculado à Universidade Livre de Bruxelas; Gabriela Zanfir-Fortuna, Kelsey Finch e Lee Matheson, membros do Future of Privacy Forum; Teki Akuetteh, pesquisadora ganense e diretora do Africa Digital Rights Hub, e Carlos Guerrero, pesquisador peruano do Instituto para la Sociedad de la Información y Cuarta Revolución Industrial.

Nacional (ICN), estabelecida pela Lei 13.444/2017, uma vez que esta é a principal iniciativa de unificação do sistema brasileiro de identificação civil. Ademais, estuda também a utilização da base de dados que constitui o sistema da ICN para autenticação de usuários na plataforma gov.br no acesso a serviços públicos, a qual serve como o principal portal do governo federal para a concretização de sua transformação digital.

Para concretizar tal análise, este trabalho parte do dilema de que o cidadão precisa ser conhecido (IGO, 2018) e, em certa medida, datificado - ou, em última instância, vigiado - pelo Estado para acessar serviços e políticas públicas. Irrompe, assim, uma encruzilhada entre o exercício da cidadania e a vigilância, cujo ponto de saída é a principal ambição das leis de proteção de dados ao afirmar direitos e deveres entre o titular dos dados e quem os manufatura. O presente *policy paper*, desse modo, debruça-se sobre quais são os riscos e benefícios a direitos fundamentais e liberdades civis que podem emergir tanto da implementação de um sistema unificado de identificação civil quanto da utilização da identidade digital como uma mediadora de acesso a serviços públicos digitalizados. A partir de uma extensa revisão bibliográfica, apoiada por abordagens qualitativas e dedutivas de análise, foi possível identificar dois grandes eixos de análise: (i) os riscos-benefícios relacionados à arquitetura informacional centralizada da ICN; e (ii) os riscos relacionados à exclusão de cidadãos do acesso a políticas públicas decorrentes da digitalização de políticas públicas.

Dessa forma, este relatório tem por objetivo auxiliar o poder público e outros agentes decisórios no processo de reflexão para a governança em rede dos riscos identificados na implementação da Identificação Civil Nacional e na utilização de sua base de dados para autenticação de usuários na plataforma gov.br. Além de se posicionar pela obrigatoriedade da condução e publicização de relatório de impacto à proteção de dados pessoais (RIPD) para tal política, este trabalho avança na discussão sobre a natureza dos riscos em jogo e, por conseguinte, sobre como mobilizar efetivamente tal ferramenta de *accountability* prevista pela Lei Geral de Proteção de Dados.

Para tanto, este documento é divido em 06 (seis) capítulos, os quais tratam dos principais temas que se relacionam com o desenvolvimento de um sistema unificado de identificação civil, quais sejam: Introdução (capítulo 1); Identidade civil nacional unificada e digitalização do governo: políticas de Estado (capítulo 2); Riscos de abuso no tratamento de dados pessoais: a arquitetura informacional da ICN e a disciplina da proteção de dados pessoais (capítulo 3); Riscos de exclusão dos cidadãos do acesso aos serviços públicos plataformizados no gov.br (capítulo 4); Endereçando os riscos a direitos fundamentais e liberdades civis: medidas de *accountability* e o Relatório de Impacto à Proteção de Dados (capítulo 5); e, finalmente, as Conclusões (capítulo 6).

Neste primeiro capítulo, será feita uma breve contextualização sobre o cenário internacional de desenvolvimento e implementação de sistemas unificados de identidade digital, momento em que serão apontados também alguns dos problemas associados a tais sistemas que já foram mapeados em pesquisas de outros países. Em sequência, no segundo capítulo, será abordado o histórico nacional de criação de um sistema único de identificação civil e o contexto de transformação digital do Brasil. Nesse ponto, serão retomadas algumas das iniciativas de digitalização do governo, as quais culminaram no cenário em que o país se encontra atualmente.

Partindo de tal cenário, o terceiro capítulo irá esmiuçar a arquitetura informacional da Identificação Civil Nacional, com intuito de descrever a estrutura da Base de Dados da ICN e como se dá o fluxo informacional dessa política pública. Dessa forma, irá auxiliar na identificação de possíveis riscos relacionados a abusos no uso dos dados pessoais tratados nesse sistema unificado de identificação civil. Posteriormente, o quarto capítulo - irá analisar a atual utilização da Base de Dados da ICN para a autenticação de usuários na plataforma gov.br, explorando os riscos de exclusão de cidadãos que dela podem decorrer.

A partir do delineamento dos riscos-benefícios decorrentes tanto da arquitetura informacional centralizada da ICN quanto da utilização de sua base de dados para autenticar usuários no acesso a serviços públicos, este *policy paper* conclui que a política de uso da BDICN para acesso ao gov.br deve ser precedida de instrumentos de transparência e *accountability*, notadamente de relatórios impacto à proteção de dados pessoais.

Assim, o texto tratará, criticamente, em seu quinto capítulo, do risco enquanto elemento central na gramática atual da proteção de dados pessoais. Finalmente, no sexto capítulo, serão feitas recomendações concretas sobre não apenas a necessidade de se conduzir e tornar público o RIPD em sede de implementação de políticas públicas como a ICN, mas, também da natureza dos efeitos adversos em jogo.

1.3. Identidade civil digital, políticas públicas e vigilância

Para situar o *policy paper* na discussão atual dos sistemas de identidade civil digital no mundo, é necessário fazer um breve histórico das reflexões mais relevantes já realizadas sobre o assunto.

Historicamente, o registro e identificação de pessoas pelo Estado ocorria para facilitar o recolhimento de impostos e para garantir que os benefícios do Estado fossem recebidos pelo cidadão. O controle da população a partir do uso de identificação diferiu ao longo do

tempo, mas certo é que a demanda por documentos de identidade é um lugar comum no mundo moderno (LYON, 2009).

Especificamente no que diz respeito a sistemas de identidade civil digital, Lyon (2009) destaca a necessária perspectiva de economia política por detrás do desenvolvimento de uma indústria de segurança, que inclui o investimento em sistemas de identidade digital, após o atentado do 11 de setembro de 2001 nos EUA.

Além dessa visão de um sistema de identidade para preservação da segurança nacional, tem despontado mundialmente uma agenda para a disseminação de sistemas de identidade para desenvolvimento socioeconômico, especialmente com foco em países e regiões mais pobres do mundo, nos quais ainda existe uma porção importante de pessoas ainda sem registro civil (MARTIN, 2021). A identidade digital seria, portanto, a solução para o registro dessa população e, consequentemente, portal para acesso a direitos essenciais, bem como a serviços e políticas públicas na educação, saúde, crédito, assistência e proteção social (MASIERO, BAILUR, 2021).

O discurso por esse potencial defendido pela agenda de identidade digital para desenvolvimento, entretanto, tem sido confrontado por registros de experiências de violação de direitos de cidadãos na aplicação prática de tais sistemas. É o que aponta a literatura acadêmica - e daí a importância de se ter a implementação de sistemas de identidade digital como objeto de pesquisa (MASIERO, BAILUR, 2021).

Na linha da agenda de identidade digital para o desenvolvimento, é importante notar que existem similaridades entre a maioria dos sistemas de identidade digital que têm sido implementados em países do Sul Global. A organização da sociedade civil Access Now (SAWHNEY, CHIMA, AGGARWAL, 2021) denomina esses sistemas de "Big ID": amplos programas de identificação, promovidos ou ligados ao setor público, que buscam designar a cada cidadão um identificador digital único e onipresente, armazenam dados biométricos e demográficos em uma base de dados centralizada e que autenticam identidades através de um sistema também centralizado, com frequência utilizando autenticação biométrica para esse processo. Inclusive, fator relevante no desenvolvimento dos sistemas de identidade digital e no acesso a serviços públicos em países de renda baixa e média é a proliferação do uso de biometria. Enquanto isso, em países ricos, o emprego de biometria é mais frequente para atividades de investigação e segurança (GELB, CLARK, 2013).

A proposta de identidade digital como forma de desenvolvimento, nessa esteira, está alinhada com a iniciativa *Identification for Development* (ID4D), do Banco Mundial. O objetivo da iniciativa é justamente fornecer acesso a serviços e promover o exercício de

direitos por meio da identidade digital. Ela considera que a identificação digital é o meio adequado para atingir o objetivo 16.9 da Agenda de Desenvolvimento Sustentável da ONU de fornecer identidade legal para todos, até 2030, incluindo certidão de nascimento (BANCO MUNDIAL, 2022a). Vale pontuar, conforme ressaltado por Martin (2021), que o objetivo de Desenvolvimento Sustentável 16.9 não menciona o uso de tecnologias digitais, mas o Banco Mundial e outros atores, sobretudo nos últimos anos, uniram as duas agendas - a de fornecimento de identidade legal e a de digitalização de serviços e sistemas - em uma agenda política específica. O Banco Mundial atua nesse âmbito com diversos países, fazendo diagnósticos dos sistemas de identificação por eles utilizados e até mesmo financiando a implementação de novos sistemas de identidade. No Brasil, até o momento, o avanço do ID4D se restringiu à elaboração de relatório de um diagnóstico do sistema de identidade (BANCO MUNDIAL, 2022b).

A implementação de sistemas de identidade digital em países do Sul Global traz uma questão imediata acerca da proteção dos dados pessoais dos cidadãos, considerando que parte significativa desses países não possui legislação protetiva de dados, ou ainda que possua, não conta com uma cultura forte de proteção de dados pessoais consolidada. A Índia, por exemplo, que tem o sistema de identidade digital com maior destaque na literatura acadêmica, o Aadhaar, o lançou há mais de uma década e ainda não tem uma legislação de proteção de dados (MARTIN, 2021). O que se verifica, assim, é um descompasso entre a proposta do sistema de identidade digital como um objetivo de desenvolvimento, que seria benéfico ao cidadão, e a infraestrutura legal dos países que o implementam. Em outras palavras, verifica-se um descompasso entre as necessidades e demandas de visibilidade por parte de quem precisa ser assistido pelo Estado para acesso a direitos e serviços e uma necessária e correspondente infraestrutura jurídica-institucional de governança. Nesse quadro, Martin (2021) destaca a necessidade de, além da legislação, os países possuírem uma capacidade regulatória efetiva de proteção de dados pessoais.

Um exemplo recente de diálogo entre proteção de dados e a implementação de um sistema de identidade digital ocorreu no Quênia. O sistema de identidade digital queniano foi criado em janeiro de 2019. A partir de março do mesmo ano, teve início o processo de coleta de dados dos cidadãos, incluindo de GPS e DNA, para alimentar o sistema de identidade. Posteriormente, em novembro de 2019, foi promulgada a legislação local de proteção de dados e, em janeiro de 2020, a Corte Superior do Quênia (Kenyan High Court), em processo ajuizado por organizações da sociedade civil impugnando o sistema de identidade digital, determinou que a coleta de dados de GPS e DNA era inconstitucional. Além disso, a Corte entendeu que a continuidade da implementação do sistema e processamento dos dados já obtidos dependia do cumprimento de uma legislação adequada a preceitos constitucionais como o da privacidade. A despeito dessa decisão, o governo continuou

a implementação do sistema, e houve novo ajuizamento de ação judicial pela sociedade civil para que, antes do uso efetivo do sistema, fosse conduzido um relatório de impacto à proteção de dados pessoais (RIPD), previsto na legislação de proteção de dados do Quênia. Enfim, em outubro de 2021, a Corte Superior do Quênia confirmou a necessidade da realização do RIPD antes da implementação do sistema (OPEN SOCIETY FOUNDATIONS, 2022; NATION, 2021).

Como no caso queniano, a pandemia da Covid-19[5] incentivou o desenvolvimento de soluções de identidade digital por todo o mundo, dado sua característica inerente de permitir a realização de transações comerciais e medidas de assistência social enquanto os indivíduos mantêm o isolamento social, assim como por serem associados com propostas de certificados de imunização e vacinação (MARTIN, 2021). Países da África e da Ásia, em especial, após o início da pandemia e alguns com apoio financeiro do Banco Mundial, iniciaram a implementação de sistemas de identidade nacional digital utilizando o MOSIP, uma plataforma *open-source*, baseada no sistema de identidade digital indiano Aadhaar, financiada pela Fundação Bill e Melinda Gates, Sir Ratan Tata Trust e Omidyar Network (MARTIN, 2021). A mesma tendência é observada no Brasil, onde o uso da Base de Dados da ICN para login no gov.br foi implementado durante a pandemia, e se viu o acesso ao gov.br e seu número de usuários crescer vertiginosamente durante o período de emergência sanitária. O número de brasileiros que utilizavam os serviços do gov.br era de 1,7 milhão em janeiro de 2019 e cresceu para 113 milhões em setembro de 2021, atingindo, em junho de 2022, 130 milhões de usuários, equivalente a 80% da população brasileira acima de 18 anos no país (C MARA DOS DEPUTADOS, 2021, GOVERNO FEDERAL, 2022c).

Do recolhimento de tributos, passando por acesso a serviços e políticas públicas e chegando ao combate à pandemia, nota-se que há historicamente uma interdependência entre vigilância e identificação do cidadão pelo Estado. Para suas interações com o Estado, o cidadão precisa ser visível (IGO, 2018). Sua identificação - e porque não, sua catalogação - é a chave da porta de entrada da burocracia estatal. Essa constatação, diante da compreensão sobre o estado da arte da implementação de sistemas de identidade civil digital pelo mundo, traz duas reflexões, as quais, em certa medida, representam pressupostos basilares que percorreram todo este estudo.

5 "Dados Virais", pesquisa realizada pela associação, se dedicou à identificação, mapeamento e análise das tecnologias utilizadas ou patrocinadas pelo poder público brasileiro para o enfrentamento da Covid-19, em todos os níveis da federação. As tecnologias selecionadas tinham como base a utilização de dados pessoais, em alguns casos, dados anonimizados dos cidadãos (ANDRADE *et al*, 2021).

A primeira delas está relacionada ao surgimento das leis de proteção de dados pessoais e a sua ligação à demanda do Estado em conhecer seus cidadãos para elaboração de políticas públicas (MAYER-SCHÖNBERGER, 1997). Leis de proteção de dados empoderam outros atores que não apenas os cidadãos, titulares dos dados. Não por outra razão, esses outros atores são chamados de agentes de tratamento de dados, afinal também detêm agência sobre tais bits de informação. Por exemplo, como será explorado mais a frente, eles detêm a prerrogativa de manipulação dos dados independentemente da necessidade do consentimento do seu titular, em determinados casos. O direito, portanto, não é um elemento neutro na correlação de forças entre quem vigia e é vigiado. O que está em disputa é como arranjos legais-institucionais de governança de sistemas de identidade civil e de proteção de dados podem ser mobilizados para reduzir as assimetrias de poder entre esses dois polos - Estado e cidadãos.

A segunda reflexão é uma espécie de naturalização da vigilância quando acoplada à figura do Estado de bem estar social. Ao mapear a literatura do campo e se apoiar em estudos empíricos qualitativos sobre a percepção pública de ameaças à privacidade, Nathalie Maréchal (2015) mostra como há pouca atenção e, por conseguinte, quase nenhuma resistência quando quem vigia é o Estado na condição de prestar algum tipo de assistência ao vigiado. Dito de outra forma, práticas e o próprio conceito de vigilância são menos visíveis quando, paradoxalmente, o cidadão é mais visível e vigiado.

Nesse mesmo sentido, em relação ao Brasil, Murakami Wood e Firmino (2009), ao averiguar a opinião da população sobre um novo sistema de identidade único nacional, constataram que a resposta majoritária a esse sistema era positiva. A percepção geral constatada pelos pesquisadores, que entrevistaram desde líderes comunitários, ativistas de direitos humanos e membros da polícia, todos de diversas seções do espectro político, foi de que o sistema seria uma garantia contra o anonimato, o qual, por sua vez, ensejaria abusos pelo Estado ou por outras pessoas maliciosas. O sistema de identidade, nesse sentido, não era visto como um meio de intrusão ou controle pelo Estado. É dizer: nessa relação de interdependência entre vigilância e identificação, havia uma maior preocupação do brasileiro em ser identificado - ser visível. Há que se considerar, portanto, quando se trata da realidade nacional, a necessidade da visibilidade dos cidadãos para acesso a políticas públicas, ainda que, é certo, sem desconsiderar a proteção de seus dados, especialmente dos mais vulneráveis, que são os mais dependentes de políticas públicas e mais frequentemente, portanto, constam nas bases de dados estatais.

Partindo dessa complexa relação entre vigilância e identificação, este *policy paper* analisa o tema da identificação civil digital não enquanto um fim em si mesmo, mas enquanto mediador da relação entre Estado e cidadão para o acesso a serviços e políticas públicas.

Masiero e Shakti (2020), nessa compreensão da identificação civil digital como mediadora da relação Estado-cidadão, delineiam três perspectivas teóricas para o sistema de identidade digital da Índia, propondo uma análise integrada e não excludente de suas funções. A primeira visão é do Aadhaar como meio de datificação dos cidadãos e, a partir de então, determinante de sua elegibilidade para acesso a políticas públicas. A segunda é do Aadhaar como plataforma que possui fundação - a base de dados dos cidadãos - e a ela acoplados estão os serviços públicos, construídos a partir dessa fundação. A terceira perspectiva desenhada pelas autoras, enfim, é o Aadhaar como forma de vigilância mediada, na qual a vigilância não é exercida apenas pelo Estado, que detém a base de dados, mas também por todas as entidades que têm acesso a ela ou podem utilizar de seus dados. Desse modo, para além de uma arquitetura de vigilância centralizada e estatal, chegaria-se a um modelo de vigilância ampla e descentralizada[6].

Transpondo tal proposta teórica ao uso da BDICN para autenticação do cidadão no gov.br, caso brasileiro analisado neste trabalho, é possível verificar a datificação dos cidadãos por meio, justamente, da Base de Dados da ICN. Ainda, conforme determinado pela Lei da Identificação Civil Nacional (LICN), em seu art. 11, as informações da ICN podem ser utilizadas para determinação da elegibilidade do cidadão a políticas públicas. Em segundo lugar, ao tornar tal base de dados uma meio de autenticação da população no gov.br, acopla-se a uma estrutura fundacional uma série de serviços - até o momento, serviços públicos, mas a BDICN já foi também utilizada para autenticação de consumidores em serviços bancários, por exemplo. Por fim, é possível, ainda, compreender a ICN sob a perspectiva de facilitadora de uma vigilância mediada, dado o amplo acesso de órgãos da administração pública a suas informações e uso secundário de dados, aspecto que será tratado com mais profundidade no capítulo 3 deste *policy paper*.

A possível aplicação do modelo de análise do Aadhaar proposto por Masiero e Shakti (2020) ao caso brasileiro e as considerações sobre como têm sido implementados sistemas de identidade civil digital de forma semelhante em países do Sul Global, sob um mesmo discurso de desenvolvimento socioeconômico, são importantes na medida em que reforçam que os

6 A pesquisa "Dados Virais", constatou percentuais mais elevados de atores privados, de origem nacional, atuando no fornecimento e desenvolvimento de tecnologias de enfrentamento à Covid-19 para o setor público pela utilização de dados pessoais, sendo em cerca de 53,84% dos casos mediante contratos não onerosos. A pesquisa ressalta necessários pontos de atenção para a relação entre setor público e privado no fornecimento de tecnologia para serviços públicos essenciais. Em primeiro lugar, ainda que na época da pandemia, a tecnologia seja fornecida de maneira gratuita, tal tecnologia pode se tornar parte essencial de um serviço público e passar a fazer parte de um serviço pago, gerando uma situação em que a prestação de serviços públicos essenciais depende de empresas privadas. Além disso, é importante verificar como políticas públicas datificadas podem aumentar a dependência do Estado em relação ao setor privado, e nesse caso, como o setor privado passa a ter acesso a bancos de dados extremamente relevantes de cidadãos, sendo essencial determinar quem faz parte da cadeia de tratamento de dados, quem são os agentes, qual o país de origem, se há transferência internacional dos dados dos cidadãos brasileiros.

apontamentos do presente texto não se limitam à realidade brasileira. Isto é, ainda que o caso analisado seja o do Brasil, entende-se que as considerações a frente tecidas podem ser transpostas a discussões internacionais e de outros países sobre o tema.

2. Identidade civil nacional unificada e digitalização do governo: políticas de Estado

2.1. O Registro de Identidade Civil

Segundo Doneda e Kanashiro (2010), o Brasil faz parte do rol de países que implementaram um sistema de identificação descentralizado. Por não haver comunicação entre os sistemas de cadastramento do Registro Geral - ou RG -, é possível que um mesmo cidadão possua mais de uma cédula de identidade, com números de identificação distintos, provenientes de diferentes estados brasileiros (DONEDA, KANASHIRO, 2010). Nesse contexto, surge a proposta de desenvolver um sistema único de identidade no Brasil, com o intuito de lhe conferir maior grau de autenticidade diante dos diversos casos de fraudes em razão da fácil duplicação de documentos.

O histórico de tal iniciativa remonta aos anos 1990 – mais especificamente, ao ano de 1997 –, momento em que foi promulgada pelo governo federal, sob a presidência de Fernando Henrique Cardoso, a Lei 9.454/1997 –, a qual estabelecia o Registro de Identidade Civil (RIC). O RIC viria, assim, a substituir a atual Carteira de Identidade brasileira: o RG. Doneda e Kanashiro (2010) apontam que, nesse novo sistema, havia a previsão legal de um número único, o qual seria utilizado para identificar todos os cidadãos brasileiros, servindo, portanto, como um mediador para todas as suas relações, fossem elas públicas ou privadas.

Para cumprir o seu objetivo de se tornar um documento único de identificação civil, o RIC foi proposto a partir de uma arquitetura que concentrava diversos documentos, como a carteira de identidade, a Carteira Nacional de Habilitação (CNH), o Cadastro de Pessoa Física (CPF), o título de eleitor, a Carteira de Trabalho e Previdência Social (CTPS), o cadastro do indivíduo nos Programas de Integração Social e de Formação do Patrimônio do Servidor Público (PIS/PASEP) e seu número de registro no Instituto Nacional de Seguro Social (INSS) (KANASHIRO, DONEDA, 2012). Essa concentração ensejaria, portanto, a junção de diversas bases de dados.

A Lei nº 9.454/1997 entrou em vigor no momento de sua publicação, mas seu art. 5º previa a necessidade de sua regulamentação, a qual deveria ocorrer no prazo de 180 (cento e oitenta) dias, com a consequente implementação no prazo de 360 (trezentos e sessenta) dias. Apesar de a regulamentação do RIC ter acontecido somente 13 (treze) anos após a sua promulgação, no ano de 2010, quando foi publicado o Decreto nº 7.166/2010, o início de

sua implementação se deu anteriormente, em 2004, momento em que houve a aquisição dos equipamentos necessários à digitalização da identificação biométrica já contida no RG dos brasileiros (KANASHIRO, DONEDA, 2012).

Uma vez que houve o processo de regulamentação do RIC, iniciaram-se os procedimentos para a implementação, de fato, desse novo sistema de identificação. Sob a responsabilidade da Secretaria Executiva do Ministério da Justiça (SE/MJ), o projeto RIC contou com a assinatura de um Acordo de Cooperação Técnica entre o Ministério da Justiça e a Universidade de Brasília, o qual previu o desenvolvimento de estudos acerca dos processos e da infraestrutura necessária para a correta implementação do Registro de Identidade Civil. Nesse âmbito, uma série de relatórios técnicos (Ministério da Justiça e Segurança Pública, s.d) foram produzidos para subsidiar o processo de tomada de decisão do poder público federal em relação a tal política pública.

Em 2015, com a propositura do Projeto de Lei nº 1775/2015, o qual previa a criação de um outro sistema único de identificação civil, o Registro Civil Nacional (RCN) – que viria a ser aprovado, posteriormente, sob o nome de Identificação Civil Nacional (ICN) -, todas as atividades relacionadas à implementação do RIC foram suspensas.

Apesar dos esforços empreendidos para se alcançar a melhor implementação do RIC, ele nunca foi, de fato, implementado. Kang, Doneda e Santos (2016) apontam para o fato de que, provavelmente, as razões pelas quais o Registro de Identidade Civil nunca tenha sido implementado estão relacionadas ao alto custo de tal projeto.

2.2. A Identificação Civil Nacional

Como apontado anteriormente, no ano de 2015 foi proposto o Projeto de Lei (PL) 1775/2015, que previa a criação de um novo sistema único de identificação civil - o Registro Civil Nacional (RCN) - o qual revogaria o Registro de Identidade Civil (RIC)[7]. De iniciativa do governo federal em conjunto com a Justiça Eleitoral, o PL que propunha a criação do RCN foi assinado e submetido, à época, pelos Ministros da Justiça e da Secretaria da Pequena e Média Empresa - respectivamente, José Eduardo Cardoso e Guilherme Afiff Domingos.

De acordo com a justificativa do PL, o projeto tinha por objetivo a criação de um registro

7 Durante a tramitação do PL 1775/2015 na Câmara dos Deputados, o artigo que revogava o RIC foi retirado, de modo que, até os dias atuais, a lei que instituiu Registro de Identidade Civil continua em vigor, entretanto, sua implementação está suspensa.

civil nacional, acompanhado de um documento nacional de identificação, o que permitiria um relacionamento mais simplificado e seguro entre o cidadão e os órgãos públicos e privados (KANG, DONEDA, SANTOS, 2016).

Segundo Kang, Doneda e Santos (2016), para que fosse possível o cumprimento de seu objetivo, o PL previa a criação de um banco de dados formado pela união de duas bases de dados: a base de dados biométricos da Justiça Eleitoral e a base de dados do Sistema Nacional de Informações de Registro Civil (SIRC), bem como outras informações não contidas no SIRC, mas que estivessem disponíveis em outras bases de dados da Justiça Eleitoral ou de outros órgãos públicos.

Durante a tramitação do PL na Câmara dos Deputados, em 2016, foi realizada uma série de audiências públicas. Foram, ao todo, 16 reuniões técnicas, havendo nelas a predominância de participação de deputados, apesar de ter havido a participação de outros setores interessados. A participação da sociedade civil, porém, foi inexpressiva: apenas dois representantes do terceiro setor participaram das audiências públicas (KANG, LUCIANO e SANTOS, 2017).

Após a realização das reuniões técnicas e uma vez recebidas as propostas de emenda ao Projeto de Lei, o então relator do PL, deputado Júlio Lopes, apresentou um parecer substitutivo, o qual propunha algumas alterações substanciais ao texto originalmente submetido (KANG, LUCIANO, 2017). Em 2017, após a aprovação do PL nº 1.775/2015 no plenário da Câmara dos Deputados, o projeto de lei passou a tramitar no Senado sob a numeração PLC nº 19/2017.

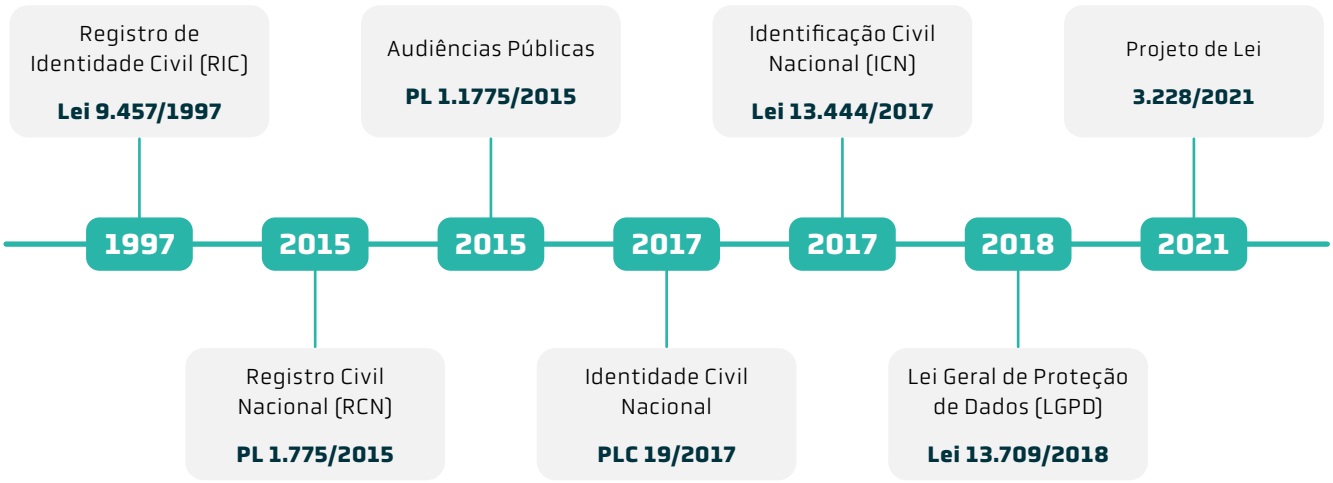
A partir desse momento, o Projeto de Lei Complementar (PLC) nº 19/2017 passou a fazer referência à criação de um sistema chamado Identificação Civil Nacional (ICN)[8]. Finalmente, ainda em 2017, o PLC foi aprovado pelo Senado e sancionado pelo então presidente Michel Temer: foi promulgada a Lei 13.444/2017 (ou LICN). Assim, a ICN passou a existir formalmente. O sistema foi estabelecido a partir de uma arquitetura informacional centralizada, herdada de outras iniciativas anteriores como o RIC, e sua composição é feita, majoritariamente, por dados biométricos, provenientes da base de dados do Tribunal Superior Eleitoral (TSE).

8 Segundo Kang e Luciano (2017), a mudança na nomenclatura do sistema de identificação se deu a partir da aceitação da emenda ao projeto de lei que visava a alteração do art. 1º do PL 1775/2015. A emenda modifica o nome do novo sistema de identificação, uma vez que, constitucionalmente, o registro civil é de caráter privado, sendo, portanto, inconstitucional a sua atribuição ao poder público, no caso à Justiça Eleitoral.

Desde a aprovação da LICN, esforços foram empreendidos para que houvesse a implementação de fato da Identificação Civil Nacional. Tais esforços foram intensificados a partir de 2018, quando da eleição do presidente Jair Bolsonaro, cuja gestão tem priorizado a transformação digital do governo brasileiro. Isso fica evidente com as movimentações feitas pela Secretaria de Governo Digital de ampliação dos serviços públicos digitalizados (GOVERNO FEDERAL, 2022) e com a definição do Projeto de Lei nº 3228/202, que altera a Lei da ICN, como uma prioridade legislativa para o ano de 2022 (BRASIL, 2022).

Ainda no que diz respeito aos esforços para a implementação da ICN, vale destacar o contrato firmado entre o Tribunal Superior Eleitoral e o Serviço Federal de Processamento de Dados (SERPRO), em dezembro de 2021 (TSE, 2021e). Segundo o instrumento, a Serpro operacionalizará a ICN, a partir da prestação de serviços de conferência biográfica e biométrica, pesquisa biográfica e emissão de Documento Nacional de Identificação (DNI), pelo período de 05 (cinco) anos (LOBO, 2022).

Abaixo, é possível visualizar uma linha do tempo que demarca as principais movimentações legislativas descritas nesta seção em direção à constituição de um sistema único de identidade civil:



A reconstrução dessa linha do tempo evidencia que o desenvolvimento de um sistema de identidade civil unificado atravessou praticamente todos os governos, de diferentes matrizes ideológicas, desde a retomada da democracia no Brasil. A instituição de um sistema desse tipo pode ser colocada, portanto, como uma política de Estado de longa data e, ao mesmo tempo, ainda em estágio de maturação.

2.3. Um breve histórico da transformação digital brasileira

As iniciativas relacionadas ao desenvolvimento de um sistema único de identidade civil brasileiro estão diretamente atreladas aos processos de transformação digital do Brasil, cujo início remonta ao ano 2000, período em que foi aprovada a Proposta de Política de Governo Eletrônico para o Poder Executivo e teve início, consequentemente, a caminhada em direção a um governo digital (THORSTENSEN, ZUCHIERI, 2020).

Apesar de diversas iniciativas de digitalização do Governo terem sido iniciadas ao longo dessas últimas duas décadas, foi somente em 2016 que se estabeleceu uma estratégia mais sólida para o desenvolvimento de um Governo Digital, denominada de Estratégia de Governança Digital (EGD). Tal política, aliada ao interesse de modificar a estrutura de governo eletrônico para a de governo digital[9], previa uma série de molduras e estruturas para orientar a implementação de programas e ações relacionadas ao processo de digitalização (OCDE, 2020).

Dois anos mais tarde, em 2018, a Estratégia de Governança Digital passou por uma série de atualizações. Essas, por sua vez, tinham por objetivo a definição de algumas prioridades relacionadas: (i) ao impulsionamento do uso de tecnologias digitais para transparência; (ii) às melhorias na prestação de serviço digital; (iii) à garantia de implementação de sistemas de identidade digital; e (iv) à integração dos serviços digitais a partir da implementação de tecnologias da informação, sistemas e dados interoperáveis, com intuito de aumentar a participação pública através de plataformas digitais (OCDE, 2020).

Findado o período de vigência de tal Estratégia, que durou entre os anos de 2016 e 2019, foi publicado novo documento do tipo, dessa vez para o período compreendido entre 2020 e 2022. Recebeu o nome de Estratégia de Governo Digital (Decreto nº 10.332, de 28 de abril de 2020) e seu objetivo final é o de oferecer digitalmente a totalidade dos serviços oferecidos pela União, por meio da plataforma gov.br. Para viabilizar o disposto na nova

9 Segundo o portal do Ministério da Economia (2019), a noção de Governo Eletrônico se dá a partir da evolução das Tecnologias da Informação e Comunicação (TICs), notadamente a Internet, que provoca mudanças nas formas como ocorrem as relações entre a Administração Pública e a sociedade. No Brasil, foram identificadas diversas iniciativas isoladas de oferecimento virtual de serviços públicos aos cidadãos, como a entrega de declaração de imposto de renda. Contudo, ainda existia uma infraestrutura deficitária, formada por diversas redes administradas isoladamente, de modo que os serviços oferecidos não atendiam a "padrões de desempenho e interatividade, interfaces com o usuário nem sempre eram amigáveis e se constatava um descompasso entre os diversos órgãos governamentais no ritmo de assimilação das TICs" (MINISTÉRIO DA ECONOMIA, 2019). O governo eletrônico, portanto, teve um papel fundamental na informatização dos processos internos da Administração Pública, porém se fazia necessário um deslocamento do foco nos processos internos da Administração para a relação entre Administração Pública e Sociedade. Nesse sentido surge a iniciativa de um governo digital, cujo objetivo é simplificar, tornar mais acessível e mais eficiente a relação entre cidadão e poder público na oferta de serviços aos cidadãos, por meio digital (MINISTÉRIO DA ECONOMIA, 2019).

norma, foi aprovada a Lei nº 14.129/2021, que dispõe sobre as regras, princípios e instrumentos para o Governo Digital e para o aumento da eficiência da administração pública.

O contexto da pandemia de Covid-19, ao modificar as dinâmicas sociais e exigir que se mantivesse o isolamento social como medida sanitária, provocou um processo de aceleração na transformação digital do governo federal. Sendo assim, de acordo com dados disponibilizados pela Agência Brasil em novembro de 2021, cerca de 72% dos serviços públicos oferecidos pelo Poder Executivo Federal foram adaptados para serem ofertados por meio de plataformas digitais (AGÊNCIA BRASIL, 2021). Nessa toada, a expectativa do governo federal é de que todos os serviços públicos federais sejam digitalizados até o ano de 2022, como é possível verificar no Decreto nº 10.996, de 14 de março de 2022, o qual altera a Estratégia de Governo Digital.

É preciso destacar, no entanto, que o processo de digitalização do governo não significa, *per se*, algo positivo. Em reportagem recente, o portal Telesíntese (2021) destacou uma fala feita pelo Ministro Aroldo Cedraz, do Tribunal de Contas da União (TCU), a qual fazia referência ao fato de a transformação digital de um país não se resumir apenas à digitalização de serviços públicos, devendo haver a compreensão de que toda a sociedade é parte desse processo. Nesse mesmo sentido, o voto proferido pelo Ministro Relator Vital do Rêgo, em sede do relatório de acompanhamento da Estratégia de Governança Digital, produzido pelo TCU em 2021, apontou que a ausência de uma abordagem sistêmica para o processo de transformação digital poderia resultar em limitações à prestação de serviços públicos de forma digital, de modo que, para que a população possa desfrutar, de fato, dessa transformação digital, a mera digitalização não é suficiente, sendo necessário que hajam investimentos em infraestrutura, conectividade, bem como em alfabetização digital dos cidadãos (TRIBUNAL DE CONTAS DA UNIÃO, 2021).

2.4. A plataforma gov.br

Em 2019, após a publicação do Decreto nº 9.756/2019, surge a plataforma gov.br. A iniciativa parte de um dos pilares da Estratégia de Governo Digital, o qual estabelece a necessidade de unificação dos canais de comunicação e de acesso a serviços públicos digitalizados.

Segundo a página de apresentação da plataforma, o gov.br está no estágio *beta* de desenvolvimento, o que significa dizer que o portal ainda está sendo aprimorado e não se encontra em sua versão finalizada. De acordo com o próprio governo federal, o gov.br:

> é um projeto de unificação dos canais digitais do governo federal. Mas ele é, acima de tudo, um projeto sobre como a relação do cidadão com o Estado deve ser: simples e focada nas necessidades do usuário de serviços públicos.
>
> Tudo começa pelo portal gov.br, que reúne, em um só lugar, serviços para o cidadão e informações sobre a atuação de todas as áreas do governo. Até dezembro de 2020 os sites do Governo estarão integrados, tornando o portal gov.br a entrada única para as páginas institucionais da administração federal, oferecendo ao cidadão um canal direto e rápido de relacionamento com os órgãos federais. (GOVERNO FEDERAL, s.d, sem paginação).

O pleno funcionamento do portal gov.br depende de processos de identificação e autenticação dos usuários, os quais acessam a plataforma a partir de um login único, constituído por seu número de CPF – Cadastro de Pessoa Física - e uma senha pessoal. As contas gov.br possuem três níveis de autenticação: bronze, prata e ouro. Tais níveis dizem respeito à forma como essas contas foram criadas e/ou validadas. Segundo o governo federal (2021), os diferentes níveis, que estão atrelados ao grau de segurança da validação dos dados do usuário, garantem diferentes tipos de acessos a serviços públicos digitais e transações que podem ser feitas via plataforma gov.br. O número de brasileiros que utilizavam os serviços do gov.br era de 1,7 milhão em janeiro de 2019 e cresceu para 113 milhões em setembro de 2021, atingindo, em junho de 2022, 130 milhões de usuários, equivalente a 80% da população brasileira acima de 18 anos no país (CÂMARA DOS DEPUTADOS, 2021, GOVERNO FEDERAL, 2022c).

Com o intuito de fortalecer o sistema nacional integrado de identificação dos cidadãos e de facilitar seu acesso aos serviços disponibilizados pela plataforma gov.br, foi firmado, em 2021, um Acordo de Cooperação Técnica (ACT) entre a Secretaria-Geral da Presidência da República, o Ministério da Economia e o Tribunal Superior Eleitoral, cujo objeto versa sobre a utilização do sistema da Identificação Civil Nacional (ICN) no contexto do portal gov.br (TRIBUNAL SUPERIOR ELEITORAL, 2021). O ACT visa a autenticação dos usuários da plataforma a partir da validação dos cadastros com os dados que constituem a Base de Dados da ICN - especialmente a base de informações biométricas da Justiça Eleitoral (TRIBUNAL SUPERIOR ELEITORAL, 2021).

A assinatura deste Acordo de Cooperação Técnica foi um dos primeiros movimentos em

direção à efetiva implementação da ICN[10], na medida em que constituiu o principal uso de sua base de dados até o momento - sua utilização para a validação e autenticação de usuários, junto à base de informações da Justiça Eleitoral, garante aos cidadãos o acesso ao nível ouro das contas gov.br e habilita-os a acessar todos os serviços públicos digitais disponíveis na plataforma.

O desenvolvimento da plataforma gov.br, vale ressaltar, faz parte de um movimento mais amplo observável internacionalmente de plataformização dos serviços públicos, acompanhando uma tendência mais geral de plataformização da sociedade. Segundo Poell, Nieborg e van Dijck (2021), a plataformização da sociedade pode ser definida como a penetração de infraestruturas, processos econômicos e estruturas de governança de plataformas digitais em diferentes setores socioeconômicos, que resulta na reorganização de práticas culturais e do imaginário social sobre essas plataformas. Nesse sentido, van Dijck, Poell e De Wall (2018) argumentam que a inserção de plataformas no cotidiano atual, ao promover a intensificação da coleta de dados sobre os indivíduos, permite que sejam datificados aspectos da vida que antes não eram quantificados, tais como, por exemplo, dados componentes de seus perfis comportamentais e dados de localização.

Inicialmente, é possível afirmar que este fenômeno de plataformização concentrava-se, majoritariamente, no setor privado, onde teve sua origem. Contudo, Dahl-Jørgensen e Parmiggiani (2020) apontam para a penetração recente das plataformas digitais no setor público, o que, por sua vez, corresponde ao desenvolvimento de infraestruturas digitais direcionadas ao oferecimento de serviços públicos aos cidadãos.

Nesse sentido, Dahl-Jørgensen e Parmiggiani (2020) afirmam ser comum a incorporação, de infraestrutura técnica pertencente a grandes empresas de tecnologia nas plataformas públicas, fato que representa um imbricamento entre o setor público e privado para o desenvolvimento de tecnologias, resultando em uma transgressão setorial[11] visível em outros momentos, como no desenvolvimento de tecnologias para combate ao Covid-19 (ANDRADE *et al.*, 2021). Essa transgressão, segundo as autoras, pode impactar os cidadãos em termos de inclusão e participação da sociedade, uma vez que as plataformas atuam diretamente na forma como os cidadãos engajam com os processos democráticos de tomada de decisão e interagem com o poder público (DAHL-JØRGENSEN, PARMIGGIANI, 2020).

10 Em fevereiro de 2022, o TSE anunciou a nova fase de implementação da Identificação Civil Nacional, a emissão do Documento Nacional de Identidade de forma faseada, de início para servidores públicos, após no Estado de Minas Gerais, e a partir de Fevereiro de 2023, disponível para toda população (TSE, 2022a).

11 Segundo Solano *et al* (2022) a noção de transgressão setorial pode ser compreendida pelo envolvimento de atores comerciais em espaços nos quais os seus modelos de negócio, práticas e molduras éticas estão em descompasso com os interesses de demais atores que compõem o debate público.

Ao lado do gov.br, dois exemplos de plataformização de serviços públicos ajudam a ilustrar o conceito. O primeiro deles é o serviço público de saúde do Reino Unido - o *National Health System* (NHS). Segundo Faulkner-Gurstein e Wyatt (2021), a lógica das plataformas passou a permear as mudanças nos objetivos e estratégias organizacionais do NHS nas últimas duas décadas. Desse modo, a sua plataformização tem sido oferecida tanto como política de Estado aberta, sem o estabelecimento de um prazo de validade, quanto como uma via estratégica para mudanças futuras. Em termos estruturais, o NHS coleta e armazena dados sobre os cidadãos que o acessam, o que serve ao propósito de facilitar e intermediar seu acesso ao serviço, e oferece infraestrutura e disponibiliza recursos de apoio à pesquisa, evidenciando a centralidade dos dados no processo de plataformização (FAULKNER-GURSTEIN E WYATT, 2021).

O componente da plataformização também é proeminente no exemplo do sistema de identidade digital indiano (Masiero e Shakti, 2020). Conforme anteriormente aludido, é possível interpretar o Aadhaar como uma plataforma que possui como base uma base de dados dos cidadãos e tem a ela acoplados serviços como a integração da identificação biométrica para recebimento pelos cidadãos dos programas de alívio de pobreza governamentais (MASIERO E SHAKTI, 2020).

3. Riscos de abuso no tratamento de dados pessoais: a arquitetura informacional da ICN e a disciplina da proteção de dados pessoais

O presente capítulo tem por objetivo apresentar a arquitetura informacional e a estrutura de governança da Identificação Civil Nacional, conforme estabelecidas pela Lei 13.444/201. A partir dessa descrição, serão identificadas as convergências e tensões entre a LICN e a LGPD e as mudanças propostas pelo Projeto de Lei nº 3228/2021, que pretende a alteração da LICN. Dentre os aspectos fundamentais abordados nesta seção, destaca-se a correlação entre uma arquitetura informacional centralizada e uma maior complexidade de governança. Para além de abordar questões de segurança de informação, o capítulo enfrenta, também, questões jurídicas controversas, como a possibilidade de usos secundários de dados pessoais da ICN e das próprias bases de dados que a constituem.

3.1. A estrutura de governança na Lei da Identificação Civil Nacional

a. O Comitê Gestor da ICN

A partir da leitura e análise das disposições legais estabelecidas na LICN, é possível identificar a existência de um órgão de governança: o Comitê Gestor da ICN (CGICN). Conforme as definições do art. 5º da Lei nº 13.444/2017, a composição do CGICN é feita exclusivamente por membros do poder público, entre eles representantes do poder público federal, do Tribunal Superior Eleitoral, da Câmara dos Deputados, do Senado Federal e, finalmente, do Conselho Nacional de Justiça.

Em termos de atribuições, o CGICN é competente para tecer recomendações sobre o padrão biométrico utilizado pelo sistema de identificação civil, os parâmetros técnicos e econômico-financeiro da prestação do serviço de conferência dos dados biométricos e as diretrizes para a administração do Fundo da Identificação Civil Nacional e gestão de seus recursos. Além disso, cabe ao CGICN orientar a implementação da interoperabilidade entre sistemas do Poder Executivo federal e da Justiça Eleitoral e estabelecer seu próprio regimento.

Trata-se, portanto, de um Comitê delineado por arranjo de governança que não se enquadra em um formato multissetorial, o qual, por sua vez, pode ser compreendido, segundo Almeida, Getschko e Afonso (2015), como aquele que visa a reunião dos principais setores interessados em determinados assuntos nos processos de tomada de decisão,

baseado em princípios democráticos de transparência e participação. Desse modo, ao congregar diversos atores da sociedade, como governo, setor privado, academia e terceiro setor, o modelo multissetorial permite a ampliação dos debates para o espaço público.

Considerando o objetivo da implementação de um sistema único de identidade civil - que se trata de uma política pública, com gerenciamento de recursos próprios e que se apoia sobre o tratamento de um alto volume de dados pessoais -, o fato de o Comitê Gestor da ICN não ser multissetorial, como são, por exemplo, o Comitê Gestor da Internet (COMITÊ GESTOR DA INTERNET BRASIL, s.d), o Comitê de Defesa dos Usuários de Serviços de Telecomunicações (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2021) e o Conselho Nacional de Proteção de Dados Pessoais (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2022), vai de encontro com a experiência brasileira de governança de sistemas complexos, a qual, historicamente, incentivou a participação de uma diversidade de setores da sociedade em processos decisórios e de aconselhamento em políticas públicas, ao lado do setor público.

Desse modo, existe a possibilidade de, pela opção legislativa de arranjo de governança para a ICN, haver a predominância de uma única perspectiva nas tomadas de decisão a ela relacionadas – potencial e predominantemente orientada a uma ideia de eficiência na prestação dos serviços e avanço da política de uma identificação única –, em detrimento da proteção do titular de dados.

b. Projeto de Lei nº 3228/2021 e as alterações no arranjo de governança da ICN

Em setembro de 2021, o governo federal encaminhou ao Congresso Nacional o Projeto de Lei (PL) nº 3228/2021, o qual altera a LICN, em movimento que trouxe à tona no debate público, novamente, os debates sobre a implementação de uma identidade civil digital (GARROTE *et al*, 2021a). O referido PL propõe algumas alterações à estrutura da ICN - inclusive modificações em sua arquitetura informacional - estas últimas, que serão mais a frente discutidas.

Elencado como uma das prioridades legislativas do governo federal para o ano de 2022, conforme disposições da Portaria nº 667/2022, o texto proposto prevê uma alteração no parágrafo primeiro do art. 5º da LICN, a qual adiciona ao rol de composição do CGICN um representante das unidades federativas e do Distrito Federal, a ser indicado pelo Ministro de Estado da Justiça e Segurança Pública. Apesar dessa proposta de alteração, os novos termos sugeridos pelo PL ainda mantêm o Comitê Gestor da ICN composto exclusivamente por membros do poder público.

c. O Comitê Gestor da ICN e o Decreto nº 10.900/2021

Ainda na esteira da discussão sobre a estrutura de governança da Identificação Civil Nacional, a Presidência da República publicou em dezembro de 2021 o Decreto nº 10.900/2021, o qual dispõe sobre o "Serviço de Identificação do Cidadão (SIC) e a governança da identificação das pessoas naturais no âmbito da administração pública federal direta, autárquica e fundacional" (BRASIL, 2021a). Tal serviço, por sua vez, é executado por meio da plataforma gov.br e a publicação do decreto cumpre com o objetivo de regulamentar sua utilização por entes públicos e privados.

Ao instituir e regulamentar o Serviço de Identificação do Cidadão[12], a norma acrescenta ao guarda-chuva da política da ICN uma nova operação de tratamento de dados. Isso ocorre porque o processo de autenticação do cidadão ao qual se refere o decreto utiliza, majoritariamente, a base de dados da Identificação Civil Nacional, combinada com o Cadastro Base do Cidadão e outras bases de dados que podem vir a ser incorporadas no SIC. É dizer, o texto legal insere a BDICN dentro de uma estrutura - informacional e de governança - ainda mais ampla.

O decreto institui, ainda, a Câmara-Executiva Federal de Identificação do Cidadão (CEFIC) e outorga a ela a competência de gestão do Serviço de Identificação do Cidadão, a qual engloba a utilização da BDICN. De tal forma, a criação da CEFIC representa, em alguma medida, uma alteração no arranjo de governança da ICN, pois gera um processo de centralização ainda maior em relação à sua atual estrutura. No caso, a composição da CEFIC prevista no art. 13 do Decreto nº 10.900/2021 conta exclusivamente com membros do governo federal: representantes da Secretaria-Geral da Presidência da República, do Ministério da Justiça e Segurança Pública e do Ministério da Economia.

Cumpre destacar que a recente criação da CEFIC dificulta a visualização de como será constituída a sua relação com o Comitê Gestor da ICN, uma vez que, inicialmente, é possível vislumbrar uma sobreposição entre as políticas e estruturas sobre as quais compete a ambos os órgãos se debruçar.

Como apontado anteriormente, a composição multissetorial de comitês gestores de políticas públicas complexas não é um elemento estranho à experiência brasileira. Isso porque o desenvolvimento e gestão desse tipo de política demandam uma pluralidade de visões

12 Segundo o art. 2º do Decreto 10.900/2021, o "Serviço de Identificação do Cidadão é o conjunto de procedimentos de gestão e verificação da identidade das pessoas naturais perante a administração pública federal direta, autárquica e fundacional, por meio da Plataforma gov.br."

necessária para que todos os setores da sociedade possam delas se beneficiar adequadamente. Desse modo, ao priorizar uma composição não multissetorial de instâncias como o CGICN e a CEFIC, a participação ativa de setores da sociedade que se beneficiarão e serão afetados diretamente pelas escolhas relacionadas à condução da ICN e da plataforma gov.br pode ser potencialmente comprometida.

3.2. A arquitetura informacional da ICN: a opção por uma estrutura centralizada

A Lei da Identificação Civil Nacional estabelece uma arquitetura informacional que dispõe sobre a constituição da Base de Dados da ICN (BDICN) e determina o fluxo dos dados pessoais que a compõem no interior da administração pública.

A leitura de seu art. 2º permite identificar a opção legislativa por uma arquitetura informacional centralizada. Isso porque a constituição da Base de Dados da ICN se dá a partir da concentração de diversas bases de dados previamente constituídas pelo poder público. Composta majoritariamente por dados biométricos, inicialmente, pelo arranjo da LICN, tal base de dados seria gerida por uma única instituição do poder público: o Tribunal Superior Eleitoral (TSE).

Mais especificamente, segundo as disposições legais, a Base de Dados da ICN é constituída pela base de dados biométricos da Justiça Eleitoral – administrada pelo Tribunal Superior Eleitoral -, a base de informações do Sistema Nacional de Informações de Registro Civil (SIRC) – que reúne os dados relativos a registros de nascimento, de casamento, de óbito e de natimortos produzidos pelos cartórios de registro civil das pessoas naturais – e da Central Nacional de Informações do Registro Civil (CRC Nacional) – essa última controlada pelo Conselho Nacional de Justiça -, bem como por outras informações, não disponíveis no SIRC, mas que estejam contidas em outras bases de dados da Justiça Eleitoral, dos institutos de identificação dos Estados e do Distrito Federal ou do Instituto Nacional de Identificação, ou disponibilizadas por outros órgãos, respeitando definições posteriores do Comitê Gestor da ICN. O fluxograma abaixo ilustra a composição da BDICN:

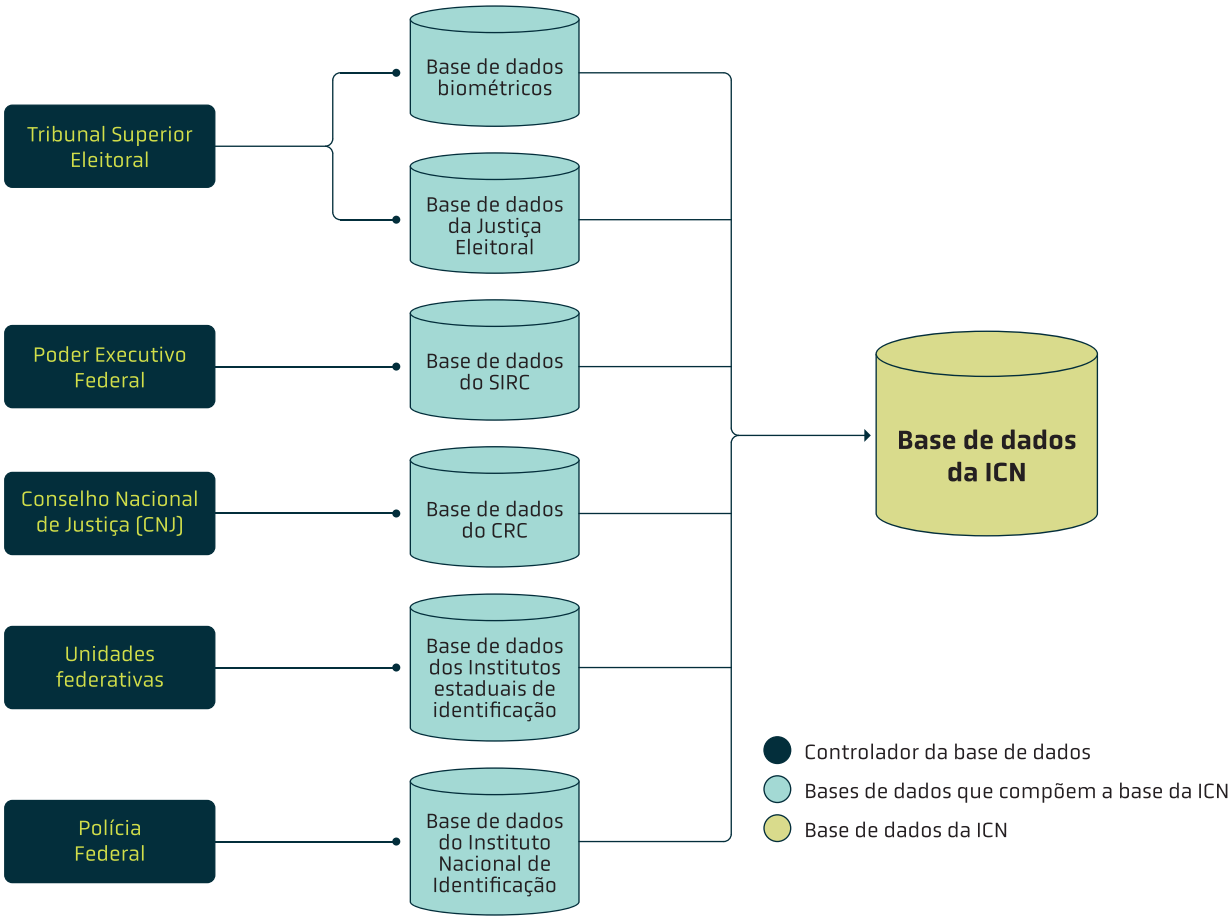


Figura 1
Arquitetura informacional da ICN.

A partir desse arranjo, a LCIN autoriza o acesso à BDICN tanto para o Poder Executivo quanto para o Legislativo, em todos os seus níveis federativos - federal, estadual e municipal -, sendo somente excepcionados o acesso aos dados eleitorais, os quais são acessíveis somente para a Justiça Eleitoral. A Lei 13.444/2017, ainda, prevê ao Tribunal Superior Eleitoral a possibilidade de oferecimento de serviços de autenticação dos cidadãos a entidades do setor privado, a partir da utilização da base de dados biométricos que compõe a Base de Dados da ICN.

Apesar de a Lei da ICN estabelecer uma arquitetura informacional centralizada, essa forma de estruturar um sistema único de identificação civil nacional não é, propriamente, uma novidade, uma vez que, como tratado no capítulo 2 deste documento, a mesma escolha foi feita quando das tratativas para a constituição do RIC. Neste ponto, porém, é importante mencionar que há alternativas ao modelo de arquitetura centralizado que vem se cristalizando nas políticas públicas de identidade civil digital implementadas - ou as quais tentou-se implementar - no Brasil.

Como apontado na seção 2.1, a implementação do RIC foi precedida de um amplo estudo exploratório e propositivo sobre as melhores formas de estruturação de um sistema único de identidade no Brasil. Tais estudos foram conduzidos pelo Ministério da Justiça e pela Universidade de Brasília, a partir de um Acordo de Cooperação Técnica, e resultaram em diversos relatórios técnicos. Dentre os documentos produzidos, destaca-se o relatório técnico "Características e Questões de Pesquisa sobre Gestão de Identidades", publicado em 2015, o qual aponta para a existência de quatro modelos de Sistemas de Gestão de Identidades Eletrônicas (SGId): centralizado, tradicional, federado e centrado no usuário.

Antes que os modelos listados acima sejam pormenorizados, é necessário apontar algumas definições de componentes que constituem um SGId. Um sistema de gestão de identidades eletrônicas é "caracterizado pelos seguintes elementos: **usuário** - aquele que deseja acessar um recurso; **identidade** - conjunto de atributos de um usuário; **provedor de identidade** (IdP) - responsável por gerenciar identidades de seus usuários e autenticá-los; **provedor de serviços** (SP) - oferece recursos aos usuários autorizados, após verificar a autenticidade de sua identidade e após comprovar que a mesma carrega todos os atributos necessários para o acesso" (BHARGAV-SPANTZEL *et al.*, 2007, apud UNIVERSIDADE DE BRASÍLIA, 2015, pp. 13-14)

O modelo de sistema centralizado de identificação de cidadãos[13] é aquele que apresenta um único provedor de identidade, o qual será responsável pela autenticação dos usuários e pelo fornecimento de serviços de informações sobre eles. Nesse arranjo de estrutura, o provedor de identidades permite o compartilhamento de identidades dos usuários entre provedores de serviços, viabilizando o uso de uma única identidade (UNIVERSIDADE DE BRASÍLIA, 2015). A crítica que se faz a esse modelo é justamente sobre o poder que o provedor de identidade possui sobre os dados dos usuários, o qual não garante que suas informações pessoais não serão compartilhadas com terceiros de forma abusiva (UNIVERSIDADE DE BRASÍLIA, 2015).

Ainda sobre a adoção de modelos centralizados, em sede do julgamento do sistema de identidade digital do Quênia, "Huduma Namba", diversos especialistas foram ouvidos perante a Corte Superior do Quênia. Dentre eles, destaca-se o depoimento do especialista Anand Venkatanarayanan, no qual é apontado o fato de que arquiteturas informacionais centralizadas de identidade digital estão mais propensas a serem alvos de incidentes de segurança, sendo essas, portanto, arquiteturas mais vulneráveis do ponto de vista de segurança da informação. Ainda, de acordo com o especialista, a escolha por sistemas

13 A escolha por modelos centralizados de sistemas de identidade pode ser verificada em alguns países como Quênia, Nigéria, Índia, Peru e Argentina.

centralizados vai de encontro aos modernos desenvolvimentos de arquiteturas informacionais, os quais apontam os sistemas descentralizados como o padrão a ser seguido (REPUBLIC OF KENYA, 2020).

Como alternativas ao modelo centralizado, existem o modelo tradicional, o federado e o centrado no usuário. Segundo Wangham *et al* (2010), o modelo tradicional é aquele amplamente utilizado em sistemas computacionais que operam *online*. A identificação do usuário ocorre de forma isolada por cada provedor de serviço, que atua também como provedor de identidade. Desse modo, é necessário que o usuário crie uma credencial para cada provedor de serviços com o qual deseja interagir, não havendo, portanto, o compartilhamento de dados entre os diversos provedores de serviço (WANGHAM *et al*, 2010).

O modelo de identidade federada, por sua vez, apoia-se sobre a autenticação dos usuários de forma distribuída entre diversos provedores de identidade, os quais estão localizados em diferentes domínios administrativos, como, por exemplo, uma empresa ou uma universidade. De acordo com Wangham *et al* (2010), os domínios administrativos são constituídos por múltiplos provedores de serviços, usuários e um único provedor de identidades. Ao permitir que identidades emitidas em um determinado domínio administrativo sejam reconhecidas e, assim, autenticadas por outro domínio, o modelo federado auxilia no gerenciamento de identidades dos usuários, de modo que eles não precisam lidar com múltiplas identidades e serem submetido diversas vezes ao processo de autenticação (WANGHAM *et al*, 2010).

Finalmente, o modelo centrado no usuário é aquele cujo objetivo é o de conferir ao usuário o controle sobre suas identidades digitais (UNIVERSIDADE DE BRASÍLIA, 2015). Nesse modelo, as identidades do usuário são armazenadas em um dispositivo físico do próprio cidadão, possibilitando que ele escolha quais dos provedores de identidade utilizarão seus dados, independentemente dos provedores de serviços que os desejam utilizar e sem que haja a necessidade de informar dados pessoais a estes provedores de serviços (UNIVERSIDADE DE BRASÍLIA, 2015). Nesse modelo, os provedores de identidades continuam atuando como terceira parte confiável na interação entre usuários e provedores de serviços, mas orientados pelos interesses dos usuários e não conforme os interesses dos provedores de serviços (UNIVERSIDADE DE BRASÍLIA, 2015).

Abaixo, na figura 2 (WANGHAM *et al*, 2010), é possível ver, de modo esquemático, como se dá o funcionamento dos modelos de gestão de identidade eletrônica tradicional, federado, centralizado e centrado no usuário:

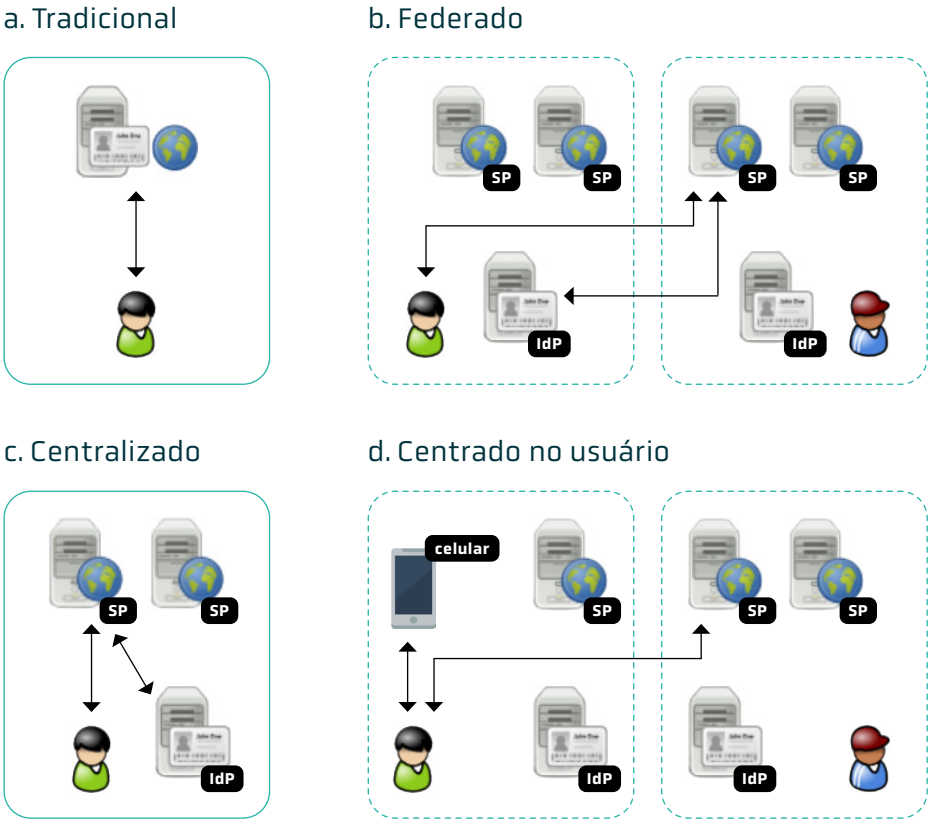


Figura 2
Classificação dos modelos de gestão de identidade eletrônica.

Com o início das discussões sobre o Projeto de Lei da Identificação Civil Nacional no ano de 2015, os estudos relativos ao RIC foram suspensos. Apesar de os relatórios produzidos indicarem a existência de diversos tipos de modelos de Sistemas de Gestão de Identidades Eletrônicas, o Estado brasileiro optou pelo modelo centralizado, o qual foi cristalizado quando da promulgação da LICN. Ao que tudo indica, tal processo ocorreu sem que houvesse um amplo debate público e uma avaliação metodologicamente amparada e sistemática sobre quais seriam os custos e benefícios decorrentes da implementação de cada um dos modelos apresentados anteriormente.

3.3. A disciplina legal da proteção de dados pessoais e o uso da BDICN para autenticação dos cidadãos no gov.br

Uma vez brevemente explicado como se estrutura a arquitetura informacional da ICN e como é composta sua base de dados, esta seção trata dos potenciais conflitos entre a LGPD e o uso da BDICN para autenticação dos cidadãos no gov.br. Esses conflitos são oriundos tanto da estruturação da BDICN, quanto da estruturação do gov.br.

a. Segurança da informação e vigilância estatal

Como visto, no Brasil, optou-se por um sistema de identidade centralizado, cuja base de dados - a Base de Dados da ICN - se origina a partir da união de diversas outras bases de dados. Um dos principais riscos que surge dessa opção é em termos de segurança da informação, na medida em que um único incidente de segurança pode ocasionar a exposição ou acesso indevido a uma grande quantidade e diversidade de dados pessoais, inclusive sensíveis. Nesse sentido, cabe mencionar que o sistema argentino centralizado de identidade civil digital sofreu um incidente de segurança em 2021. Na oportunidade, o grupo responsável pelo ataque ao sistema liberou fotos de documentos de identidade em redes sociais, em movimento que permitiu que fossem elaborados documentos falsos dessas pessoas, assim como o número internamente utilizado pelo governo atribuído a cada cidadão (BRODERSEN; BLANCO, 2021) e (BRODERSEN; BLANCO, 2021b).

De forma semelhante, em 2018, foi investigado um acesso não autorizado à base de dados do sistema de identidade indiano Aadhaar, também organizado de maneira centralizada. Repórteres do jornal Tribune conseguiram comprar acesso, através de um usuário e senha, ao site do detentor da base de dados de identidade civil (UIDAI), o que lhes permitiu consultar qualquer número de Aadhaar no site e assim acessar a foto, nome, endereço, telefone e email do cidadão a quem o número de Aadhaar pertencia (BBC, 2018).

Voltando-se à realidade brasileira, é importante registrar que os últimos anos foram marcados por uma série de incidentes de segurança significativos com bases de dados públicas, como do Ministério da Saúde e do Ministério da Educação, em 2020 e 2021, respectivamente (IDEC, 2020) e (NAÍSA, 2021). Não só, mas em dezembro de 2021, no decorrer de uma semana, um mesmo grupo de hackers invadiu servidores do Ministério da Saúde, Ministério da Economia, Agência Nacional de Transporte e páginas do Governo Digital (MURAKAWA, 2021).

Não à toa, a segurança dos dados é preocupação latente na LGPD, que determina em seu art. 49 que qualquer sistema utilizado para tratamento de dados pessoais deve ser estruturado de forma a atender os requisitos de segurança. O art. 47 da Lei destaca, ainda, a obrigação dos agentes de tratamento ou de qualquer outra pessoa que intervenha em uma das fases do tratamento em garantir a segurança da informação em relação aos dados pessoais, mesmo após o término do tratamento. O art. 46 da LGPD também fala na adoção de medidas de segurança, técnicas e administrativas para proteção dos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Fica evidente, pelas disposições da LGPD, que considerações relativas à segurança da informação devem ser incorporadas na arquitetura de quaisquer sistemas, desde o momento de sua estruturação. E constituir um sistema centralizado, como é a ICN, implica em um maior risco de segurança, o qual deve ser - igualmente em maior medida - endereçado.

Não é em vão que a existência de sistemas centralizados para tratamento de dados pessoais não parece ser a opção legislativa da LGPD, ainda que adotada como regra derrogável, para o tratamento de dados pelo poder público. Em seu art. 25, a lei prevê que os dados sejam mantidos em formato interoperável e estruturado para uso compartilhado, prevendo, portanto, a necessidade de compartilhamento (intercâmbio) de dados entre diferentes órgãos e entidades do poder público para execução de políticas públicas.

A opção por um modelo centralizado corresponde necessariamente a uma maior complexidade de governança. Via de regra, trata-se de um modelo que, se não desincentiva, torna, ao menos, mais desafiadora a implementação de boas práticas basilares, tais quais a minimização na coleta de dados, ciclo de vida dos dados, gerenciamento de identidades e incidentes de segurança. Sobre o tema, Lister (1970) afirma que existe um aumento nas oportunidades do governo de vigiar os seus cidadãos e na intensidade dessa possível vigilância pela existência de sistemas centralizados de larga escala de dados pessoais, o que pode causar alterações fundamentais na sociedade e no balanço de poder entre Estado e cidadão. Mais especificamente, o autor lista seis ameaças imediatas à privacidade decorrentes desses sistemas (LISTER, 1970, p.209):

(1) Com uma maior eficiência de sistemas de armazenamento e pesquisa de informações, reduz-se o incentivo a restringir a coleta de dados ao essencial e, por consequência, se coletam mais informações do que é imediatamente ou prospectivamente necessário;
(2) Como há uma maior eficiência em armazenamento, não existe um incentivo para fazer o descarte dos dados, que podem ser mantidos mais facilmente, mesmo que também sejam mais facilmente deletáveis;
(3) Os novos sistemas de dados permitem um uso mais completo da informação, que pode ser correlacionada e revelar padrões de crenças ou comportamentos. Isso significa que pode haver uma busca precisa em uma ampla base de dados mesmo que para um propósito de relativa baixa prioridade;
(4) Materiais podem ser disseminados com maior facilidade: a informação que antes estava disponível apenas localmente vai ser acessível a qualquer um no país com acesso a um terminal;
(5) O mero fato de a informação ser dada por um sistema pode fazer com que ela pareça mais confiável ou valiosa para quem a recebe, o que pode ocasionar

na perda de habilidade crítica de avaliação da possibilidade de a informação estar errada e da necessidade de sua verificação, já que os dados podem ficar obsoletos;

(6) O dano que esses grandes sistemas centralizados causam em casos de erro é majorado. Inversamente, se o dado circulasse somente em uma comunidade limitada, o dano em caso de um erro seria igualmente limitado.

Em poucas palavras, a concentração de dados, como se dá na Base de Dados da ICN, implica necessariamente em um grau de exposição maior de risco e de vulnerabilização do cidadão. É o que explica Lyon (2009, p. 4) ao considerar que, diante desses sistemas, o cidadão passa a ser observável nos seus mais diferentes papéis - enquanto consumidor, trabalhador, aposentado, viajante, (potencial) criminoso etc. Um fluxo informacional que, ao condensar todas essas esferas sociais, tem maiores chances de ser abusivo (NISSENBAUM, 2010).

b. Hipóteses de tratamento de dados pessoais pelo Poder Público

Como já delineado neste texto, dentre os dados congregados na Base de Dados da ICN há, além de uma série de dados pessoais não sensíveis, importante volume de dados sensíveis, assim compreendidos a partir da definição do art. 5º, inciso II, da LGPD: dados biométricos oriundos da justiça eleitoral e dados de raça e etnia, oriundos do Sistema Nacional de Informações de Registro Civil (SIRC) e da Central Nacional de Informações do Registro Civil (CRC Nacional).

Como se sabe, qualquer atividade de tratamento de dados pessoais precisa estar lastreada em uma das bases legais previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD. Quando a atividade de tratamento for realizada pelo poder público, esses dispositivos devem ser interpretados de forma conjunta com o art. 23 da mesma lei, o qual destaca que o tratamento de dados pessoais por esse tipo de agente deverá, necessariamente, atender uma finalidade pública.

A constituição da Base de Dados da ICN e seu uso para identificação do cidadão em transações envolvendo entes públicos e privados encontra base direta na Lei da ICN, a qual atribui ao TSE a competência de gestão de todos os dados pessoais - sensíveis e não sensíveis - dos cidadãos. Nesse sentido, justificar as atividades de tratamento de dados relacionadas à manutenção da BDICN a partir da disposição no art. 11, inciso II, a da LGPD, que menciona a "obrigação legal ou regulatória do controlador" parece adequado.

Em um segundo momento, em se tratando da utilização do banco de dados da ICN para autenticação de usuários no gov.br, uma possível base legal adequada a ser eleita pelo poder público para o tratamento de dados pessoais realizado seria a de execução de política pública, prevista no art. 7º, inciso III e art. 11, inciso II, b, da LGPD. No caso, a política pública em questão seria a de acesso aos serviços digitais públicos, justamente por meio da plataforma gov.br.

Para que a opção adequada pela base legal da execução de políticas públicas para atividades de tratamento de dados, a ANPD, em seu guia "Tratamento de Dados Pessoais pelo poder público", editado em janeiro de 2022, conceitua o termo política pública, desdobrando-o em dois aspectos. O primeiro deles a existência de um ato formal que institui a política (seja ele de natureza normativa, como lei ou regulamento, ou por ajustes contratuais, como contratos, convênios e instrumentos congêneres). Entretanto, o manual ressalta que para o tratamento de dados sensíveis não há referência na LGPD às políticas públicas instituídas em ajustes contratuais. De tal modo, para tais atividades seria necessária uma política pública prevista em lei ou regulamento, uma vez que as hipóteses de tratamento de dados sensíveis são disciplinadas de forma mais restrita (ANPD, 2022).

Ainda, conforme a ANPD (ANPD, 2022), o segundo aspecto relevante para a configuração de uma política pública é material: "a definição de um programa ou ação governamental específico, a ser executado por uma entidade ou por um órgão público." (ANPD, 2022, p. 13). Em regra, assim, o conteúdo de uma política pública incluiria seus objetivos, metas, prazos e meios de execução (ANPD, 2022).

No caso objeto deste *policy paper* - a utilização da Base de Dados da ICN para autenticação de usuários na plataforma gov.br -, existe um Acordo de Cooperação Técnica, firmado em 15 de março de 2021 entre Secretaria Geral da Presidência, Ministério da Economia e Tribunal Superior Eleitoral para: "I – Especificar e implementar a prestação do serviço de conferência de dados da BDICN, por meio da plataforma GOV.BR." (BRASIL, 2021b). A política pública aqui em questão está, portanto, disciplinada por um ajuste contratual. Isso desperta atenção, uma vez que há um volume importante de dados sensíveis tratados pelo poder público para viabilizar a ICN e o uso de sua base de dados para autenticação do cidadão no gov.br. Desse modo, os requisitos para uso adequado da base legal do art. 11, inciso II, alínea (b), não estariam satisfeitos[14].

14 O gov.br é disciplinado pelo decreto 8936/2016 e a ICN pela Lei 13444/2017.

c. A centralidade dos dados biométricos e a larga escala das atividades de tratamento

Conforme já extensamente delineado, a Base de Dados da ICN é constituída por dados biométricos. Tais dados advêm da base de dados biométricos da Justiça Eleitoral e são coletados, inicialmente, para atender à finalidade de tornar o processo eleitoral ainda mais seguro (TSE, s.d.).

Segundo informações disponibilizadas pelo portal do Tribunal Superior Eleitoral (TSE) atualizadas em 17 de maio de 2022, existem mais de 118 milhões de pessoas que possuem a identificação biométrica registrada junto ao órgão, o que corresponde a cerca de 80% do eleitorado brasileiro (TSE, 2022b). Há, ainda, a expectativa de que seja coletada a identificação biométrica de todo o eleitorado nacional até o ano de 2026.

A biometria, uma das técnicas utilizadas pela ICN e a principal técnica utilizada na autenticação dos usuários na plataforma gov.br, é o conjunto de métodos e procedimentos utilizados para o reconhecimento de indivíduos baseado em seus atributos físicos, comportamentais e fisiológicos, como a impressão digital, o rosto, a íris e a voz (DANTCHEVA, ELIA e ROSS, 2016). Um sistema clássico de biometria, nessa linha, coleta dados biométricos de determinado indivíduo, extrai deles uma série de informações e as compara com outras características presentes em bases de dados com intuito de verificar se determinado sujeito é realmente quem ele diz ser (DANTCHEVA, ELIA e ROSS, 2016). Segundo os autores Dantcheva, Elia e Ross (2016), é possível, ainda, a partir dos dados biométricos, deduzir outros tipos de características de seus titulares, como idade, gênero e etnia.

Considerando não só que a Base de Dados da ICN é centralizada, mas também que contém dados biométricos, aumenta-se a gravidade de um potencial incidente de segurança[15]. De acordo com texto do Informe do Alto Comissariado das Nações Unidas para os Direitos Humanos, de agosto de 2018 (UNITED NATIONS, 2018):

15 "Dados biométricos são algo de difícil conceituação. Mas, em apertada síntese, decompondo a palavra em questão, poder-se-ia afirmar que são dados mensuradores das características corporais de um determinado indivíduo. Logo, tais dados representam uma particularidade única do indivíduo, já que eles não podem ser alterados ou modificados por estarem "presos" à unicidade do corpo humano. Por isso, outros dados pessoais, como registro de identidade e o número no cadastro nacional de pessoas físicas, podem até serem considerados como identificadores únicos, mas não com o grau de precisão e particularidade dos dados biométricos. Isto porque, os dados biométricos são inalteráveis em decorrência da singularidade corporal, diferentemente do que ocorre quando um dado é atribuído a um indivíduo pelo controle estatal. Nesse sentido, dados biométricos identificam um sujeito em nível global, diferentemente do registro de identidade que tem um alcance nacional. Por essa imutabilidade, singularidade e alcance é que os dados biométricos deveriam ser considerados como dados sensíveis, por serem identificadores únicos com o mais alto grau de precisão que nenhum outro dado detém a mesma capacidade. Por tal razão, os dados biométricos podem ser tão ou mais lesivos que outros dados pessoais sensíveis. Do seu acesso podem decorrer as mais diversas atividades fraudulentas, potencializando-se, ainda mais, os chamados roubos de identidade (identity thefts)." (GPOPAI, 2015, p.7).

> A criação de bases de dados massivas de dados biométricos traz preocupações relevantes em relação aos direitos humanos. Esses dados são particularmente sensíveis, já que por definição são ligados inseparavelmente a uma pessoa em particular e à sua vida, e tem o potencial de serem gravemente abusados. Por exemplo, roubo de identidade baseado em dados biométricos é extremamente difícil de remediar e pode afetar de forma séria os direitos de um indivíduo. Além disso, dados biométricos podem ser utilizados para propósitos diferentes daqueles para os quais foram coletados, incluindo a perseguição e monitoramento ilegal de indivíduos. Considerando tais riscos, deve ser dada atenção de maneira específica para questões de necessidade e proporcionalidade na coleta de dados biométricos. Contra esse plano de fundo, é motivo de preocupação que alguns Estados estão embarcando em amplos projetos baseados em dados biométricos, sem ter adequada proteção legal e procedimental para tanto (UNITED NATIONS, 2018, p.5, tradução livre)

Apesar de a LGPD não definir o que são dados biométricos, em seu art. 5º, inciso II, ela os classifica como dados pessoais sensíveis. Por essa razão, a eles é atribuído um regime diferenciado e mais protetivo, na medida em que compreende-se que o tratamento desse tipo de dado tem maior potencial discriminatório (KONDER, 2019). Nesse sentido, a Seção II da LGPD, ao abordar o tratamento dos dados sensíveis, define que ele poderá ocorrer somente: (i) quando houver o consentimento do titular ou seu responsável legal, de forma específica, destacada e para finalidades específicas; ou (ii) sem o fornecimento de consentimento do titular de dados, desde que seja indispensável para a execução de algumas hipóteses estabelecidas, taxativamente, nas alíneas do art. 11, inciso II.

Dentre as possibilidades de tratamento de dados sensíveis sem o fornecimento de consentimento pelo titular de dados, destaca-se, para o uso da Base de Dados da ICN para autenticação dos cidadãos no gov.br, a alínea (b) do art. 11, II da LGPD, a qual prevê a possibilidade de "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos" (BRASIL, 2018). A opção por lastrear determinada atividade de tratamento de dados nessa base legal, contudo, de acordo com o parágrafo 2º do art. 11 da Lei Geral de Proteção de Dados, evoca a necessidade de publicização da dispensa do consentimento do titular.

Nesse sentido, apesar de a atividade de tratamento de dados pessoais executada pelo poder público para a implementação da Identificação Civil Nacional e da prestação de serviço de autenticação de cidadãos na plataforma gov.br estar amparada pelo princípio

da legalidade[16], a publicização da dispensa de consentimento dos titulares de dados em ambos os processos é elemento fundamental para que o poder público esteja em conformidade com a LGPD.

No caso do uso da Base de Dados da ICN para autenticação do cidadão no gov.br, deve-se melhor materializar tal determinação de publicização de informações sobre o tratamento de dados. Nessa linha, cumpre destacar a obrigação de se ter um termo de uso e política de privacidade específica sobre a atividade de autenticação dos usuários no portal gov.br disponível a qualquer tempo para o usuário. No momento de escrita deste relatório, tais documentos somente são disponibilizados na criação da conta no portal e quando se faz o *login* na plataforma por meio de dispositivos móveis, não sendo facilmente acessíveis posteriormente[17]. É dizer, considerando as disposições da LGPD, é recomendável uma jornada de transparência que, além de notificar o titular de dados da ocorrência do tratamento em outros momentos que não apenas quando da sua entrada no sistema, tenha uma interface não apenas textual, de modo que agregue quantitativamente e qualitativamente na informação prestada ao usuário.

Ainda na esteira da utilização de dados biométricos pela Identificação Civil Nacional e para a autenticação dos cidadãos para acesso a serviços públicos por meio do gov.br, uma questão que se faz relevante diz respeito à qualidade dos dados, estabelecida na Lei Geral de Proteção de Dados Pessoais, em seu art. 6º, inciso V, como um dos princípios que deve orientar toda e qualquer atividade de tratamento de dados pessoais. Segundo a disposição legal, o princípio da qualidade dos dados se caracteriza pela "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (BRASIL, 2018).

Trata-se da expressão brasileira do princípio da exatidão disposto na Convenção 108 do Conselho da Europa e nas *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, publicadas pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE). O princípio da qualidade dos dados, segundo Danilo Doneda (2019), visa garantir aos titulares de dados que os seus dados armazenados sejam correspondentes e fiéis à realidade, a partir da noção de que o tratamento de dados pessoais seja realizado "com cuidado e correção, e de que sejam realizadas atualizações conforme a necessidade"

16 O Princípio da Legalidade pode ser compreendido como uma "(...) diretriz básica da conduta dos agentes da Administração. Significa que toda e qualquer atividade administrativa deve ser autorizada por lei. Não o sendo, a atividade é ilícita" (FILHO, 2020, p. 95)

17 A partir da navegação no portal, é possível identificar o termo de uso referente ao uso de informações de navegação no gov.br, não havendo qualquer menção ao processo de autenticação de usuários da plataforma. Para ver mais, acesse: https://www.gov.br/pt-br/termos-de-uso.

(DONEDA, 2019, p. 182). Em resumo, assim como os demais princípios de proteção de dados pessoais, a qualidade dos dados deve orientar qualquer atividade de tratamento de dados pessoais, de modo a evitar inconsistências relacionadas aos dados utilizados.

Partindo desse conceito e voltando-se as lentes à ICN e ao gov.br, o Tribunal Superior Eleitoral afirmou terem sido identificadas algumas inconsistências na Base de Dados da ICN, especialmente na base de dados biométricos que a compõe. No ano de 2018, segundo o órgão eleitoral, cerca de 9 milhões de eleitores – que correspondiam a 12,21% dos eleitores daquele ano – apresentaram problemas na identificação biométrica imediata no momento da votação (PUPO, 2018). De acordo com o Tribunal, esse número equivalia àqueles eleitores que votaram sem a biometria, em razão da impossibilidade de completar o processo de identificação, e aos eleitores que apenas conseguiram ser identificados biometricamente após diversas tentativas frustradas.

Nessa esteira, mais recentemente, em agosto de 2021, o TSE instituiu uma comissão para gerir o tratamento de inconsistências biométricas do Cadastro Eleitoral (TSE, 2021c). A Comissão Gestora do Processo de Tratamento das Duplicidades ou Multiplicidades Biométricas do Cadastro Eleitoral tem por objetivo a atuação em direção à correção de tais inconsistências que, desde o ano de 2014, somam cerca de 52 mil casos relacionados às duplicidades ou pluralidades biométricas.

Apesar das movimentações para se garantir a qualidade dos dados, os mais de 50 mil casos de inconsistências já identificados pela Justiça Eleitoral revelam a necessidade de se atentar para o princípio da qualidade dos dados, ainda mais considerando os avanços dos Tribunal Superior Eleitoral em direção ao aumento de sua base de dados biométricos, como se pode observar pela Ação Nacional de Identificação Civil para as Pessoas Presas (TSE, 2021d), conduzida pelo Conselho Nacional de Justiça (CNJ) e pelo TSE.

É essencial que se volte a atenção ao princípio da qualidade dos dados na medida em que sua potencial violação ensejaria o risco de exclusão de cidadãos, titulares de dados, tanto do acesso aos serviços públicos disponibilizados via plataforma gov.br quanto da própria política pública de identificação civil. Essa segregação ocorreria em razão da dificuldade e/ou inviabilidade de uma correta identificação e autenticação dos usuários, decorrente da imprecisão dos dados biométricos coletados.

d. Uso secundário e uso compartilhado de dados pessoais no âmbito do poder público

A noção elástica de compatibilidade para usos secundários de dados pessoais

Conceitualmente, o uso secundário de dados pessoais é caracterizado quando há seu tratamento para finalidade diversa daquela que justificou sua coleta (WIMMER, 2021a). No caso analisado neste relatório, é importante considerar a existência de dois momentos separados para avaliar duas camadas distintas de usos secundários de dados referentes, de modo geral, à BDICN: (i) o momento da composição da Base de Dados da ICN; e (ii) o momento do uso da Base de Dados da ICN para autenticação do cidadão no gov.br.

Conforme já exposto, a Base de Dados da ICN está disciplinada por lei (art. 2º, Lei 13.444/2017) e é formada de outras bases de dados já previamente compostas, ou seja, resultou da união de bases de dados que já existiam. Tem-se, assim, que os dados que compõem a BDICN foram coletados, inicialmente, para propósitos específicos, de acordo com cada uma das bases de dados originais posteriormente juntadas - por exemplo, a biometria da Justiça Eleitoral foi coletada com a finalidade de votação nas eleições e os dados de registro civil eram mantidos para, justamente, fins de registro civil. Ao serem somados em uma única base, a BDICN, tais dados pessoais estão em uso secundário.

Para além da Identificação Civil Nacional, este relatório se debruça sobre o uso de tal base de dados para autenticação dos cidadãos no acesso a serviços públicos via plataforma gov.br. Para que isso possa ocorrer, há ainda uma segunda etapa em que se verifica o uso secundário de dados. Afinal, a BDICN foi composta tendo por finalidade amparar a política da Identificação Civil Nacional, conforme o art. 1º da LICN, e, neste caso, está sendo utilizada para outra finalidade - justamente, autenticar o cidadão no acesso a serviços públicos pelo gov.br.

A LGPD, é importante ressaltar, não veda o tratamento de dados para fins secundários. Pelo contrário, traz previsão expressa para tanto, mas seu texto condiciona a operação à verificação de compatibilidade entre contexto do uso secundário e o contexto no qual o dado foi originariamente coletado. Esse termo "compatibilidade" é mencionado pela LGPD em três momentos. Dois deles são as passagens que prescrevem o conceito dos princípios da finalidade e adequação[18]. Há entre eles uma relação de complementaridade que se dá menos pela sua alocação topográfica sequencial e mais pela estrutura gramatical dos referidos dispositivos, a exemplo do que se tem nas chamadas oração principal e subordinada. Se o princípio da finalidade introduz a ideia de que o "tratamento posterior" deve

18 O terceiro está ligado diretamente à base legal do consentimento (art. 9º, §2º).

ser compatível, é o princípio da adequação que explica que essa coadunação é aferível de "acordo com o contexto" do processamento de dados, como se vê da conceituação e da esquematização em figura abaixo[19]:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

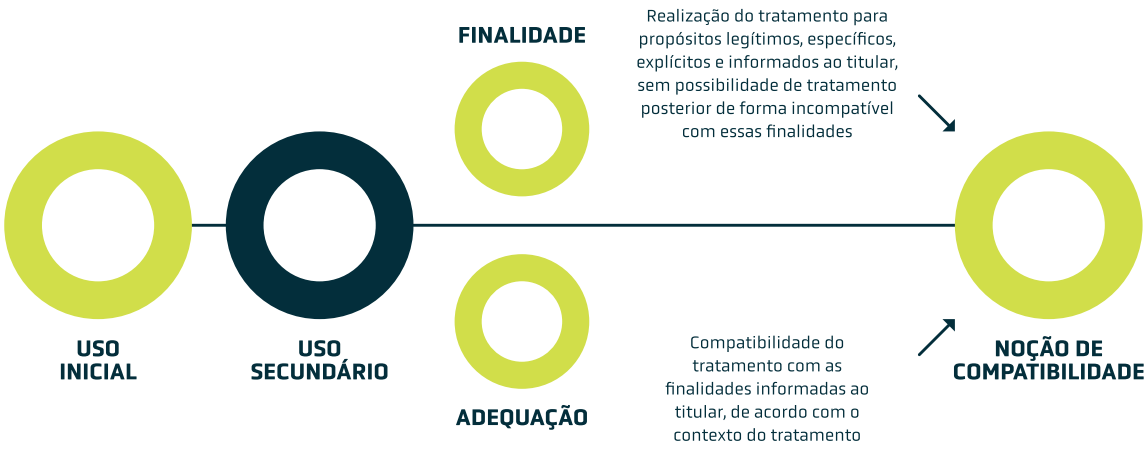


Figura 3
Resumo esquemático do uso secundário de dados pessoais.

Ao conectar essa dupla de princípios com o princípio da boa-fé e com a teoria da privacidade contextual (NISSENBAUM, 2010), Bioni (2021) ressalta que se trata de uma abordagem atenta ao quão dinâmico é, e deve ser, o fluxo informacional. Além da aproximação do texto da LGPD com uma teoria que se afasta de uma definição estática do que compõe um tratamento de dados compatível, o legislador valeu-se de um conceito jurídico indeterminado - uma técnica legislativa que talha o comando legal de forma abstrata a ponto de exigir do intérprete uma busca metajurídica, isto é, das características do contexto da relação entre titular e agente de tratamento:

> não é delimitado por um propósito específico e duro - em linha com o que dispõe a expressão finalidades determinadas (...), mas

19 A referida imagem foi cedida pela instituição Data Privacy Brasil Ensino e compõe o material didático da primeira aula do curso: "Privacidade e Proteção de Dados Pessoais: teoria e prática".

> direcionado a uma gama de ações passíveis de serem executadas no contexto de uma relação. Com isso, a privacidade contextual mostra-se útil, já que é elástica suficiente para governar o uso secundário dos dados pessoais que não podem ser previamente especificados e controlados de maneira rígida (...) uma análise mais aberta que perquire a respeito das duas características, se (...) estão de acordo com o contexto da relação subjacente ao fluxo informacional (...) Esse é o elemento que dá um mínimo de previsibilidade (segurança) frente a tais espaços de incertezas do fluxo informacional (Bioni, 2022, p. 231-234)

Atenta à necessidade de estabilização desse conceito jurídico de "compatibilidade", a ANPD (2022) sugere a consideração dos seguintes aspectos:

> (i) o contexto e as circunstâncias relevantes do caso concreto; (ii) a existência de conexão fática ou jurídica entre a finalidade original e a que fundamenta o tratamento posterior; (iii) a natureza dos dados pessoais, adotando-se posição de maior cautela quando abrangidos dados sensíveis; (iv) as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos; e (v) o interesse público e a finalidade pública específica do tratamento posterior, bem como o seu vínculo com as competências legais dos órgãos ou entidades envolvidos, nos termos do art. 23 da LGPD (ANPD, 2022, p. 13)

Acerca da legítima expectativa do titular de dados, em específico, a opinião 06/2014 do WP 29 acerca do Legítimo Interesse afirma que as considerações para avaliar a expectativa legítima dos titulares sobre o uso secundário dos dados coletados são semelhantes às do princípio da finalidade:

> É importante considerar se o status do controlador dos dados, a natureza da relação ou do serviço fornecido, ou das obrigações legais ou contratuais aplicáveis (ou outras promessas feitas no momento da coleta dos dados) poderiam criar legítima expectativa de limites mais rígidos de confidencialidade e em relação ao uso secundário. Em geral, quanto mais específico e restrito o contexto da coleta de dados, é mais provável haver limitações no uso. Aqui, novamente, é necessário considerar o contexto factual e não apenas o texto nas entrelinhas (WP 29, 2014, p. 40, tradução livre)

Diante desse quadro, para avaliação do uso secundário de dados no emprego da política brasileira de identidade civil digital e plataformização de serviços públicos, devem ser analisadas, em primeiro lugar, as bases de dados que compõem a ICN e o uso secundário que se dá ao serem operacionalizadas para uma base unificada da ICN. Em segundo lugar, é também necessário avaliar o uso secundário da própria Base de Dados da ICN no acesso ao gov.br. É esse o contexto e as circunstâncias em que as atividades se inserem.

Passando-se aos seguintes requisitos estabelecidos pela ANPD para a avaliação do uso secundário de dados, tem-se que, de maneira geral, em ambas essas etapas de atividades de tratamento é possível o estabelecimento de uma conexão jurídica entre a finalidade original do tratamento e a posterior - seja pela LICN ou pelo Acordo de Cooperação Técnica firmado em março de 2021 para utilização da BDICN no gov.br. Em relação à primeira camada de tratamento, qual seja, a composição da Base de Dados da ICN, a conexão jurídica entre a finalidade original do tratamento e a posterior está estabelecida pela LICN, em seu art. 2º, que determina quais bases de dados a ICN utilizará. Já em relação à segunda camada de tratamento, o momento do uso da Base de Dados da ICN para identificação do cidadão no gov.br, o Acordo de Cooperação Técnica assinado entre TSE e SGD determina, em sua cláusula 1.2, a prestação de serviços de conferência de dados da BDICN por meio da plataforma gov.br. (BRASIL, 2021b).

Em paralelo, sabe-se que todas as bases que compõem a BDICN contêm dados sensíveis, utilizados, majoritariamente, para o cumprimento da finalidade de identificação dos cidadãos. Isso fica evidente a partir da análise sobre quais informações são coletadas pelos agentes de tratamento, como por exemplo: a Justiça Eleitoral, que procede com a coleta de impressão digital e foto do eleitor; os cartórios de registro civil que, ao emitirem certidões de óbito, revelam dados sobre de raça/etnia, conforme art. 80, § 3º, Lei 6.015/1973; e os institutos de identificação que coletam impressão digital do polegar direito e fotografia da pessoa identificada, conforme art. 3º, alínea (f) da Lei 7.116/1983, para que ocorra a emissão de carteiras de identidade. O tratamento de dados sensíveis, como se sabe, se dá em regime mais protetivo, de modo que seu uso secundário deve ser realizado, igualmente, com maior cautela.

Ademais, como apontado anteriormente, a legítima expectativa do titular de dados é também um elemento que pode ser considerado na análise do uso secundário de dados (WP, 2014). Nos casos aqui analisados, ao considerar o contexto em que se deu a coleta das informações que compõem as bases que constituem a ICN, entende-se que havia uma expectativa de um uso restrito dos dados. Significa dizer que o uso secundário dos dados, identificado tanto na constituição da BDICN quanto no uso desta base de dados para autenticar usuários na plataforma gov.br, ao subverter a legítima expectativa dos titu-

lares de dados, tem o potencial de impactar os direitos destes.

Enfim, no que diz respeito ao requisito de interesse e finalidade pública das operações, entende-se que há um cumprimento. Afinal, ainda que possuam importantes riscos a serem endereçados, as políticas de identificação civil unificada e de digitalização de serviços públicos estão amparadas por uma busca pela diminuição dos sub registros e pela ampliação no acesso a serviços por parte dos brasileiros.

A despeito da importância do estabelecimento de critérios gerais de compatibilidade por parte da ANPD, entende-se que, a depender do caso concreto de que se está diante, a definição de novos parâmetros para tal averiguação tem condições de garantir uma análise mais granular e atenta da situação. Nesse sentido, propõe-se, para escrutínio da compatibilidade do uso primário e secundário de dados nas políticas da ICN e do gov.br, dois novos critérios, com o intuito de informar mais a fundo a discussão: a natureza do agente de tratamento de dados e o grau de conexão entre a arquitetura informacional da base que guarda os dados em uso primário e aquela que os guarda em uso secundário.

Considerando esses novos critérios, somados às ponderações acima, feitas a partir dos parâmetros sugeridos pela ANPD, chegou-se à conclusão de que o grau de compatibilidade entre as finalidades estabelecidas para a coleta inicial dos dados e para o uso secundário destes mesmos dados foi médio na primeira etapa de uso secundário de dados - isto é, na composição da BDICN, considerando a maior parte das bases de dados originais juntadas para a criação deste grande banco de informações - adiante pormenorizadas uma a uma. Tal conclusão, porém, excetua o uso da base de dados biométricos da Justiça Eleitoral para criação da BDICN, na medida em que, neste caso específico, não foi identificada conexão fática entre a finalidade original que justificou a coleta de dados biométricos e a finalidade estabelecida para o tratamento secundário, o que resultou em um baixo grau de compatibilidade.

Inclusive, no que diz respeito à base de dados biométricos da Justiça Eleitoral, a coleta da impressão digital, assinatura e foto do eleitor é realizada com uma finalidade muito bem delimitada: identificar o cidadão enquanto eleitor. No tratamento posterior dado pela ICN, a individualização do titular direciona-se para uma gama muito mais ampla de transações, que potencialmente se esparrama por todas as relações travadas entre o cidadão e o Estado e, até mesmo, com entidades privadas (JUSTIÇA ELEITORAL, s.d.). Ainda que estejam ligadas por uma mesma perspectiva macro que é a de singularização do cidadão, há um distanciamento fático significativo entre o contexto inicial da coleta - do cidadão no seu papel de eleitor diante do TSE (Poder Judiciário) enquanto controlador - e os referidos usos secundários - do cidadão na sua condição de potencial assistido pelo Estado diante

do Poder Executivo enquanto controlador -, bem como enquanto potencial consumidor quando entidades privadas também ingressam na cadeia. Com isso, há uma transgressão do fluxo informacional entre esferas bastante distintas capaz de frustrar a legítima expectativa do titular dos dados. Tudo isso, somado ao elevado nível de criticidade de dados biométricos em comparação até mesmo a outros tipos de dados sensíveis (vide: capítulo 3, seção 3.3 c), leva à avaliação de uma baixa compatibilidade entre a finalidade original e o uso secundário dos dados biométricos da base do TSE para a constituição da BDICN.

Por sua vez, as bases de dados do SIRC e do CRC Nacional, também mescladas para composição da BDICN, são constituídas pela união de bases de dados de cartórios de registros civis em que são registrados os dados de nascimento, de casamento, de óbito e de natimorto, conforme a Lei nº 6.015/1973. Tal como a ICN, elas também atestam atributos biográficos da pessoa natural, dentre os quais há dados sensíveis, como é o caso de informações relacionadas à raça e etnia, sem os quais não seria possível o exercício de uma série de direitos. Não só, mas servem também ao propósito de identificar o cidadão em suas relações com o Estado. Há, portanto, uma conexão fática e jurídica entre a finalidade original de coleta dos dados de registro de dados da vida civil do cidadão com a finalidade secundária da ICN.

Há, contudo, uma diferença estrutural do sistema notarial frente ao da ICN sob o ponto de vista da arquitetura informacional. Enquanto os cartórios do registro civil estruturam-se sob uma lógica descentralizada, a ICN é, por excelência, um modelo centralizado e que agrega dados de várias outras esferas. Além disso, a coleta dos dados, a partir de seu contexto, no sistema notarial, traz a expectativa de um uso restrito, como para obtenção de uma certidão de nascimento, casamento ou óbito. Há um distanciamento, portanto, da finalidade secundária de composição do banco de dados da ICN, que disponibiliza os dados para uma ampla gama de entidades governamentais, todas as relações do cidadão com o governo, e até mesmo particulares. Dessa forma, entende-se que o grau de compatibilidade da arquitetura informacional da ICN e do CRC é baixo, de modo que, ao final, a compatibilidade entre o uso primário e o uso secundário de dados, para este caso, seria média.

Por fim, as bases de dados dos Institutos de Identificação dos Estados e do Distrito Federal e do Instituto de Identificação Nacional, as quais também compõem a ICN, contêm dados das carteiras de identidade emitidas por essas entidades, conforme a Lei nº 7.116/1983. Assim como a ICN e os cartórios de registro civil, as bases dos Institutos de Identificação dos Estados e do Distrito Federal e do Instituto Nacional de Identificação atestam atributos biográficos da pessoa natural necessários para o exercício de uma série de direitos. Existe, portanto, uma conexão fática entre a finalidade original de coleta de dados, de registro de dados da vida civil do cidadão, com a finalidade secundária, da ICN, de identificação do

cidadão em suas relações com o governo e entidades privadas.

Em paralelo, de forma semelhante às bases de dados do SIRC e do CRC Nacional, as bases dos Institutos de Identificação dos Estados e do Distrito Federal e do Instituto Nacional de Identificação registram dados biográficos da pessoa natural necessários para exercício de uma série de direitos, ainda que a partir de arquiteturas opostas: descentralizadas no institutos de identificação e centralizadas na ICN. Existe também uma conexão jurídica entre as finalidades estabelecidas pela LICN de identificar o cidadão em suas relações com o Estado e particulares e a finalidade estabelecida na lei da carteira de identidade (Lei nº 7.116/1983, art. 6º), de fazer prova dos dados incluídos na carteira de identidade para relacionamento com terceiros. Existem dados sensíveis envolvidos na operação, já que, de acordo com a Lei nº 7.116/1983, art. 3º, alínea (f), a carteira de identidade contém fotografia e a impressão digital do dedo direito do identificado, os quais são, a depender do contexto em que tratados, dados biométricos. Quanto à expectativa legítima dos titulares, verifica-se a expectativa de um uso restrito destes dados, pelo próprio contexto da coleta, cuja finalidade específica era a de obtenção de um documento - no caso, o RG. Da ponderação desses critérios, compreende-se que, ao final, o grau de compatibilidade entre o uso primário da base de dados dos institutos de identificação e seu uso secundário na composição da BDICN é médio.

Ao lado de todas essas atividades que envolvem o uso secundário de dados na constituição da BDICN, há ainda a segunda grande etapa em que esse tipo de operação ocorre: a utilização da Base de Dados da ICN para identificação do cidadão no login do gov.br. Neste caso, existe uma forte conexão fática entre a finalidade original e a finalidade secundária dos dados: a finalidade da ICN é a identificação do cidadão em suas relações com o Estado e com entes privados, e, sendo o gov.br a plataforma que concentra os serviços digitalizados do Estado, pode-se dizer que a identificação do cidadão no gov.br está abarcada pela finalidade da ICN. É dizer, na medida em que o acesso a serviços públicos digitalizados se constitui como relação Estado-cidadão, pode-se dizer que há uma convergência das finalidades inicial e secundária de tratamento de dados. Há, também, uma conexão jurídica entre essas finalidades, já que a utilização da BDICN no gov.br está regulamentada pelo ACT firmado entre o governo federal e o TSE.

Aqui, é de difícil avaliação a expectativa legítima dos titulares de dados em relação ao uso da BDICN para sua autenticação no gov.br, uma vez que a própria constituição da BDICN não se dá, necessariamente, de acordo com sua legítima expectativa, como explicado acima. Acerca da arquitetura informacional, tanto a BDICN quanto o gov.br são arquiteturas centralizadas - a BDICN combina diversas bases de dados de maneira centralizada, enquanto o gov.br combina diversas fontes de informação do governo, a nível federal,

estadual e municipal, em um único portal, centralizando a oferta de serviços e informações públicas. Considerando o grau de conexão fática e jurídica entre a finalidade original e a finalidade secundária e o grau de conexão de arquitetura informacional, ambos altos, a compatibilidade entre a finalidade original da BDICN e a finalidade secundária do seu uso no gov.br é, igualmente, alta.

Independente dos graus de compatibilidade avaliados, é importante ressaltar que a prevalência de dados sensíveis, constatável em todas as bases de dados, assim como a legítima expectativa dos usuários de uso mais restrito dos dados a partir do contexto da coleta, recomenda maior cautela em todas as operações de uso secundário dos dados.

Considerando os aspectos sugeridos pela ANPD (2022, p. 13)[20] e os novos critérios aqui propostos, buscando sintetizar a análise acima pormenorizada, foi elaborada a tabela abaixo, para esquematizar a compatibilidade entre a finalidade do uso original e a dos usos secundários de dados pessoais dos cidadãos:

20 (i) o contexto e as circunstâncias relevantes do caso concreto; (ii) a existência de conexão fática ou jurídica entre a finalidade original e a que fundamenta o tratamento posterior; (iii) a natureza dos dados pessoais, adotando-se posição de maior cautela quando abrangidos dados sensíveis; (iv) as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos; e (v) o interesse público e a finalidade pública específica do tratamento posterior, bem como o seu vínculo com as competências legais dos órgãos ou entidades envolvidos, nos termos do art. 23 da LGPD (ANPD, 2022, p. 13)

Base de Dados	Agente de Tratamento de Dados	Observações sobre o agente de tratamento de dados	Grau de conexão fática e jurídica entre a finalidade original e a posterior	Natureza, tipo dos dados pessoais e Impacto sobre direitos e liberdades fundamentais	Grau de Conexão de Arquitetura Informacional	Grau de compatibilidade
Base de dados biométricos da Justiça Eleitoral	Tribunal Superior Eleitoral	Pessoa Jurídica de Direito Público e pertencente ao Poder Judiciário	**Baixo** (identificação do titular dados na condição específica de eleitor)	**Sensível** (biométrico) e **alto impacto** em razão de irreversibilidade de roubo de identidade	**Baixo** (não envolve combinação de outras bases de dados)	**Baixo**
Sistema Nacional de Informações de Registro Civil (SIRC) (Decreto 9.929, de 22 de julho de 2019)	Cartório de Registro Civil	Pessoa Jurídica de Direito Privado e serviço por delegação pública	**Alto** (identificação do titular para o exercício de uma série de direitos com entidades públicas e privadas)	**Sensível** (raça e etnia) e **alto impacto** em razão de irreversibilidade de roubo de identidade	**Baixo** (envolve combinação de base de dados, mas a partir de um modelo descentralizado)	**Médio**
Central Nacional de Informações do Registro Civil (CRC Nacional) Provimento nº46 do CNJ (CNJ, 2015)	Cartório de Registro Civil	Pessoa Jurídica de Direito Privado e serviço por delegação pública	**Alto** (identificação do titular para o exercício de uma série de direitos com entidades públicas e privadas)	**Sensível**[21] (raça e etnia) e **alto impacto** em razão de irreversibilidade de roubo de identidade	**Baixo** (envolve combinação de base de dados, mas a partir de um modelo descentralizado)	**Médio**
Bases de dados Institutos de Identificação dos Estados e do DF	Institutos de Identificação dos Estados e DF	Pessoa Jurídica de Direito Público	**Alto** (identificação do titular para o exercício de uma série de direitos com entidades públicas e privadas)	**Sensível** (foto e biometria) e **alto impacto** em razão de irreversibilidade de roubo de identidade[22]	**Baixo** (envolve combinação de base de dados e a partir de um modelo descentralizado)	**Médio**
Instituto Nacional de Identificação	Instituto Nacional de Identificação	Pessoa Jurídica de Direito Público	**Alto** (identificação do titular para o exercício de uma série de direitos com entidades públicas e privadas)	**Sensível** (foto e biometria) e **alto impacto** em razão de irreversibilidade de roubo de identidade[23]	**Baixo** (envolve combinação de base de dados e a partir de um modelo descentralizado)	**Médio**
BDICN	Tribunal Superior Eleitoral (controlador) SERPRO (operador)[24]	Pessoa Jurídica de Direito Público e Empresa Pública, respectivamente	**Alto** (identificação do titular para o exercício de uma série de direitos com entidades públicas e privadas)	**Sensível** (biométrico) e **alto impacto** em razão de irreversibilidade de roubo de identidade	**Alto** (envolve combinação de diversas bases de dados de maneira centralizada)	**Alto**

21 Certidão de óbito contém dados de raça/etnia, conforme art. 80, § 3º, Lei 6.015/1973.

22 Carteira de Identidade contém impressão digital do polegar direito do identificado e fotografia 3x4, conforme art.3, alínea (f), lei 7.116/1983.

23 Carteira de Identidade contém impressão digital do polegar direito do identificado e fotografia 3x4, conforme art. 3, alínea (f), lei 7.116/1983.

24 Contrato celebrado entre o TSE e o SERPRO para "Operacionalização da Identificação Civil Nacional (ICN) abrangendo serviços de conferência biográfica e biométrica, pesquisa biográfica e emissão de Documento Nacional de Identificação (DNI)": TSE (2021e)

Uso compartilhado de dados no poder público

A LGPD define em seu art. 5º, XVI, o uso compartilhado de dados como:

> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (BRASIL, 2018);

Conforme pontuado anteriormente, a Lei da Identificação Civil Nacional traz hipóteses de uso compartilhado dos dados ao facultar acesso à Base de Dados da ICN aos poderes Executivo e Legislativo dos Municípios, Estados, Distrito Federal, e União, em seu art. 3º, desde que o uso seja feito com a mesma finalidade da ICN em si - qual seja, de "identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados", conforme o art. 1º da LICN. Além disso, verifica-se também o uso compartilhado de dados no emprego da BDICN para autenticação do cidadão no gov.br.

Além do art. 5º, o art. 25 da LGPD, integrante da seção da lei que disciplina o tratamento de dados pelo poder público, prevê a manutenção dos dados "em formato interoperável e estruturado para o uso compartilhado". Adiante, o art. 26 da LGPD determina o uso compartilhado para "atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei."

A ANPD (2022), em consonância com as disposições legais, definiu o compartilhamento de dados pessoais como "a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública" (ANPD, 2022, p.17).

Nessa linha, a Autoridade (2022) estabeleceu os seguintes requisitos como principais para serem observados nos processos de compartilhamento de dados pessoais pelo poder público: (a) formalização e registro do uso compartilhado de dados pessoais pelo poder público; (b) indicação do objeto (dados pessoais objeto de compartilhamento) e finalidade específica do compartilhamento; (c) base legal (art. 7º ou art. 11 da LGPD); (d) duração do tratamento; (e) transparência e direitos dos titulares; (f) prevenção e segurança (ANPD,

2022, p. 17-19). Outros requisitos podem ser necessários a depender das particularidades do caso, inclusive podendo haver autorização ou vedação para novo compartilhamento ou transferência posterior dos dados pessoais, requisitos específicos para compartilhamento de dados pessoais com entidades privadas conforme a LGPD e a elaboração de um relatório de impacto à proteção de dados pessoais (ANPD, 2022).

O que se tem, então, é que, existindo operações calcadas no uso compartilhado e secundário de dados pessoais, impõem-se uma série de medidas de governança mais robustas, como as acima listadas. No presente documento, tais medidas de governança devem se aplicar, em específico, ao uso compartilhado da Base de Dados da ICN pelo gov.br para identificação dos cidadãos. Esse uso está disciplinado no Acordo de Cooperação Técnica firmado entre o Poder Executivo e o TSE, de março de 2021 (TSE, 2021b; BRASIL, 2021b).

No acordo, fica formalizado o uso compartilhado de dados pessoais pelo poder público, indicando que será compartilhada a Base de Dados da ICN, com a finalidade de "promover o fortalecimento de um sistema nacional integrado de identificação do cidadão (...) no contexto da plataforma GOV.BR" (BRASIL, 2021b). Não é mencionada a base legal do tratamento a partir da Lei Geral de Proteção de Dados. Acerca da duração do tratamento, o acordo tem prazo de duração de 60 meses, sendo prorrogável pelas partes por número indeterminado de vezes. Ademais, o documento não faz qualquer menção aos direitos dos titulares ou medidas de transparência sobre esse acordo, assim como a medidas de prevenção e segurança para o tratamento de dados pessoais.

De fato, a Lei Geral de Proteção de Dados é mencionada uma única vez no ACT, em sua cláusula quarta, que determina como uma das metas do Acordo o estabelecimento de regras de adequação dos serviços à Lei Geral de Proteção de Dados: "em especial, prevendo a disponibilização de ferramentas que garantam a rastreabilidade do acesso aos dados e à gestão do consentimento, bem como prever os papéis que cada um dos partícipes desempenhará em conformidade com a Lei nº13.709/2018, especialmente quanto ao disposto em seu art.9º, e em conformidade com as previsões do art.7º".

Neste *policy paper*, são discutidos a partir da estrutura da ICN tanto a transparência e os direitos dos titulares (Capítulo 3, seção 3.3f), quanto os aspectos de prevenção e segurança (Capítulo 3, seção 3.3a). As principais conclusões são da opacidade da ICN e da dificuldade dos exercícios dos direitos dos titulares, assim como do maior risco à segurança dos dados pelo modelo centralizado escolhido pela ICN.

Freios e contrapesos no uso secundário e compartilhado de dados no poder público: teoria da separação informacional

Wimmer (2021a) aponta como problemática central da LGPD a existência de uma lacuna no que diz respeito às possibilidades e aos limites para o compartilhamento e uso secundário de dados pessoais no âmbito do poder público, isto é, a inexistência de critérios claros que disciplinam tais atividades. Essa falta de limites expressos, de seu turno, pode levar a usos abusivos dos dados, que violem os direitos de seus titulares. Diante desse quadro, a autora propõe em seu trabalho três parâmetros a serem considerados para legitimar o compartilhamento e uso secundário de dados no poder público.

O primeiro deles seria a compatibilidade de finalidades entre o tratamento original e o uso secundário, entendimento expressamente adotado pela LGPD, como já visto neste relatório. Se não houvesse tal compatibilidade, outros dois elementos adicionais, a depender das condições concretas do caso, poderiam ser considerados para superar tal incompatibilidade: uma nova autorização fornecida pelo titular do dado ou a existência de uma previsão legal específica. Tais entendimentos mais flexíveis encontram amparo na Resolução do Conselho da Europa sobre a proteção da privacidade de indivíduos face a bases de dados eletrônicas no setor público, de 1974, nas Diretrizes da OCDE sobre privacidade atualizadas em 2013 e na lógica adotada pela GDPR (WIMMER, 2021a, p. 137). Em qualquer um dos casos, devem ser aplicados os princípios de proteção de dados, por meio das salvaguardas materiais e procedimentais que se fizerem necessárias na atividade de tratamento, além de ser fornecida ao indivíduo afetado adequada informação sobre a operação e serem considerados os princípios constitucionais protetivos da liberdade individual, privacidade e livre desenvolvimento da personalidade.

Wimmer (2021a) centraliza sua discussão sobre o compartilhamento de dados nas iniciativas de governo eletrônico, como o gov.br, ressaltando que o debate sobre compartilhamento e uso secundário de dados no âmbito do poder público desperta duas perspectivas que se opõem: uma que defende o amplo compartilhamento de dados entre entes públicos, para propiciar uma oferta de melhores serviços públicos, eficiência e desburocratização; e outra, que chama atenção para os riscos decorrentes de tais iniciativas, como a vigilância estatal.

Longe de ser um embate entre um interesse público e voltado para coletivo (melhores políticas públicas) e um interesse privado voltado para o indivíduo (direito à privacidade e proteção de dados), Wimmer (2021a) destaca como o direito à privacidade e à proteção de dados tem uma dimensão metaindividual e está também relacionado ao interesse público.

Esse tema do compartilhamento de dados pessoais no âmbito do poder público está sendo discutido na ADPF 695, pendente de julgamento pelo STF até a finalização da escrita deste relatório, em maio de 2022. A ação discute o compartilhamento de dados da Carteira Nacional de Habilitação dos cidadãos Brasileiros originalmente coletados pelo Departamento Nacional de Trânsito (DENATRAN) pelo Serviço Federal de Processamento de Dados (SERPRO) com a Agência Brasileira de Inteligência (ABIN), que tem como fundamento o Decreto nº 10.046/2019 (Decreto que regulamenta a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base Cidadão e o Comitê Central de Governança de Dados). Tal decreto dispensa a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para efetivação do compartilhamento de dados entre órgãos e entidades da administração pública federal.

Em 24 de junho de 2020, o Ministro Relator Gilmar Mendes indeferiu a medida cautelar da ADPF, entendendo por sua perda de objeto, uma vez que o Poder Executivo já havia revogado o termo de autorização de compartilhamento. Na decisão, entretanto, o Ministro determinou o prosseguimento da ação, destacando a relevância do seu objeto - o Decreto 10.046/2019, do Cadastro Base Cidadão:

> (...) o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (art. 5º, caput e incisos X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea (STF, 2021, p. 47).

Em análise de tal texto legislativo, o Ministro Gilmar Mendes afirmou que este vai contra a lógica de afirmação do princípio da finalidade, reduzindo e por vezes eliminando quaisquer barreiras ao livre fluxo de compartilhamento de dados pessoais na administração pública, em especial diante de seus art. 5º e 11.

O Ministro também destacou que reconhecer a autonomia do direito fundamental à proteção de dados pessoais leva necessariamente à consciência de que o regime jurídico de privacidade é estrutural dos regimes democráticos, e não um valor contraposto ao interesse público, de mera proteção de direitos individuais. Por fim, adiantou não existir indicação, a priori, de "uma autorização irrestrita no ordenamento jurídico brasileiro ao livre fluxo e compartilhamento de dados no poder público, inclusive para realização das atividades de inteligência nacional" (STF, 2021, p. 38-39), não sendo o Estado, portanto, uma única unidade informacional.

Essa ideia de que o Estado não é uma única unidade informacional é, muitos anos antes, apresentada por Simitis (1987). Para o autor, o princípio da finalidade é um dos quatro elementos básicos de qualquer regulação da proteção de dados e pode ser definido como uma barreira normativa ao uso multifuncional desregulado dos dados. Nessa esteira, a divisão organizacional, já existente no Estado moderno no âmbito da administração pública direta (e.g., as pastas dos diferentes ministérios) e indireta (e.g., autarquia, fundações e agências reguladoras), deve ser espelhada sob o aspecto informacional. O que o autor propõe, portanto, é o conceito de separação informacional dos poderes, de acordo com o qual o que vai determinar a possibilidade de acesso a um dado é a função específica da agência-entidade governamental que pretende tratá-lo e a sua relação com a finalidade que levou à coleta do dado - e não, simplesmente, o fato de o agente de tratamento ser parte do Estado (Simitis, 1987) e de constatar-se, em potencial, um interesse público no tratamento.

O modelo brasileiro da ICN - que é resultado da agregação de uma série de bases de dados que perpassam a esfera eleitoral, a notarial e o próprio Poder Executivo e garante amplo acesso às suas bases de dados às agências e entidades governamentais - colide diretamente com a teoria da separação informacional dos poderes. Essa colisão, vale dizer, é ainda mais agravada pelo uso secundário da ICN para alimentar o gov.br, uma plataforma que datifica e projeta o cidadão para todas as suas relações para com o Estado e, em alguns casos, com particulares.

A presente seção expôs, de início, uma definição de uso secundário de dados pessoais, e a importância do princípio da finalidade para avaliar a legitimidade do uso secundário. A partir dos critérios trazidos pela ANPD (2022), foram avaliados dois usos secundários de dados pelo poder público, analisados neste documento: o uso das bases de dados do TSE, SIRC, CRC e Institutos de Identificação para composição da BDICN, conforme a LICN, e o uso da Base de Dados da ICN para autenticação dos cidadãos no gov.br. A avaliação foi baseada no grau de compatibilidade entre a finalidade do uso para o qual o dado foi originalmente coletado e a finalidade do uso secundário. O grau de compatibilidade dos dois usos secundários analisados foi médio. A única exceção foi a base de dados eleitoral, cujo uso secundário na constituição da BDICN foi avaliado com baixo grau de compatibilidade.

Uma vez feitas as considerações e avaliações acerca do uso secundário de dados pelo poder público, esta seção tratou do uso compartilhado de dados por agentes do setor público, valendo-se das diretrizes estabelecidas pela ANPD (2022), utilizadas como um substrato analítico para a avaliação realizada. Na seção, foram trazidos também o caso da ADPF 695 e o conceito de separação informacional de poderes, que em um mesmo sentido apontam que o Estado não pode ser tratado como uma única unidade informacional, com um livre fluxo de dados entre agências e entidades governamentais.

Considerando a gramática dos riscos em proteção de dados pessoais, a ser pormenorizada no Capítulo 5 deste documento, o uso compartilhado ou secundário de dados de maneira abusiva, sem considerar a finalidade para a qual os dados foram coletados, pode ser compreendido como um risco para os cidadãos. Isso porque dados inicialmente coletados para a finalidade de identificação civil poderiam, por exemplo, ser usados abusivamente por agências de inteligência estatal, para suas atividades de inteligência, a exemplo do caso concreto impugnado na ADPF 695.

O acesso à BDICN conforme previsto na LICN e no PL nº 3228/2021

A Lei da Identificação Civil Nacional, em seu art. 3º, garante acesso à Base de Dados da ICN, excetuadas as informações eleitorais, aos Poderes Executivo e Legislativo de todos os níveis da federação. Adiante, no parágrafo primeiro do mesmo dispositivo, a lei dispõe, inclusive, que o Poder Executivo dos entes federados poderá integrar aos seus bancos de dados as informações da Base de Dados da ICN, com exceção dos dados biométricos[25].

Em paralelo, o Projeto de Lei nº 3228/2021, de autoria do governo federal, pretende alterar a Lei da Identificação Civil Nacional de forma a permitir a replicação da Base de Dados da ICN em ambientes do Poder Executivo Federal, removendo a exceção de acesso aos dados biométricos, mantendo apenas a restrição de acesso às informações eleitorais[26].

O que se verifica na LICN e na proposta que a alteraria é a remoção de barreiras de acesso aos dados pessoais dos cidadãos pelo poder público. A princípio, a lei não traz exigências quanto à finalidade específica e determinada para o compartilhamento dos dados, o que contraria o princípio da finalidade previsto na LGPD. Ainda mais preocupante, os dados compartilhados poderiam ser integrados às bases de dados de novas entidades e órgãos do poder público de forma definitiva. Além de gerar um problema crítico de segurança da

25 Art. 3º O Tribunal Superior Eleitoral garantirá aos Poderes Executivo e Legislativo da União, dos Estados, do Distrito Federal e dos Municípios acesso à base de dados da ICN, de forma gratuita, exceto quanto às informações eleitorais.

§ 1º O Poder Executivo dos entes federados poderá integrar aos seus próprios bancos de dados as informações da base de dados da ICN, com exceção dos dados biométricos.

26 Art. 2º .....

§ 1º A base de dados da ICN será armazenada e gerida pelo Tribunal Superior Eleitoral, que a manterá atualizada e adotará as providências necessárias para assegurar a integridade, a disponibilidade, a autenticidade e a confidencialidade de seu conteúdo e a interoperabilidade entre os sistemas eletrônicos governamentais, facultada ao Tribunal Superior Eleitoral a replicação da base de dados em ambientes computacionais do Poder Executivo federal.

Art. 3º .....

§ 1º-A O disposto no § 1º poderá se aplicar a dados biométricos quando expressamente autorizado no instrumento de que trata o § 3º do art. 2º.

informação na medida em que se perde o controle de quem, quando e para o que se acessa tais dados, também é de se questionar: qual a pertinência de um ente federado do Poder Executivo, de atuação local, ter uma base de dados nacional de identidade, de cidadãos que não estão sob sua jurisdição?

Como já frisado neste *policy paper*, qualquer compartilhamento e uso secundário de dados no poder público deve ser guiado pelos princípios da proteção de dados - especialmente, no caso da ICN e do gov.br, os princípios da finalidade, adequação e necessidade. O PL nº 3228/2021, nesse sentido, se coloca em rota de colisão com tais princípios da LGPD, exacerbando riscos aos direitos e liberdades civis dos titulares de dados, tornando ainda mais complexas as considerações acerca da governança da ICN sob o ponto de vista de segurança da informação.

e. O cruzamento de bases de dados oficiais

Políticas públicas como a ICN possuem relação direta com a concretização do princípio da não discriminação, um dos objetivos fundamentais da República, disposto no art. 3º da Constituição Federal, e que está refletido na LGPD, a qual, de seu turno, estabelece no rol de princípios da proteção de dados pessoais a não discriminação (art. 6º, inciso IX).

Segundo a Lei Geral de Proteção de Dados, as atividades de tratamento de dados pessoais devem se orientar pela não discriminação ilícita e abusiva. Por sua vez, a garantia de tal princípio quando a atividade de tratamento de dados pessoais se dá no interior da Administração Pública é atravessada pela necessidade de que se tenha ampla publicidade e transparência das atividades de tratamento.

No caso da Identificação Civil Nacional, existe uma previsão legal no art. 11 da LICN[27] sobre a possibilidade de cruzamento de bancos de dados oficiais com intuito de verificar o cumprimento de requisitos necessários à elegibilidade de determinado cidadão para a concessão ou manutenção de benefícios sociais.

Nesse sentido, o acesso a determinados benefícios sociais estaria vinculado ao processo de cruzamento de dados pessoais do beneficiário para a verificação de cumprimento dos requisitos legais necessários a tal acesso. Desse modo, é possível afirmar o risco dessa

27 Redação do art. 11 da Lei 13.444/2017: "O poder público deverá oferecer mecanismos que possibilitem o cruzamento de informações constantes de bases de dados oficiais, a partir do número de inscrição no CPF do solicitante, de modo que a verificação do cumprimento de requisitos de elegibilidade para a concessão e a manutenção de benefícios sociais possa ser feita pelo órgão concedente".

atividade de tratamento de dados incorrer em resultados excludentes. Conforme Relatório Especial da ONU em Extrema Pobreza e Direitos Humanos, de 11 de outubro de 2019 (United Nations, 2019), Estados estão crescentemente se utilizando de tecnologias digitais e dados em seus sistemas de proteção e assistência social, muitas vezes de maneira prejudicial aos mais vulneráveis socioeconomicamente. Há uma proliferação de valores neoliberais hostis aos sistemas de assistência social e proteção, que são implementados de forma conjunta com a tecnologia, em desrespeito aos direitos humanos:

> O estado de bem-estar social digital já é uma realidade ou está emergindo em diversos países no mundo. Nesses estados, sistemas de proteção social e assistência são crescentemente dirigidos por dados digitais e tecnologias utilizadas para automatizar, realizar predições, identificar, vigiar, detectar, colocar como alvo e punir. Esse relatório reconhece as atrações irresistíveis para os governos assumirem essa direção, mas avisa dos riscos de se ingressar em uma distopia do estado de bem-estar social. O relatório argumenta que as empresas de Big Tech operam como se não se aplicasse a elas direitos humanos, e isso é especialmente problemático quando o setor privado está em um papel de liderança no desenho, construção e operação de parte significativa do estado de bem estar social digital. O relatório recomenda que ao invés de obcecar sobre fraude, economia de custos, sanções e definições de mercado de eficiência, o ponto de partida deveria ser como os orçamentos de assistência social podem ser transformados através da tecnologia para garantir um padrão maior de vida para os vulneráveis (UNITED NATIONS, 2019, p.1, tradução livre)[28].

Esses potenciais resultados discriminatórios decorreriam, por exemplo, do cruzamento de bases de dados que, não necessariamente, guardam pertinência com a finalidade de verificar o cumprimento de requisitos para o acesso a benefícios sociais, como dados sobre raça, etnia e gênero. Assim, pode-se falar na posibilidade de discriminação negativa de cidadãos, sendo ainda mais necessário o estabelecimento de parâmetros claros de governança sobre os dados que serão eventualmente cruzados para avaliação da elegibilidade para políticas públicas.

Recentemente, na Holanda, a autoridade fiscal adotou um sistema de decisão contendo um algoritmo que criava perfis de risco para indivíduos que requisitavam benefícios sociais

28 Tradução livre das autoras do *policy paper*.

para cuidado de crianças sob sua responsabilidade. O objetivo do sistema era identificar potenciais pedidos fraudulentos ou com incorreções de maneira mais precoce. Após a análise de pesquisadores, entretanto, foi constatado que um dos fatores que foi considerado um risco para se ter um pedido fraudulento ou com incorreções foi a nacionalidade da pessoa requisitando o benefício, o que, por certo, recai em hipótese de discriminação massiva e perfilamento racial (AMNESTY INTERNATIONAL, 2021).

Nessa seara, ainda, e voltando-se ao contexto nacional, cumpre destacar a decisão do Ministro Luís Roberto Barroso em sede do Mandado de Segurança nº 36150, impetrado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) contra acórdão do Tribunal de Contas da União (TCU) que determinava o compartilhamento de dados individualizados do Censo Escolar e do ENEM para a realização de auditoria do Bolsa Família (STF, 2021).

Apesar de reconhecer a competência constitucional do TCU para a realização de auditorias e inspeções de natureza contábil, financeira, orçamentária e patrimonial nos órgãos da Administração Pública, o Ministro Barroso evidenciou a importância do princípio da finalidade para a coleta de dados pessoais. Segundo a decisão, os dados requeridos pelo TCU foram coletados pelo INEP para o cumprimento de finalidades específicas, sob a garantia de sigilo do Instituto. Nesse sentido, o Ministro relator afirma que o compartilhamento de tais dados para uma finalidade diversa daquela inicialmente pactuada configuraria uma desvirtuação do princípio da finalidade e, consequentemente, representaria uma subversão à autorização daqueles que forneceram os seus dados.

É possível traçar um paralelo entre esse caso e o que dispõe o art. 11 da LICN, uma vez que, ao cruzar os dados que compõem a Base de Dados da ICN – tratados com a finalidade específica de identificação civil dos cidadãos – com outros dados, a fim de se verificar o cumprimento de requisitos para o acesso a benefícios sociais, o poder público poderia incorrer em um desvio de finalidade. Desse modo, tem-se uma potencial violação do princípio da não discriminação, pela produção de resultados excludentes, e uma violação do princípio da finalidade, ambos dispostos na LGPD[29].

29 Sobre uso compartilhado e secundário de dados, ver a subseção 3.3d deste *policy paper*.

f. Omissões da LICN: exercício dos direitos dos titulares de dados e publicidade–transparência do tratamento de dados pessoais

Como apontado anteriormente, trata-se a ICN de uma política pública, amparada pelo princípio da legalidade, e que se sustenta sobre o tratamento em larga escala de dados pessoais, especialmente dados biométricos - é dizer, dados sensíveis. Isso significa que o tratamento de dados pessoais feito pelo poder público a partir da BDICN, como é a autenticação dos cidadãos para acesso a serviços públicos via gov.br, evoca a necessidade de convergência entre dois grandes grupos de princípios: aqueles definidos pela Lei de Proteção de Dados – que devem orientar toda e qualquer atividade de tratamento de dados -, e os princípios constitucionais que regem a Administração Pública (WIMMER, 2021b).

Há um suposto conflito entre a necessidade de que as atividades executadas pela Administração Pública sejam transparentes e a garantia da proteção de dados dos titulares (WIMMER, 2021b). Tal conflito, no entanto, pode ser caracterizado meramente como aparente, uma vez que a transparência das atividades de tratamento do poder público são fundamentais para a garantia de direitos dos titulares, especialmente quando se considera que, para a Lei Geral de Proteção de Dados, em seu art. 6º, inciso VI, a transparência é definida como "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

A despeito dessa convergência, o que se depreende a partir da execução da política pública da Identificação Civil Nacional é que existe certa opacidade sobre como ocorrem as operações de tratamento dos dados pessoais utilizados para a identificação dos cidadãos e a autenticação destes dentro da plataforma gov.br.

Tal dificuldade vai de encontro com algumas disposições presentes na LGPD, especialmente aquelas que dizem respeito à atividade de tratamento de dados pessoais pelo poder público. Conforme o art. 23, inciso I da referida lei, o tratamento de dados pessoais por pessoas jurídicas de direito público será autorizado para o cumprimento de obrigação legal que atenda o interesse público, desde que:

> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos (BRASIL, 2018)

Na mesma esteira de se estabelecer a publicidade e, portanto, a transparência das atividades de tratamento de dados pessoais pelo poder público como um dever da Administração Pública, a Autoridade Nacional de Proteção de Dados (ANPD), em seu Guia Orientativo sobre o Tratamento de Dados Pessoais pelo poder público, evidencia que a Lei de Governo Digital (Lei 14.129/2021) estabelece medidas específicas sobre a publicidade e transparência das atividades de tratamento de dados pessoais pelo poder público, de modo a viabilizar a concretização dos direitos dos titulares, enumerados no art. 18 da LGPD. Segundo o art. 25 da Lei de Governo Digital:

> Art. 25. As Plataformas de Governo Digital **devem dispor de ferramentas de transparência e de controle do tratamento de dados pessoais que sejam claras e facilmente acessíveis e que permitam ao cidadão o exercício dos direitos previstos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).**
>
> § 1º As ferramentas previstas no *caput* deste artigo devem:
>
> I - disponibilizar, entre outras, as fontes dos dados pessoais, a finalidade específica do seu tratamento pelo respectivo órgão ou ente e a indicação de outros órgãos ou entes com os quais é realizado o uso compartilhado de dados pessoais, incluído o histórico de acesso ou uso compartilhado, ressalvados os casos previstos no inciso III do *caput* do art. 4º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
>
> II - permitir que o cidadão efetue requisições ao órgão ou à entidade controladora dos seus dados, especialmente aquelas previstas no art. 18 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).
>
> § 2º A Autoridade Nacional de Proteção de Dados (ANPD) poderá editar normas complementares para regulamentar o disposto neste artigo. (BRASIL, 2021c, grifo nosso)

Isso significa que existe uma expectativa sobre a publicidade de atos estatais, de modo a incentivar a criação de:

> "uma espécie de cidadania ativa, própria dos modelos republicanos, uma vez que propicia aos cidadãos o controle da atividade pública, supervisionando, sobretudo, a gestão da coisa pública. Neste sentido, Daniel Sarmento (2014, p. 2017, apud MULHOLLAND, MATERA, 2020, p. 225) afirma que 'o republicanismo enfatiza a importância da esfera pública como local de trocas de razões, exercendo importante papel de supervisão sobre o funcionamento concreto das instituições políticas formais'" (MULHOLLAND, MATERA, 2020, p. 225).

Dadas essas disposições, é possível falar em uma potencial incompatibilidade entre o dever de transparência estatal e a Identificação Civil Nacional. Tal tensão se justifica pelo fato de o governo federal não disponibilizar um acesso facilitado, aos cidadãos, a documentação que contemple tanto a finalidade das atividades de tratamento de dados envolvidas na Identificação Civil Nacional quanto os procedimentos e técnicas de tratamento de dados pessoais utilizadas pela ICN e pelo serviço de autenticação de usuários na plataforma gov.br. Desse modo, gera-se o risco de dificultar ou até mesmo impossibilitar o exercício dos direitos dos titulares, bem como a fiscalização, pela sociedade civil, das referidas políticas públicas. Tais direitos, enumerados no art. 18 da LGPD, visam possibilitar ao titular de dados a capacidade de gerenciamento sobre os seus próprios dados (SILVA, 2020), de modo a se alcançar a autodeterminação informativa, disposta como um dos fundamentos da proteção de dados pessoais no Brasil.

Para os fins deste documento, serão tratados os direitos dos titulares dispostos nos incisos I, II e III do art. 18, os quais correspondem à confirmação da existência do tratamento, ao acesso aos dados e à correção de dados incompletos.

Segundo Silva (2020), o direito à confirmação de existência de tratamento de dados, disposto no art. 18, inciso I da LGPD, deriva do princípio da transparência, devendo ser garantido sem qualquer oposição pelo agente de tratamento, uma vez que

> a ausência de confirmação do tratamento de dados é prejudicial à garantia dos demais direitos, principalmente considerando os casos em que o requisito invocado para o tratamento de dados não é consentimento, situações estas em que o titular dos dados somente poderá ter ciência da coleta de dados mediante a comunicação da confirmação por parte do responsável pelo tratamento. (SILVA, 2020, p. 196)

Por sua vez, o direito de acesso aos dados, previsto no art. 18, inciso II da LGPD, é um desdobramento lógico do direito à confirmação de tratamento de dados, de modo que o seu exercício tem por objetivo a verificação, pelo titular de dados, de como os seus dados têm sido tratados (SILVA, 2020), isto é, se o tratamento de dados ocorre de forma segura e cumprindo sua finalidade.

Nesse sentido, Silva (2020) argumenta que o referido direito decorre do princípio do livre acesso, o qual é caracterizado pela "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (BRASIL, 2018), segundo o art. 6º, inciso VI da Lei Geral de Proteção de Dados.

Em paralelo, o direito à correção dos dados incompletos deriva do princípio da qualidade de dados, o qual foi abordado no Capítulo 3, seção 3.3c deste documento, sendo a garantia dos dados atualizados fundamental para o cumprimento da finalidade de determinada atividade de tratamento de dados pessoais, sobretudo de atividades que ocorram no bojo da execução de políticas públicas, como é o caso da Identificação Civil Nacional e da utilização de sua base de dados na autenticação de usuários na plataforma gov.br. Em atenção ao direito à correção de dados incompletos, deve o agente de tratamento, como uma boa prática, manter um registro histórico das modificações e atualizações realizadas, ampliando o acesso às informações pelo titular de dados (SILVA, 2020).

Aqui, a opacidade identificada na política pública de autenticação de usuários na plataforma gov.br, a partir da utilização da Base de Dados da ICN, tem o potencial de inviabilizar o exercício de direitos pelos titulares de dados pessoais. Tal potencial pode ser identificado na ausência de um canal de comunicação direto e adequado para que os cidadãos possam solicitar a confirmação da existência do tratamento de dados, o acesso aos seus dados tratados, bem como a retificação dos dados eventualmente incorretos e desatualizados.

4. Riscos de exclusão dos cidadãos do acesso aos aos serviços públicos plataformizados no gov.br

O objetivo deste capítulo é analisar vulnerabilidades sociais que podem gerar a exclusão dos cidadãos do acesso a serviços públicos no gov.br, por meio de autenticação a partir da Base de Dados da ICN. A seção, desse modo, irá explorar a segunda principal categoria de riscos mapeados na pesquisa, decorrentes da estruturação de tal política pública.

Conforme pontuado no capítulo 2 deste relatório, um dos objetivos da Estratégia de Governo Digital é a digitalização dos serviços públicos - e o gov.br é central para essa tarefa. Assim sendo, é essencial manter no horizonte as possíveis consequências que a automatização de serviços públicos para os mais vulneráveis socialmente. Como alerta Eubanks (2018), o uso de sistemas automatizados para gerenciar serviços públicos, principalmente ligados a benefícios sociais e gerenciamento da pobreza, pode aumentar a exclusão de grupos já socialmente marginalizados, impedindo que os mais vulneráveis acessem serviços sociais.

Tal conclusão de Eubanks (2018) decorre de uma investigação empírica de casos estadunidenses, a partir dos quais ela expõe como a aplicação de sistemas automatizados não aumentou a eficiência de serviços ou reduziu fraudes - afirmações e defesas usualmente usadas para implementação desses sistemas. Pelo contrário, tal disseminação aumentou vulnerabilidades socioeconômicas já existentes e intensificou a marginalização de pessoas já marginalizadas. Desse modo, o argumento da autora é de que sistemas automatizados são uma forma de "casa dos pobres" digitalizadas, em referência a locais nos quais os mais vulneráveis socialmente eram confinados nos EUA por política pública entre os séculos XVII e XX - e onde tinham suas vidas gerenciadas, mas sem se erradicar a pobreza. Apesar de o caso estadunidense, que embasa as pesquisas da autora, tratar de uma realidade geográfica e de instrumentos de política pública diferentes, os motivos para exclusão decorrente da automação de tomadas de decisão, como vulnerabilidades sociais, racismo, deficiências, exclusão de crianças e adolescentes e dificuldades com documentação são comuns também ao cenário brasileiro. Nesse sentido, esta seção constrói um breve retrato de vulnerabilidades que podem levar à exclusão de pessoas dos bancos de dados da ICN (BDICN), ou do uso do gov.br, e que não parecem ter sido consideradas no desenho dessas políticas públicas.

Para pensar o cenário brasileiro de possíveis exclusões, cabe iniciar por uma análise de vulnerabilidade social. A vulnerabilidade social no Brasil é composta a partir de desi-

gualdades estruturais enraizadas na sociedade e de uma pobreza que é generificada e racializada, com as mulheres negras no estrato mais pobre da população. Antes do início da pandemia do novo coronavírus, em 2019, 33% das mulheres negras estavam abaixo da linha da pobreza, sendo que em 2021 esse índice subiu para 38%, similar ao de homens negros. Enquanto isso, para mulheres e homens brancos, o nível era de 15% antes da pandemia e de 19% em 2021 (ROUBICEK, 2021).

Os fatores que levam a uma vulnerabilidade social também podem estar combinados, como a seguir descrito por Escóssia (2019), que constatou haver um número desproporcional de mulheres negras na pobreza ou extrema pobreza sem documentos de identificação.

4.1. Exclusão pela inadequação dos documentos de identidade

a. Falta de documento de identidade

No Brasil, para que se emita um documento de identidade, é necessário primeiro que seja emitida uma certidão de nascimento ao cidadão. A falta de registro civil da certidão de nascimento é denominada pelo IBGE subregistro, termo que se refere ao número de nascimentos não registrados no ano de sua ocorrência ou no primeiro trimestre do ano subsequente (IBGE, 2020). Não existem dados no Brasil sobre o número de adultos que hoje vivem sem registro de nascimento, sendo esses indivíduos, portanto, invisíveis para o Estado (ESCÓSSIA, 2019).

Para ter seus dados pessoais registrados no Banco de Dados da ICN, é necessário ter um documento de identidade, carteira de motorista ou título de eleitor, todos documentos cuja emissão depende de ter-se, previamente, uma certidão de nascimento. Apenas após a emissão da certidão de nascimento - chamada "documento fundador" - o cidadão pode obter outro documento - usualmente a carteira de identidade, que traz as informações do registro civil e adiciona um registro biométrico, com a coleta de impressões digitais (ESCÓSSIA, 2019). Se um cidadão não possui uma certidão de nascimento, portanto, não terá seus dados pessoais registrados no BDICN e, portanto, não poderá acessar o gov.br ou os serviços públicos por lá disponíveis.

Desde o final da década de 90 e ao longo dos anos 2000, foram implementadas campanhas governamentais para erradicar o subregistro. É especialmente relevante, dentre elas, a que envolveu a previsão da gratuidade da certidão de nascimento, instituída pela Lei nº 9.534/1997 (IBGE, 2020). Antes delas, a taxa estimada de subregistro, em 1990, era de 29,3%. Em 2002, os números caíram para 20,3% e, mais recentemente, conforme

dados de 2017, a taxa é de 2,6% do total de nascimentos (VILAS BÔAS, 2019; ESCÓSSIA, 2019). Entretanto, a despeito da decrescente do percentual, é importante ressaltar que a taxa está distribuída de maneira desigual no país, sendo mais alta nas regiões Norte (9,4%) e Nordeste (3,5%), as mais pobres do país (VILAS BÔAS, 2019). Nessa situação, é mais provável que os mais pobres e os mais velhos não tenham registro e sejam, portanto, excluídos da Base de Dados da ICN e do acesso aos serviços públicos por meio do gov.br.

Retratando o fenômeno de adultos sem registro de nascimento, Escóssia (2019) realizou uma etnografia acompanhando usuários de um serviço público gratuito de emissão de certidão de nascimento, resultante de uma pareceria entre dois projetos do Tribunal de Justiça do Estado do Rio de Janeiro (TJRJ): a Justiça Itinerante e o Serviço de Promoção e Erradicação do sub-registro de Nascimento e a Busca de Certidões (Sepec). Esses usuários não possuíam nenhuma documentação até procurar o serviço, e a autora explorou a dualidade entre o documento como chave para o controle estatal, mas também para o acesso a direitos - dualidade esta também já explorada neste *policy paper*. Pessoas sem registro de nascimento não têm nenhum outro documento, portanto não podem votar, ter emprego formal, conta em banco ou bens em seu nome. Em relação ao atendimento de saúde, só conseguem se for de emergência e, para educação, as escolas exigem documentação para matricular crianças (ESCÓSSIA, 2019).

A autora, em suas observações, constatou que as pessoas sem registro tinham em comum a raça (preta ou parda), o gênero feminino e a pobreza ou extrema pobreza. Outro aspecto conclusivo relevante é de que muitas vezes a falta de registro era geracional: se a mãe não possuir registro, não consegue registrar seus filhos (ESCÓSSIA, 2019), o que promove um ciclo de exclusão de difícil rompimento:

> O sub-registro segue sendo um problema associado à exclusão social e à cidadania diferenciada a que uma parcela da população brasileira é submetida. A baixíssima escolaridade, a falta de dinheiro, o subemprego e a péssima condição financeira e social, muitas vezes em condições de miséria e doença, acabam transformando o adulto sem documento num cidadão pouco autônomo e com baixa capacidade de inserção no mundo do trabalho. É o resultado de uma cidadania construída na negação de direitos ou no acesso marginal a eles, e uma cidadania passiva, paciente, forjada na síndrome do balcão, e que não tem pressa para assegurar direitos alheios (ESCÓSSIA, 2019, p.82).

Os usuários do serviço público gratuito de emissão de certidão observados por Escóssia (2019) tinham diferentes motivações para buscar o registro de nascimento, que podiam ser múltiplas para uma mesma pessoa. Um motivo frequente era o acesso a políticas públicas e benefícios sociais, principalmente o Bolsa Família, que exigia, quando ativo, certidão de nascimento, documento de identidade e CPF dos beneficiários, inclusive das crianças na família. Outro motivo era um evento que obrigasse a ter o documento de maneira urgente, como era o caso de Maria, uma usuária do serviço que tinha um tumor maligno no peito que só poderia ser operado e tratado se ela apresentasse seus documentos. O terceiro motivo foi chamado pela autora de conversão: quando pessoas possuíam uma trajetória de vida de uso abusivo de álcool e drogas e não tinham documentos ou os tinham perdido e, como parte das alterações em suas vidas, durante o tratamento do abuso, desejavam recuperar ou tirar pela primeira vez seus documentos. Por fim, havia pessoas que estavam atrás de um sentimento mais intangível de conhecer suas origens e seu histórico familiar a partir do documento (ESCÓSSIA, 2019)[30].

O acesso ao gov.br só se dá por um login que depende do cadastro do cidadão na BDICN, ou seja, uma pessoa sem documento de identidade não acessa os serviços públicos disponíveis no gov.br, gerando uma exclusão de parte da população. Uma possível adequação para evitar exclusão seria uma entrada sem login para acesso às informações dos serviços disponíveis, combinada com a disponibilização de informações sobre como o cidadão pode agir se não está cadastrado na ICN ou se não possui documentos de identificação civil.

b. Documento de identidade inadequado

Além de não possuir documento de identidade, há também um risco de exclusão no acesso a serviços públicos via gov.br de cidadãos cujo documento está em desacordo com sua identidade de gênero, realidade de muitas pessoas transgêneros no Brasil. Vale ressaltar, trata-se de população extremamente vulnerabilizada em nível nacional: o Brasil é o país com o maior número de assassinatos de pessoas trans no mundo (LOPEZ, 2020; SUDRÉ, 2020). Quando o documento está em desacordo com a identidade de gênero, a pessoa será discriminada no acesso aos serviços públicos, uma vez que terá que utilizar seu nome de registro, o que pode até mesmo levá-la a evitar buscar tal acesso.

30 Um dos méritos do trabalho de Escóssia é dar voz e vida ao que normalmente vemos como números, tal como sub-registro. A vida de pessoas sem documento de identidade é vulnerável perante o Estado. Em diário feito pela Revista Piauí (LIMA, 2022), conta-se a história de Maria Cristina de Oliveira, natural de Miguel Alves, PI. Entre janeiro e fevereiro de 2022, Maria passou trinta dias na Maternidade do hospital municipal Promorar, após ter dado à luz, porque não tinha documentos, não era registrada, e o hospital negou sua alta, apesar da inexistência de qualquer previsão legal nesse sentido.

Existem duas maneiras de uma pessoa transgênero ter documentos em conformidade com a sua identidade de gênero: uma delas é a alteração pela via administrativa, em cartório de registro civil, permitida a partir dos 18 anos e realizada de forma paga. Após a alteração na certidão de nascimento, cabe à pessoa comparecer à Receita Federal, para alteração das informações no CPF, e em cada órgão público emissor de outros documentos pessoais. A outra é a utilização do nome social no documento ou no cadastro em cada órgão público que possibilite. A importância do nome social para preenchimento de fichas e cadastros fica clara conforme Mapeamento das Pessoas Trans Realizado no Município de São Paulo, o qual indica que a taxa de utilização do nome social no preenchimento de cadastros e fichas é de 83% entre as mulheres trans, 80% entre as travestis e 72% entre os homens trans (CEDEC, 2021). roblemas com o campo de nome social, com consequências discriminatórias para os direitos das pessoas trans, já ocorreram com cadastros digitais do governo, como o Cadsus, em janeiro de 2022 (DAMASCENO, 2022).

O nome social é relevante também para crianças e adolescentes transgêneros, para os quais a retificação do registro só é possível judicialmente. Em pesquisa conduzida pela ONG Caribou Digital (2020), foi identificado o conflito entre a definição das próprias identidades de gênero por crianças e jovens no Brasil e a identidade estática definida no seu nascimento, a qual, via de regra, será a registrada na BDICN.

No caso das pessoas transgênero, portanto, há um risco maior de que os dados contidos na ICN não correspondam à sua identidade de gênero, seja porque a pessoa ainda não realizou a retificação, ou porque a retificação ainda não consta das bases de dados utilizadas pela ICN. Há também um risco de conflito de dados, por exemplo entre uma pessoa com a certidão de nascimento já com nome retificado, mas sem essa retificação no banco de dados da justiça eleitoral. Seria necessário, portanto, uma política própria para garantir a preservação da qualidade dos dados de acordo com a identidade de gênero de cada indivíduo desse grupo especialmente vulnerável de forma a não haver discriminação, e com facilitação da retificação dos dados junto à BDICN.

4.2. A exclusão de sujeitos hipervulneráveis: crianças e adolescentes, pessoas com deficiência e idosos

a. Crianças e adolescentes

A Constituição Federal, em seu art. 227, e o Estatuto da Criança e do Adolescente, em seu art. 4º, parágrafo único, alínea (c), garantem a absoluta prioridade das crianças no acesso a direitos por meio de políticas públicas. Em paralelo, o Comentário Geral 25 do Comitê dos

Direitos da Criança da ONU sobre os Direitos da Criança[31] em relação ao ambiente digital estabelece que os Estados devem promover o uso de sistemas de identificação digital que incluam o registro de nascimento de todas as crianças recém-nascidas. Também determina que os Estados assegurem o reconhecimento desses registros pelas autoridades nacionais, de modo a garantir o acesso das crianças a serviços, como educação e bem-estar social, considerando a falta de registro como facilitadora da violação de direitos (conforme já endereçado na seção do subregistro, 4.1.a.).

Apesar dessas previsões legais, duas das principais bases de dados da ICN - a base de dados da Justiça Eleitoral e dos Departamentos Estaduais de Trânsito - não contemplam crianças nem a grande maioria dos adolescentes brasileiros: podem estar no banco de dados da Justiça Eleitoral apenas adolescentes com mais de 16 anos, e no do Detran, com 18 anos. Na Lei da ICN, por sua vez, não existe nenhum artigo que esteja direcionado às crianças e adolescentes especificamente.

As crianças e adolescentes devem ser respeitadas e ter acesso a direitos conforme seu estágio de desenvolvimento, também devendo ser contempladas pelo acesso a serviços públicos através do gov.br, de maneira adequada a sua faixa etária. É evidente que qualquer operação de dados de sujeitos com menos de 18 anos deverá ser estruturada de maneira diferenciada e pautada pela vulnerabilidade específica e presumida desse grupo e pelas proteções constitucionais e legais a ele garantidas, mas é importante que, como cidadãos, eles estejam abrangidas pela Identificação Civil Nacional.

b. Idosos

O art. 3º do Estatuto do Idoso garante aos idosos (pessoas com mais de 60 anos) absoluta prioridade no acesso aos direitos, sendo a proteção do envelhecimento um direito social.

Conforme pesquisa realizada pelo Sesc São Paulo e pela Fundação Perseu Abramo, em 2020, os idosos, de modo geral, se sentem excluídos do mundo digital e têm dificuldade em ler. Ao levantamento, 40% dos idosos relataram ter algum tipo de dificuldade em ler e escrever, seja pela falta de escolaridade básica, analfabetismo ou analfabetismo funcional. Ainda, apenas 19% indicou fazer uso efetivo da Internet, sendo que 72% dessa população disse nunca ter utilizado um aplicativo e 62% nunca ter utilizado redes sociais

31 Para a ONU, conforme a Convenção sobre os Direitos da Criança, são consideradas crianças os indivíduos com menos de 18 anos. De acordo com o Estatuto da Criança e do Adolescente, vigente no Brasil, crianças são indivíduos com até doze anos de idades incompletos e adolescentes aqueles dos doze aos dezoito anos de idade.

(BOCCHINI, 2020)[32].

Tanto pela dificuldade com a leitura, quanto com o uso da Internet, grande parte da população idosa fica potencialmente excluída do uso do gov.br e, consequentemente, do acesso a serviços públicos. É recomendável, portanto, uma política específica pensada para que esse segmento da população tenha adequado acesso e manejo dos serviços públicos plataformizados e que seja incluído digitalmente de maneira efetiva.

c. Pessoas com deficiência

Os direitos das pessoas com deficiência têm previsão em diploma específico: o Estatuto da Pessoa com Deficiência (Lei nº 13.146/2015), cujo objetivo é "assegurar e promover, em condições de igualdade, o exercício dos direitos e das liberdades fundamentais por pessoa com deficiência, visando à sua inclusão social e cidadania" (BRASIL, 2015).

A plataforma gov.br dispõe de dois mecanismos de acessibilidade: alto contraste e versão em libras. Entretanto, nem todas as tecnologias de autenticação utilizadas na plataforma são necessariamente acessíveis a todos os públicos. Já foi reportado, por exemplo, que usuários com deficiência visual têm maior dificuldade com ferramentas de reconhecimento facial e, em alguns casos, para operacionalizá-las, necessitam de auxílio por ferramentas como vibração no aparelho ou comando de voz, além de um desenho específico do algoritmo para contemplá-los (KEANE, 2016).

Outro problema que pode surgir para pessoas com deficiência é relativo ao uso da biometria, que prevê o registro das impressões digitais. Os aparelhos para captação e leitura de biometria são construídos de forma a presumir um corpo modelo - o qual não existe - e têm limitações de tamanho e posição dos scanners, de modo que pessoas com deficiência nos membros superiores podem ter dificuldades para ter suas digitais captadas.

A LICN, por outro lado, não tem artigos específicos que tratem das pessoas com deficiência ou sobre como garantir sua inclusão na base de dados de maneira igualitária. Tampouco parece a estrutura da plataforma gov.br incorporar tal tipo de preocupação. Assim, o uso da BDICN para o acesso a serviços públicos por meio do gov.br gera um risco de discriminação e exclusão a pessoas com deficiência.

32 Pesquisa realizada com 2.369 pessoas com mais de 60 anos, nas cinco regiões do país, com margem de erro de até 2,5 pontos percentuais.

4.3. Exclusão por falta de acesso à Internet ou dificuldades de acesso à Internet

Outra hipótese de exclusão decorrente da atual estruturação dos serviços de autenticação para acesso a serviços públicos via gov.br se dá pela falta de acesso à Internet, situação que impossibilita o cidadão de utilizar o portal, o qual funciona unicamente no formato online, por smartphone ou desktop.

De acordo com a pesquisa TIC Domicílios (2021), em 2020, a proporção de domicílios brasileiros com acesso à Internet chegou a 83% - um crescimento de 12 pontos percentuais em relação ao ano anterior. Esse aumento foi mais acentuado nos estratos socioeconômicos mais vulneráveis, sobretudo entre as classes C (cujo acesso foi de 80%, em 2019, para 91% em 2020) e DE (cujo acesso foi de 50%, em 2019, para 64%, em 2020). Em termos populacionais, estima-se que 81% da população com 10 anos de idade ou mais foi usuário da rede em 2020, um aumento de sete pontos percentuais em relação ao ano anterior, tendo o crescimento maior também sido nos estratos socioeconómicos mais vulneráveis, entre as classes C (de 78% para 85%) e DE (de 57% para 67%) (CETIC.br, 2021).

Esses números representam um avanço bastante relevante para a realidade brasileira, mas ao mesmo tempo demonstram que 19% da população não é usuária da Internet - e, consequentemente, estaria excluída do uso do serviço do gov.br. Ademais, é importante notar que entre as classes D e E, o número de domicílios com Internet é significativamente mais baixo que a média - 67% versus 83% -, o que demonstra que, quanto maior a vulnerabilidade social, maior a chance de não se ter Internet no domicílio e, consequentemente, de se ter uma maior dificuldade de acesso aos serviços públicos digitalizados no gov.br. Existe também uma desigualdade regional de acesso à rede (IDEC, 2022), que implica em uma provável distribuição desproporcional de acesso aos serviços plataformizados: a região Nordeste tem o menor percentual de domicílios com acesso (79%) e a região Sudeste o maior (86%). As demais regiões têm os seguintes percentuais de acesso à Internet por domicílio: Norte (81%), Centro-Oeste (81%), Sul (84%) (CETIC.br, 2021).

Conjuntamente ao relatado aumento dos índices de acesso à Internet dos estratos socioeconômicos mais vulneráveis, houve entre 2019 e 2020 um aumento na proporção dos usuários que procuraram informações oferecidas por websites de governo (de 28% para 42%) e que realizaram algum serviço público pela Internet (de 28% para 37%). No entanto, importante ressaltar como esses números ainda são baixos e englobam uma minoria das pessoas que navegam pela rede. Ainda, cumpre pontuar que a realização dessas atividades online foi mais frequente entre usuários da área urbana (39%), de classe A (63%) e com Ensino Superior (68%), populações que já realizavam uma variedade maior de atividades na Internet (CETIC.br, 2021), o que mostra uma tendência que, em se aplicando ao

gov.br, excluiria os usuários mais vulneráveis do seu uso.

Ainda em matéria de acesso à Internet, em 2020 o telefone celular continuou, como em 2019, sendo o principal dispositivo utilizado por quase o total da população brasileira com 10 anos de idade ou mais que acessa o ambiente digital (99%). Para mais da metade dos usuários que utilizam o celular como principal dispositivo (58%), o acesso se deu exclusivamente pelo aparelho, proporção que cresce a 90% para aqueles que estudaram apenas até a Educação Infantil ou que pertencem às classes DE (CETIC.br, 2021). O uso exclusivo do celular para acesso à Internet também se verificou em maior medida entre os que se autodeclararam pretos ou pardos (65% e 60%, respectivamente) e que residem na região Nordeste (72%) (CETIC.br, 2021), dados que indicam que quanto maior a vulnerabilidade social, maior o uso exclusivo do celular para acesso à Internet.

Em paralelo a tais taxas, pesquisa realizada pelo Instituto Brasileiro de Defesa do Consumidor - Idec e Instituto Locomotiva (2021) retratou o acesso à Internet dos estratos socioeconômicos CDE. Os dados obtidos confirmam que a maioria das pessoas utilizava o celular para acessar a Internet (91%) e indicam também o uso majoritário da rede de Internet do próprio celular - 3G/4G (90%). Diante desses números, e em relação ao acesso a serviços eletrônicos do governo, a pesquisa constatou que 39% não tiveram acesso a políticas públicas pela falta de Internet em seu smartphone, 33% não tinham acessado serviços públicos e 28% não tinham acessado benefícios assistenciais, como o auxílio emergencial. Isso se relaciona diretamente ao dado de que, em média, os indivíduos entrevistados tiveram acesso à Internet apenas durante 23 dias no mês anterior, sendo que, no restante do tempo, tiveram a Internet bloqueada por falta de pagamento para uso adicional.

O que todas essas taxas atestam é uma maior vulnerabilidade dos estratos socioeconômicos CDE no que diz respeito ao acesso ao ambiente digital. Mesmo superando a barreira do acesso à Internet, os cidadãos não necessariamente conseguirão utilizar dispositivos adequados para uma navegação proveitosa ou conseguirão arcar com uma conexão constante, de modo que seu uso de serviços de governo digital é dificultado. É dizer, o acesso ao gov.br aparece por detrás de maiores barreiras para as pessoas mais vulneráveis socialmente, o que pode resultar em sua exclusão dos serviços públicos contidos na plataforma. A fim de mitigar tal exclusão, duas medidas são simultaneamente recomendadas: (i) primeiro, é necessário que sejam mantidos canais físicos para o cadastro e acesso aos serviços públicos, com qualidade no mínimo igual ao atendimento pelo meio digital; e, (ii) segundo, deve haver maior investimento em políticas públicas para universalização do acesso à Internet, de forma plena e com qualidade.

5. Endereçando os riscos a direitos fundamentais e liberdades civis: medidas de *accountability* e o Relatório de Impacto à Proteção de Dados

5.1. A "risquificação"[33] da proteção de dados pessoais

Os capítulos anteriores deste relatório trataram de delinear algumas implicações da atual estrutura informacional e de governança da Identificação Civil Nacional, bem como os riscos decorrentes da utilização da ICN para autenticação de usuários no gov.br para o acesso a serviços públicos federais prestados por meio da plataforma.

Nesse sentido, o elemento risco assume um papel fundamental para a análise realizada ao longo deste documento, sendo necessário, portanto, compreendê-lo em sua estrutura. Segundo Raphaël Gellert (2016), a noção de risco pode ser apreendida a partir de duas definições: (i) a sua definição literal; e (ii) a sua concepção técnica.

Em uma perspectiva literal, o risco pode ser compreendido como a possibilidade de um perigo futuro.

A concepção técnica, por sua vez, compreende o risco a partir de um duplo ponto de vista: a sua utilização para o processo de tomada de decisão, baseado na avaliação de eventos futuros. Logo, Gellert (2016) argumenta que o risco é constituído de dois elementos distintos, mas que são conjuntamente operacionalizados: a previsão de eventos futuros, sejam eles positivos ou negativos, e a tomada de decisão com base nessa previsão. A partir desse olhar, as leis de proteção de dados pessoais podem ser compreendidas enquanto uma de várias ferramentas para a governança de riscos decorrentes de Tecnologias da Informação e Comunicação (TICs) (GELLERT, 2015).

Na mesma esteira, Claudia Quelle (2015) aponta, justamente, que as últimas gerações de leis de proteção de dados pessoais internalizaram mais ainda uma abordagem baseada no risco, sendo ele o elemento que calibra as obrigações legais, de modo que o peso da regulação será correspondente ao seu grau de adversidade (QUELLE, 2015).

33 O conceito de risquificação da proteção de dados pessoais foi cunhado, pela primeira vez, pelo autor Alessandro Spina no artigo "A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics", publicado no European Journal of Risk Regulation, em 2017 (SPINA, 2017).

A partir dessas premissas, segundo Rafael Zanatta (2017, p. 9), o processo de "risquificação" da proteção de dados pessoais faz com que a matéria passe a ser constituída pelos seguintes elementos:

> (i) instrumentos de tutela coletiva e participação de entidades civis no diálogo preventivo com autoridades independentes de proteção de dados pessoais, (ii) obrigações e instrumentos de regulação ex ante atribuídas aos controladores para identificação de riscos a direitos e liberdades fundamentais, (iii) disseminação de metodologias de "gestão de risco" e calibragem entre riscos gerados pelo tratamento e uso de dados pessoais e imunidades jurídicas construídas pela discussão ética sobre os limites do progresso técnico.

Este processo de risquificação torna-se relevante na medida em que é retomado o debate sobre a precaução aplicada à disciplina da proteção de dados pessoais, superando-se uma abordagem centrada unicamente nos mecanismos regulatórios voltados para a punição e reparação (*ex post*) quando da ocorrência de um dano. No contexto brasileiro de proteção de dados pessoais, o debate sobre precauções e medidas regulatórias ex ante é materializado pelo princípio da responsabilização e prestação de contas[34] - ou *accountability*[35]. Conforme o art. 6º, inciso X da Lei Geral de Proteção de Dados, o referido princípio pode ser compreendido como a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (BRASIL, 2018). A esse respeito, Bruno Bioni e Maria Luciano afirmam que:

> o princípio da precaução apresenta dois vetores de regulação que merecem atenção: a) a abertura do debate regulatório a todos os atores envolvidos na implementação dessa tecnologia (e nas escolhas que ela impõe), de desenvolvedores àqueles que sofrerão seus possíveis efeitos, o que é um requisito obrigatório de um sistema democrático com históricas dinâmicas de assimetria de poder e informação; b) a atribuição de obrigações que reduzam as incer-

34 Para os fins deste documento, as expressões "*accountability*" e "responsabilização e prestação de contas" serão utilizadas de forma intercambiável e como sinônimos.

35 Segundo a Information Commissioner's Office (ICO), *accountability* é um dos princípios de proteção de dados pessoais, o qual versa sobre a responsabilidade de determinada organização estar em conformidade com a legislação de proteção de dados pessoais, bem como sobre a capacidade de demonstrar tal adequação à legislação. Ver mais em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability--and-governance/#whataccountability

> tezas quantos aos benefícios e riscos em questão (...).
>
> Nesse sentido, leis gerais de proteção de dados pessoais (..) apresentam um ferramental precaucionário a ser analisado. A sua calibração variará a escala em baixa, moderada e alta quanto ao nível de prudência (...). Ao contrário de paralisia ou inação, a execução de relatórios de impacto à proteção de dados pessoais, de mecanismos de auditoria e conversas com os órgãos reguladores e outros atores afetados são ações que podem servir de força motriz consciente e responsável para o lançamento dessa tecnologia no meio ambiente (BIONI, LUCIANO, 2019, p. 19, grifo nosso)

Nesse cenário, as avaliações de impacto à proteção de dados pessoais - também chamadas relatório de impacto à proteção de dados pessoais (RIPD) -, como se vê, desponta como uma das principais ferramentas precaucionárias, de regulação *ex ante* e prestação de contas para o desenvolvimento de políticas e atividades que envolvem o tratamento de dados pessoais.

5.2. Uma "teoria geral" das Avaliações de Impacto à Proteção de Dados[36]

As avaliações de impacto não são instrumentos de governança novos. Surgiram a partir da necessidade de se conferir certo grau de certeza a eventos incertos, decorrentes da emergência de novos perigos para a sociedade em níveis individuais e coletivos (KLOZA *et al*, 2020)[37]. É dizer, as avaliações de impacto, segundo Kloza *et al* (2020, p. 2), são ferramentas usadas com intuito de analisar as:

> possíveis consequências de uma iniciativa sobre um interesse ou interesses sociais relevantes, se essa iniciativa puder apresentar perigos a esses interesses. Essa ferramenta tem o objetivo de apoiar o processo decisório informado sobre se se deve começar a iniciativa e sob quais condições, acabando por se traduzir num meio de proteção dos referidos interesses sociais.

36 Vale dizer, de antemão, que as Avaliações de Impacto à Proteção de Dados Pessoais são os instrumentos europeus equivalentes ao relatório de impacto à proteção de dados pessoais, estabelecido pela Lei Geral de Proteção de Dados Pessoais.

37 Destaca-se que este artigo foi originalmente publicado no ano de 2017, e a sua tradução para o português, feita pela Associação Data Privacy Brasil de Pesquisa, foi publicada em 2020. Tal tradução foi resultado de uma parceria entre o Data Privacy Brasil e o d.pia.lab – o Laboratório de Bruxelas sobre Avaliações de Impacto à Proteção de Dados e à Privacidade, vinculado à Universidade Livre de Bruxelas.

Conforme Kloza *et al* (2020), o desenvolvimento de avaliações de impacto em áreas como a de saúde, regulação e privacidade e proteção de dados pessoais se deu em razão de experiências positivas na condução dessas documentações em outras áreas, tais como a ambiental.

Em termos da proteção de dados pessoais, a disseminação de Avaliações de Impacto à Privacidade (AIP) – precursora das Avaliações de Impacto à Proteção de Dados Pessoais ou, como são chamadas no Brasil, relatório de impacto à proteção de dados pessoais (RIPD) – e avaliações de impacto à proteção de dados (AIPDs), a partir dos anos 1990, pode ser relacionada a três fatores:

> (1) o caráter crescentemente invasivo de tecnologias emergentes sobre as vidas dos indivíduos e sobre o tecido social; (2) a crescente importância do tratamento de dados pessoais para a economia contemporânea, segurança nacional, pesquisa científica, desenvolvimento tecnológico, relações interpessoais, dentre outros, e (3) a diminuição da confiança em tecnologias emergentes e a sua utilização por entidades públicas e privadas (KLOZA *et al*, 2020, p. 2)

Nesse sentido, Clarke (2009), ao tratar das Avaliações de Impacto à Privacidade, salienta que as AIPs - e o mesmo vale para os RIPDs - se distinguem de outras atividades organizacionais como as atividades de conformidade com legislações de proteção de dados, sobretudo em razão de seu caráter *ex ante*, isto é, devido ao fato de serem conduzidas previamente ao início da atividade de tratamento de dados.

Sendo assim, o autor estabelece alguns elementos fundamentais para a caracterização das Avaliações de Impacto à Privacidade, dos quais destacam-se os seguintes: (i) as AIPs devem ser conduzidas tendo por escopo um projeto ou iniciativa, diferindo de uma estratégia organizacional de privacidade; (ii) a natureza das AIPs é antecipatória, uma vez que devem ser conduzidas previamente ou em paralelo ao desenvolvimento de determinada atividade; (iii) as avaliações de impacto à privacidade possuem um amplo escopo, que deve levar em consideração os sujeitos afetados por determinada atividade de tratamento de dados; (iv) as AIPs devem endereçar tanto os problemas (riscos) da atividade quanto as soluções para tais problemas; e (v) as AIPs consistem em um processo que requer engajamento intelectual de toda a organização.

Em diálogo com o que dispõe Clarke (2009), Kloza *et al* (2020), afirmam que a condução de uma avaliação de impacto – e, no contexto deste relatório, uma avaliação de impacto à proteção de dados pessoais – possui vantagens de duas ordens: o auxílio no processo de

tomada de decisões informadas, com base na avaliação de risco, e a proteção de interesses sociais.

No que diz respeito à primeira vantagem, é possível ver o deslocamento da racionalidade regulatória para um pensamento antecipado (*ex ante*). Tal deslocamento, segundo Kloza *et al* (2017), atrai organizações tanto do setor público, como do setor privado, que passam a refletir sobre as consequências decorrentes da implementação de determinada atividade de tratamento de dados. Esse processo de reflexão resulta em um aumento da confiança pública, uma vez que se passa a ter uma busca ativa por meios de minimizar e, até mesmo, evitar consequências negativas das operações que serão realizadas (KLOZA *et al*, 2020).

Além disso, ainda na esteira da primeira vantagem, Kloza *et al* (2020) destacam que a condução de avaliações de impacto à proteção de dados pessoais auxiliaria no processo de conformidade – apesar de não se confundir com este - e de demonstração de *accountability* diante de agentes regulatórios.

Sobre a vantagem relacionada à proteção de interesses sociais, as avaliações de impacto à proteção de dados pessoais auxiliam na proteção, em nível individual e coletivo, de interesses socialmente relevantes, como os direitos humanos. Afinal, seu intuito é justamente mapear e prever medidas para mitigar interferências negativas de atividades de tratamento de dados nos direitos dos titulares de dados. Nesse sentido, as avaliações de impacto à proteção de dados pessoais podem auxiliar no fortalecimento da justiça procedimental, cujos pilares vão ao encontro do próprio conceito das avaliações e consistem em: participação (voz), neutralidade, respeito e confiança (TYLER, 2008, pp. 30–31 apud KLOZA, 2014, p. 4).

A compatibilidade entre esses pilares e a natureza das documentações ex ante aqui abordadas é mais facilmente verificável com relação ao princípio da participação. Significa dizer que, ao permitirem que os indivíduos vocalizem "suas preocupações (e.g. por meio de participação social)" (KLOZA *et al*, 2020, p. 3), as AIPDs teriam o potencial de fortalecer a ideia de justiça procedimental, uma vez que o princípio da participação seria atendido (KLOZA, 2014).

Outro ponto crucial nessa seara é a compreensão de que a avaliação de impacto à proteção de dados pessoais parte da noção de que o direito à proteção de dados pessoais é autônomo frente ao direito à privacidade. Tal autonomia ficou evidente quando da promulgação do Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD). É possível identificar, em tal regulamento, a previsão expressa da avaliação de impacto à proteção de dados pessoais, que em seu art. 35º estabelece:

> 1 - Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, **for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares**, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que [sic] apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. (UNIÃO EUROPEIA, 2018, p. 53, grifo nosso).

O Regulamento Geral sobre Proteção de Dados Pessoais, como se vê, vincula a condução de uma AIPD à existência de risco elevado para os direitos civis e liberdades fundamentais dos titulares de dados, conforme as disposições do art. 35, nº 1, colocando-os como o foco para o qual a avaliação de impacto deve se direcionar. É, portanto, o elevado grau de risco da atividade o gatilho para que se conduza uma avaliação de impacto à proteção de dados pessoais.

Para além de vincular a condução de uma AIPD à existência de uma operação de tratamento de dados que for suscetível de implicar elevado risco aos titulares, o RGPD estabelece algumas situações, de modo não exaustivo, em que é obrigatória a condução de uma avaliação de impacto:

> 3 - a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
> b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, nº 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º[38]; ou
> c) Controlo sistemático de zonas acessíveis ao público em grande escala. (UNIÃO EUROPEIA, 2018, p. 53).

38 Segundo o art. 9º (1) Regulamento Geral sobre Proteção de Dados Pessoais da União Europeia, são categorias de dados especiais: aqueles que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical; os dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa

Em paralelo a tais situações, o Grupo de Trabalho do Artigo 29 para Proteção de Dados publicou as "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é suscetível de resultar num elevado risco para efeitos do Regulamento (UE) 2016/679". A publicação se deu em 2017, antes da entrada em vigor do Regulamento Europeu sobre Proteção de Dados Pessoais, - mas após sua aprovação -, e as orientações pretendem dirimir a subjetividade da noção de "*risco elevado*".

Segundo tais orientações, a condução de uma AIPD é especialmente importante quando há a implementação de uma nova tecnologia de tratamento de dados. O texto recomenda, ainda, a condução de uma AIPD mesmo em situações nas quais não fica evidente se há sua obrigatoriedade, tendo em vista que tais avaliações são instrumentos fundamentais para auxiliar os agentes de tratamento no cumprimento da legislação de proteção de dados (GRUPO DE TRABALHO DO ARTIGO 29 PARA PROTEÇÃO DE DADOS, 2017).

O documento destaca, ademais, o fato de o RGPD apresentar uma lista não exaustiva de atividades que podem ensejar um tratamento de dados de elevado risco, de modo que podem existir outros tipos de atividades que nessa categoria se enquadrem. É dizer, o Regulamento faculta às Autoridades Nacionais de Proteção de Dados a elaboração de listas que contenham operações de tratamentos que podem implicar um alto risco aos direitos e liberdades dos titulares de dados. Tais listas, segundo as orientações do Grupo de Trabalho do Artigo 29 (2017, p. 10-12), devem observar nove critérios, alguns deles já compreendidos no art. 35, nº 3, dos quais destaca-se: (i) quando houver decisões automatizadas que produzam efeitos jurídicos ou afetem de modo similar a pessoa singular; (ii) quando houver a existência de dados sensíveis de natureza altamente pessoal; (iii) quando houver tratamento de dados relativos a titulares vulneráveis, que podem incluir crianças, empregados, segmentos mais vulneráveis da população que necessitem de proteção especial e todos aqueles casos em que seja possível ser identificado um desequilíbrio entre a posição do titular de dados e o agente de tratamento; e (iv) quando o tratamento de dados impedir os titulares de dados de exercer um direito ou de utilizar um serviço ou contrato.

5.3. O Relatório de Impacto à Proteção de Dados Pessoais no Brasil

As avaliações de impacto não são instrumentos estranhos ao ordenamento jurídico brasileiro, uma vez que possuem previsão legal tanto no art. 225, inciso IV da Constituição Federal, quanto no art. 6º da Lei das Agências Reguladoras (Lei 13.848/2019) (BIONI, RIELLI, 2020). Com a aprovação da Lei Geral de Proteção de Dados, em 2018, o Brasil passou a contar, finalmente, com a previsão legal de um instrumento semelhante à avaliação de impacto à proteção de dados pessoais: o relatório de impacto à proteção de

dados pessoais (RIPD). Assim como a ferramenta europeia, o RIPD é conceituado, segundo o art. 5º, inciso XVII, da LGPD como:

> documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. (BRASIL, 2018)

Em consonância ao que aqui se chamou de uma "teoria geral" das avaliações de impacto à proteção de dados, o RIPD tem por objetivo ser uma ferramenta capaz de mitigar os riscos aos direitos fundamentais e liberdades civis dos titulares de dados. Segundo Gomes (2019), a partir da definição de relatório de impacto presente no art. 5º, inciso XVII da LGPD, é possível identificar duas espécies de riscos que devem ser abarcadas pelo instrumento: (i) os riscos às liberdades civis; e (ii) os riscos aos direitos fundamentais. Aqui, considera-se como direitos fundamentais aqueles que estão dispostos no art. 5º da Constituição Federal, e como liberdades civis as liberdades religiosa, de expressão, de pensamento e de associação (GOMES, 2019).

Segundo Bioni e Rielli (2020), apesar de a legislação brasileira de proteção de dados pessoais estabelecer alguns esclarecimentos sobre o RIPD, estes não são suficientes. Segundo os autores (2020, p. 35), além "de menções à possibilidade de sua elaboração ou requisição pela Autoridade (e.g. art. 4º, §3º; 10, §3º e 32), a única disposição um pouco mais robusta sobre esse instrumento surge no art. 38 (...)", cujo parágrafo primeiro dispõe sobre o conteúdo mínimo de um relatório de impacto à proteção de dados pessoais.
Para além dos dispositivos acima mencionados, a LGPD não estabeleceu uma procedimentalização mínima sobre a condução do RIPD, tanto no que diz respeito ao que corresponde à noção de risco, elemento disparador da condução de um RIPD (GOMES, 2020; BIONI, RIELLI, 2020, p. 34), quanto no que tange aos elementos relativos a qual metodologia deveria ser utilizada para a condução de tal relatório.

Apesar de o objetivo deste *policy paper* não estar diretamente relacionado a discussões acerca de metodologias para elaboração de relatórios de impacto à proteção de dados, não se pode deixar de pontuar sua importância. Gomes (2020), nessa seara, aponta para o fato de que a utilização de metodologias para a condução de um relatório de impacto é tão importante quanto o próprio relatório. Existem, inclusive, diversas possibilidades metodológicas para a elaboração de um RIPD, como por exemplo a metodologia de custo-benefício. No entanto, como aponta Gomes (2020, p. 17), "qualquer metodologia que seja aplicada precisa de fundamentação e referencial".

A autora ainda aponta que, no que diz respeito às metodologias para elaboração de RIPDs, o essencial é compreender que "(...) o referencial dessa metodologia é o próprio titular dos dados, de modo que o produto final seja, de fato, uma documentação que mensura os riscos às liberdades civis e aos direitos fundamentais dos titulares". (GOMES, 2020, p. 17)

Nesse ponto, vale ressaltar a Ação Direta de Inconstitucionalidade (ADI) 6387[39]. Tal ação, proposta pelo Conselho Federal da OAB, visava a declaração de inconstitucionalidade da Medida Provisória (MP) nº 954/2020, a qual autorizava a "obtenção de dados pessoais de consumidores de serviços de telecomunicação (telefones fixos e celulares)" (BIONI, 2021, p. 102) para viabilizar a Pesquisa Nacional por Amostragem de Domicílios (PNAD), feita pelo Instituto Brasileiro de Geografia e Estatística (IBGE). Em sede de apreciação da ADI, a Ministra Rosa Weber, ao proferir decisão sobre pedido de Medida Cautelar, destacou o caráter antecipatório do relatório de impacto à proteção de dados - o qual nomeou de relatório de impacto de segurança da informação -, reforçando que ele deve ser conduzido antes do início da operação de tratamento de dados.

Considerando o contexto normativo brasileiro, Gomes (2020) compreende que a Autoridade Nacional de Proteção de Dados Pessoais assumirá um importante papel na regulamentação do RIPD, a partir da emissão de orientações sobre o tema. A ANPD, nos termos do art. 57-J da Lei Geral de Proteção de Dados Pessoais e de acordo com as suas competências estabelecidas pelo Decreto nº 10.474 de 2020, tornou pública a sua agenda regulatória para o biênio 2021-2022, por meio da Portaria nº 11 de janeiro de 2021 (ANPD, 2021), e, justamente, estabeleceu o relatório de impacto à proteção de dados pessoais entre suas prioridades temáticas para o período.

O início da primeira fase de seu processo regulatório estava datado para o primeiro semestre de 2021 e, até o momento de finalização deste documento, em maio de 2022, a Autoridade sediou reuniões técnicas para tomada de subsídios sobre o tema. Assuntos relevantes à disciplina do RIPD foram abordados nas reuniões técnicas, que contaram com a participação de especialistas, tais como a necessidade de o RIPD ser conduzido segundo uma abordagem metodológica sólida (GARROTE *et al*, 2021).

Apesar de o processo de regulamentação do RIPD ainda não ter sido finalizado no Brasil, a Autoridade Nacional de Proteção de Dados, ao se debruçar sobre a aplicação da Lei Geral de Proteção de Dados para agentes de pequeno porte (Resolução Cd/ANPD nº 2 de

39 Segundo Bioni (2021), esse julgamento foi responsável por uma mudança paradigmática na jurisprudência do Supremo Tribunal Federal (STF), uma vez que reconheceu o direito à proteção de dados pessoais como um direito autônomo, enquadrando-o como um novo direito fundamental.

2022), iniciou o delineamento sobre o que deve se compreender como atividades de tratamento de dados de alto de risco aos titulares de dados (ANPD, 2022). Segundo o art. 4º da Resolução, é considerado tratamento de alto risco aquele que atender, cumulativamente, a pelo menos um dos critérios gerais e um dos critérios específicos estabelecidos, conforme vê-se abaixo:

> Art. 4º Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:
>
> I - critérios gerais:
>
> a) **tratamento de dados pessoais em larga escala; ou**
> b) **tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;**
>
> II - critérios específicos:
>
> a) uso de tecnologias emergentes ou inovadoras;
> b) vigilância ou controle de zonas acessíveis ao público;
> c) **decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular;** ou
> d) **utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.**
>
> § 1º O tratamento de dados pessoais em larga escala será caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.
>
> § 2º O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade. (ANPD, 2022, sem paginação, grifo nosso).

Ademais, o Guia Orientativo Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral, de autoria da ANPD e do TSE, dispõe que RIPD é um instrumento importante de *accountability* no contexto eleitoral, uma vez que nele pode haver o tratamento de grande volume de dados sensíveis, como opiniões e filiações políticas. Ainda, de acordo com o guia, não obstante a LGPD não discipline os contextos em que a elaboração do RIPD é obrigatória, ela é altamente recomendável em cenários de alto risco, sendo exemplo de tal cenário os que envolvem tratamento de dados sensíveis e em larga escala.

De acordo com esses indicativos da compreensão da ANPD acerca do tema, a operação de dados envolvida nas políticas públicas da ICN e do gov.br atrai quatro dos seis elementos listados para caracterizá-la como uma atividade de alto risco, do ponto de vista geral e específico:

Critérios Gerais (Art. 4º, inciso I, da Resolução Cd/ ANPD nº 2 de 2022)	**ICN e Gov.br** (Atividade de Tratamento de Dados de Alto Risco)
Tratamento de dados pessoais em larga escala será caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado (Art. 4º, I, "a", § 1º)	A ICN é uma política de Estado que visa combater a subidentificação de cidadãos brasileiros, considerados invisíveis ao Estado. Segundo informações disponibilizadas pelo portal do Tribunal Superior Eleitoral (TSE) atualizadas em 17 de maio de 2022, existem mais de 118 milhões de pessoas que possuem a identificação biométrica registrada junto ao órgão, o que corresponde a cerca de 80% do eleitorado brasileiro (TSE, 2022b). O gov.br, por sua vez, por meio da digitalização, pretende ampliar o acesso a serviços públicos. Segundo dados do governo federal, a plataforma gov.br possuía 57 milhões de usuários únicos em fevereiro de 2022 (GOVERNO FEDERAL, 2022)[40].
Tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares, que será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade (Art. 4º, I, "b", § 2º)	A finalidade do tratamento de dados consiste em identificar o cidadão para a fruição de uma série de direitos no contexto da sua relação com o Estado. Em resumo, o tratamento de dados em questão impacta significativamente os atos da vida civil do titular dos dados nas mais diferentes esferas e contextos, bem como seu acesso a serviços públicos.

40 Estes mesmos dados apontam que houve um aumento de 19% no número total de usuários únicos em relação ao mês de janeiro de 2022.

As atividades de tratamento de dados nas políticas da ICN e do gov.br atraem os 02 (dois) critérios gerais para caracterizá-las enquanto uma atividade de alto risco	
Critérios Específicos (Art. 4º, inciso I, da Resolução Cd/ ANPD nº 2 de 2022)	**ICN e Gov.br** (Atividade de Tratamento de Dados de Alto Risco)
Decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular (Art. 4º, II, "c")	O processo de identificação do cidadão envolve necessariamente o uso de dados biográficos e biométricos - aspectos da personalidade do titular - para singularizá-lo. Ainda, de modo a viabilizar o tratamento de dados de larga escala em questão, há um grau de automatização substancial no fluxo informacional da ICN, bem como previsão na LICN sobre cruzamento de dados de cidadãos com intuito de verificar o cumprimento de requisitos necessários ao acesso a benefícios sociais.
Utilização de dados pessoais sensíveis (Art. 4º, II, "d")	Há o tratamento de uma série de dados sensíveis, dentre eles destacando-se os biométricos, para que haja a plena individualização do cidadão.
Utilização de dados pessoais de crianças, de adolescentes e de idoso (Art. 4º, II, "c")	Há o tratamento de dados de adolescentes com mais de 16 anos e idosos, considerados hipervulneráveis pelas Leis nº 8.069 de 1990 e º 10.741 de 2003.
As atividades de tratamento de dados nas políticas da ICN e do gov.br atraem todos os três critérios específicos para caracterizá-la enquanto uma atividade de alto risco	

No atual contexto regulatório brasileiro, a ICN e o gov.br já podem ser classificados como atividades de tratamento de dados de alto risco. Em atenção ao princípio da *accountability*, os controladores de tais bases de dados já deveriam ter elaborado relatórios de impacto à proteção de dados para a demonstração da eficácia das ações adotadas para proteção dos dados de grande parte da população brasileira: uma medida de prestação de contas que iria ao encontro da implementação de um sistema de identidade civil nacional e plataformização de serviços públicos que reforça o laço de confiança entre cidadão e Estado.

a. O setor público e a publicização do relatório de impacto à proteção de dados

Como visto anteriormente, trata-se, o RIPD, de documento oriundo de um processo complexo no qual os riscos aos direitos fundamentais e liberdades civis dos titulares de dados decorrentes de determinada atividade de tratamento de dados pessoais são descritos e avaliados. Trata-se, ainda, de um processo no qual são estabelecidas medidas, salvaguardas e mecanismos de mitigação desses riscos, sendo o elevado grau de risco, portanto, o elemento central para engatilhar a condução deste documento.

Considerando o fato de o RIPD ser uma poderosa ferramenta de *accountability* e de garantia de direitos dos titulares de dados, um outro elemento tão relevante quanto sua condução é sua publicização.

Aqui, novamente, a Lei Geral de Proteção de Dados Pessoais é silente, ou seja, não determina diretamente as condições que ensejam a publicização do relatório de impacto, apesar de estabelecer, em seu art. 32, que a Autoridade Nacional de Proteção de Dados poderá solicitar a agentes do poder público a publicação do RIPD. Extrai-se, desse dispositivo, que a publicização do relatório de impacto assume contornos especiais quando a sua condução está atrelada a uma atividade de tratamento de dados executada pelo poder público, como é o caso da Identificação Civil Nacional e do uso da Base de Dados da Identificação Civil Nacional na plataforma gov.br.
Nesse cenário, uma interpretação sistemática das disposições da Lei Geral de Proteção de Dados Pessoais e dos princípios constitucionais da Administração Pública leva à conclusão da existência de uma obrigação geral de publicização de RIPD pelo setor público, uma vez que, conforme tratado no capítulo 3, seção 3.3b, ele tem o dever de tornar públicas as suas atividades de tratamento de dados, especialmente quando há dados sensíveis e quando a base legal escolhida para justificar o tratamento não é o consentimento.

Tal dever decorre, ainda, dos princípios constitucionais que regem a atividade da Administração Pública, especialmente o princípio da publicidade. Segundo Carvalho Filho (2020), o princípio da publicidade indica que os atos da administração pública devem ser públicos, sendo necessária sua ampla divulgação entre os administrados, uma vez que somente com a transparência das atividades da Administração Pública será possível que os indivíduos tenham controle sobre a legitimidade de determinada conduta – no caso aqui em análise, controle sobre as atividades de tratamento de dados pessoais.

A publicidade dos atos da Administração Pública se relaciona, portanto, diretamente com os princípios estabelecidos pela Lei Geral de Proteção de Dados Pessoais, notadamente o princípio da responsabilização e prestação de contas (ou *accountability*), disposto no art. 5º, inciso X da LGPD, na medida em que, ao considerar a assimetria de poder entre o agente de tratamento e o titular de dados, garante que esse último tenha amplo acesso a como as atividades de tratamento de dados são conduzidas, o que inclui o RIPD.

A esse respeito, Gomes (2020) adverte que a publicidade do instrumento está diretamente ligada à necessária visibilidade sobre qual é a metodologia adotada para fins de cognição, avaliação e mitigação dos riscos aos direitos e liberdades fundamentais do titular dos dados. Ou seja, tão ou mais importante que o processo de gerenciamento de riscos em si, é disputá-lo e colocá-lo sob escrutínio público para que o relatório seja um instrumento que

cumpra com as suas aspirações de salvaguardar os direitos fundamentais e liberdades civis dos titulares de dados.

Harris (2020) aponta que o tratamento de dados para o exercício do poder público pode levantar questões em termos dos preceitos que fundamentam o Estado de Direito. Isso ocorre em razão da possibilidade de se reduzir a transparência no funcionamento de determinada política pública, de modo que a transparência assume um papel fundamental para permitir que os cidadãos, titulares de dados, compreendam o funcionamento da atividade de tratamento de dados utilizada na implementação de políticas públicas (HARRIS, 2020). Nesse sentido, a autora destaca que o processo de desenvolvimento de um relatório de impacto torna-se uma oportunidade para a implementação do princípio da publicidade, cujo cumprimento se desdobra em medidas de transparência ativa e passiva dos agentes do poder público, e o princípio da participação pública (HARRIS, 2020).

Ainda, Harris (2020), ao tratar da publicização de relatórios de impacto pelo setor público, afirma que a sua publicação por padrão aumentaria a transparência, prestação de contas e responsabilização (*accountability*) dos agentes públicos de tratamento, na medida em que permitiria a fiscalização da sociedade civil e o amplo debate público sobre tais operações de tratamento de dados, resultando em uma maior relação de confiança entre a Administração Pública e os administrados.

A título de exemplo, vale citar que existem casos de sucesso em que relatórios de impacto à proteção de dados foram conduzidos pelo poder público e a sua publicização resultou em melhorias qualitativas quanto aos riscos existentes em determinadas operações de tratamento de dados. Desde junho de 2019, o governo holandês, por meio da empresa Privacy Company, tem conduzido relatórios de impacto à proteção de dados sobre algumas aplicações oferecidas pela Microsoft e utilizadas em universidades e escolas locais, como Teams, OneDrive, SharePoint e Azure AD, visando identificar os riscos aos titulares de dados. Tais relatórios foram publicizados após suas elaborações, explicitando quais eram os riscos que foram identificados, bem como as fragilidades dessas aplicações. Esse processo levou, posteriormente, a negociações entre o governo holandês e a Microsoft para que a empresa tomasse medidas aptas a mitigar os riscos de grau elevado aos titulares de dados. Tais negociações resultaram no comprometimento da Microsoft em atender às demandas que emergiram da condução do relatório de impacto à proteção de dados pessoais e, consequentemente, em uma maior proteção aos cidadãos holandeses diretamente afetados por tais riscos (PRIVACY COMPANY, 2022).

b. Relatório de Impacto à Proteção de Dados: uma necessária relação entre regulação–governança *ex ante* e *ex post*

Neste documento, tem sido debatido o fato de que as avaliações de impacto e, mais especificamente, o RIPD, cumprem o objetivo de permitir que todos os sujeitos envolvidos e interessados nas operações de tratamento de dados possam entender e influir no processo de tomada de decisão (BIONI *et al*, 2020). Significa dizer, segundo Kloza (2014), que as avaliações de impacto se relacionam com um aspecto de justiça procedimental, uma vez que elas não se resumem apenas à obtenção de um resultado justo, mas de um caminho percorrido até esse resultado que também o seja.

Nesse sentido, Bioni *et al* (2020, p. 8) argumentam que, para além de auxiliar no processo de conformidade com a legislação de proteção de dados, as avaliações de impacto: "são tributárias do que se convencionou chamar de devido processo informacional. Isto é, assegurar que haja não apenas medidas de transparência, mas de contenção sobre uma decisão que afetará liberdades públicas e individuais".

Portanto, é preciso que haja uma confluência entre dois tipos regulatórios: a regulação *ex ante* e a regulação *ex post*. A primeira, como apontado nas seções 5.1 e 5.2 deste documento, está intimamente relacionada com a própria natureza dos processos de risquificação da proteção de dados e de condução de relatórios de impacto à proteção de dados. Isto é, segue uma racionalidade antecipatória que visa avaliar os riscos e benefícios da implementação de determinada operação de tratamento de dados pessoais, sobretudo pelo poder público. Já a regulamentação *ex post* deve orientar a racionalidade regulatória após a condução de um relatório de impacto, partindo da concepção de que o RIPD é um instrumento vivo e que precisa ser atualizado sempre que houver alguma alteração na atividade de tratamento de dados pessoais. Ou seja, a concretização de efeitos adversos e benefícios ao longo da operação de dados é um aprendizado para a sofisticação progressiva do gerenciamento de riscos em questão.

Tal necessidade de imbricação entre dois modelos regulatórios se manifesta a partir da compreensão de que o relatório de impacto deve ser incorporado e revisado em todo o ciclo de vida de determinado projeto. Deve, portanto, ser conduzido tão logo seja possível, visando influenciar no modo como a operação de tratamento – ou, no caso deste documento, a política pública pautada pelo processamento de dados – será desenhada; e acompanhando todo o ciclo evolutivo dessa operação, de modo que o RIPD seja revisitado caso novos riscos sejam identificados (KLOZA, 2014).

Nesse sentido, considerando os elevados riscos aos titulares de dados que foram identifi-

cados ao longo dos capítulos 3 e 4 deste *policy paper* - os quais são decorrentes tanto da própria arquitetura informacional da Identificação Civil Nacional quanto da utilização da Base de Dados da ICN para a autenticação de usuários na plataforma gov.br -, a condução de relatórios de impacto à proteção de dados torna-se obrigatória para ambos os processos. Tal obrigatoriedade evidencia o RIPD como um importante processo a ser desenvolvido pelos agentes de tratamento do setor público.

Assim, a condução adequada – e orientada para os princípios relacionados à justiça procedimental – de relatórios de impacto à proteção de dados auxiliará no processo de garantia dos direitos fundamentais dos titulares de dados. Como resultado, será possível construir uma ponte para se alcançar a justiça social, a partir do desenvolvimento de um sistema de identificação civil cujas operações de tratamento de dados sejam mais transparentes e cujos riscos aos titulares de dados sejam devidamente identificados e mitigados. Assim, será possível enfrentar adequadamente o dilema visibilidade-exclusão com a priorização da inclusão de sujeitos historicamente invisibilizados e excluídos do acesso a serviços públicos e às políticas públicas básicas para o pleno exercício da cidadania.

6. Conclusões

6.1. Sumarização dos riscos decorrentes da ICN e do uso da BDICN para autenticação do cidadão no gov.br

Ao longo deste documento, tem sido apontado o fato de que a implementação da Identificação Civil Nacional ainda não se deu de forma plena, apesar dos constantes esforços empreendidos nos últimos anos. Assim sendo, o principal uso atual da Base de Dados da ICN ocorre no âmbito da plataforma gov.br, a qual corresponde à iniciativa do governo federal de unificar a prestação de serviços públicos digitais em um único ambiente.

Partindo desse cenário, este relatório, apoiado na relação dialética estabelecida pelo dilema visibilidade-exclusão, buscou mapear os riscos aos cidadãos – também identificados como titulares de dados – que tanto a arquitetura informacional da ICN quanto a sua relação com a plataforma gov.br apresentam. Esses riscos foram divididos em duas categorias: (i) riscos relacionados à arquitetura informacional e ao arranjo de governança da ICN - ou riscos de abusos no uso de dados pessoais; e (ii) riscos de exclusão de cidadãos, decorrentes tanto do fenômeno de plataformização de serviços públicos, quanto do uso da BDICN para autenticação de usuários da plataforma gov.br.

Quanto à primeira categoria, os riscos identificados estão relacionados à dimensão de visibilidade proposta pelo dilema mencionado anteriormente e decorrem da própria arquitetura informacional e do arranjo de governança da ICN estabelecidos pela Lei da ICN, a qual propõe a criação de uma única base de dados centralizada, composta por diversas outras bases de dados públicas, como a base de dados biométricos da Justiça Eleitoral. Esses riscos, que foram melhor detalhados no capítulo 3 deste documento, estão sumarizados na tabela abaixo:

Fonte do risco identificado	Motivo	Direitos fundamentais e liberdades civis potencialmente violados pelos riscos identificados
Ausência de pluralidade de visões no processo de governança de uma política pública complexa	Uma composição não multissetorial de um órgão de governança, como o Comitê Gestor da ICN e a Câmara-Executiva Federal de Identificação do Cidadão (CEFIC) – esta última estabelecida	São justamente as escolhas de governança que determinarão quais direitos e liberdades serão afetados. Nesse sentido, a limitação da participação da sociedade tem

	pelo Decreto nº 10.900/2021 -, tem o potencial de não contemplar a pluralidade de visões necessárias ao adequado processo de governança de uma política pública tão complexa quanto a ICN e o gov.br.	o potencial de afetar o regime democrático do Estado brasileiro, bem como todos os direitos fundamentais e liberdades civis dos cidadãos abarcados pela ICN.
Usos secundários e/ou compartilhados abusivos dos dados pessoais constantes na Base de Dados da ICN, em contraste ao princípio da finalidade (art. 6º, I, LGPD)	Existe um risco de usos secundários abusivos de dados pessoais na política da ICN, visível, sobretudo, em quatro momentos: **(i)** Na constituição da BDICN, que se deu a partir da junção de bases de dados de outras esferas públicas, cuja finalidade não é necessariamente compatível com a política da ICN; **(ii)** Na utilização da BDICN para autenticação de usuários na plataforma gov.br, que poderia significar uma desvirtuação da finalidade original das atividades de tratamento de dados da ICN; **(iii)** Utilização da BDICN para o cruzamento de dados de cidadãos com intuito de verificar o cumprimento de requisitos necessários ao acesso a benefícios sociais; **(iv)** Possibilidade de acesso à BDICN pelos poderes Executivo e Legislativo de qualquer nível federativo sem procedimento para verificação de finalidade.	**(i)** Violação da autodeterminação informativa, compreendida como um desdobramento do direito fundamental à proteção de dados pessoais, disposto no art. 5º, LXXIX da Constituição Federal. **(ii)** Violação da dignidade da pessoa humana, estabelecida como um dos fundamentos da República Federativa do Brasil, conforme art. 1º, III da Constituição Federal. **(iii)** Violação do princípio da não discriminação, estabelecido como um dos fundamentos da República brasileira, no art. 3º, IV, e da dignidade da pessoa humana, definido no art. 1º, III, ambos da Constituição Federal. **(iv)** Violação da autodeterminação informativa, compreendida como um desdobramento do direito fundamental à proteção de dados pessoais, estabelecido pela Constituição Federal o art. 5º, LXXIX.
Tratamento discriminatório aos cidadãos e práticas autoritárias	Além de possuir uma arquitetura informacional centralizada, a Base de Dados da ICN dispõe de uma diversidade enorme de dados, inclusive de dados biométricos, o que pode potencializar: **(i)** práticas vigilantistas por parte do Estado; **(ii)** a exclusão ilegal de cidadãos ao acesso a benefícios de assistência social com base em tratamento discriminatório desses dados, fundamentado no art. 11 da LICN.	**(i)** Vigilância em massa cria *chilling effect*, reduzindo a participação nos espaços públicos de cidadãos por receio de estarem sendo vigiados pelo governo, ameaçando assim a liberdade de expressão e manifestação, garantidas no art. 5º, IV, IX e XVI (ARTICLE 19). **(ii)** O tratamento discriminatório ameaça a igualdade garantida pela Constituição em seu art. 5º, caput, inciso I. O mesmo art. 5º também estabelece, como alvo de punição da lei qualquer prática discriminatória prejudicial aos direitos e

		liberdades fundamentais (art. 5º, inciso XLI) e a inafiançabilidade e imprescritibilidade do crime de racismo (art. 5º, inciso XLII).
Violação do princípio da qualidade dos dados (art. 6º, V, LGPD)	Segundo o TSE existem algumas inconsistências na base de dados biométricos: **(i)** Em 2018, 9 milhões de eleitores tiveram algum tipo de problema na identificação biométrica imediata durante as eleições. **(ii)** Desde 2014, foram identificados cerca de 52 mil casos relacionados à duplicidade ou pluralidade de biometrias.	**(i)** Impossibilidade do acesso a serviços públicos via plataforma gov.br, cuja prestação é garantida pelo art. 175 da Constituição. Ademais, a depender do serviço público cujo acesso for obstado, fere-se diretamente outros direitos fundamentais, a exemplo dos direitos sociais relativos ao trabalho e à seguridade social - como a impossibilidade de emitir a Carteira de Trabalho e Previdência Social (CTPS) e realizar a prova de vida junto ao Instituto Nacional do Seguro Social (INSS) -, ambos estabelecidos constitucionalmente como direitos sociais no art. 6º. **(ii)** Dificuldades na identificação do eleitor para o exercício do direito ao sufrágio, estabelecido no art. 14 da Constituição Federal.
Incidentes de segurança envolvendo a Base de Dados da ICN	Considerando o fato de que a BDICN possui dados biométricos (sensíveis) de mais de 110 milhões de brasileiros, o que configura um tratamento de dados em larga escala, a escolha por uma arquitetura informacional centralizada torna-se mais propensa a ser alvo de incidentes de segurança severos, uma vez que um único episódio poderia dar acesso a uma grande quantidade e diversidade de dados pessoais dos cidadãos, inclusive dados sensíveis, como os dados biométricos. Além disso, os incidentes de segurança envolvendo dados biométricos revelam um potencial lesivo ainda maior, uma vez que são dados diretamente relacionados ao corpo do titular e, consequentemente, não podem ser alterados.	Violação da dignidade da pessoa humana, estabelecida como um dos fundamentos da República Federativa do Brasil, conforme art. 1º, III da Constituição Federal. Segundo Informe do Alto Comissariado das Nações Unidas para os Direitos Humanos, de agosto de 2018 (A/HRC/39/29), "roubo de identidade baseado em dados biométricos é extremamente difícil de remediar e pode afetar severamente os direitos de um indivíduo."

Inviabilização do exercício dos direitos dos titulares previstos na LGPD pelos cidadãos	A plataforma gov.br, que utiliza a Base de Dados da ICN para autenticação de seus usuários, até onde se tem visibilidade de sua interface e política de privacidade, não possui um canal de comunicação direto e adequado para que os cidadãos possam solicitar a confirmação da existência do tratamento de dados, o acesso aos seus dados tratados e a retificação de dados incorretos ou desatualizados.	Violação da autodeterminação informativa, compreendida como um desdobramento do direito fundamental à proteção de dados pessoais, disposto no art. 5º, LXXIX da Constituição Federal.

Por sua vez, a segunda categoria de riscos mapeados trata daqueles riscos que emergem da utilização da BDICN para a autenticação de usuários na plataforma gov.br, visando a autorização do acesso a serviços públicos pelos cidadãos, e da estruturação da plataforma em si. Desse modo, tais riscos – que foram pormenorizados no capítulo 4 deste documento – se relacionam diretamente com a segunda dimensão do dilema proposto acima, qual seja, a exclusão de cidadãos de acesso a políticas públicas e serviços públicos. Eles podem ser visualizados de maneira esquemática na tabela a seguir:

Fonte do risco identificado	Motivo	Direitos fundamentais e liberdades civis potencialmente violados pelos riscos identificados
Exclusão do acesso a serviços públicos de pessoas que não possuem qualquer documento de identidade	A plataforma gov.br utiliza a BDICN para a autenticação de seus usuários a partir de um login único, de modo que, a fim de ter acesso aos serviços públicos digitalizados via gov.br, os cidadãos precisam ter seus dados pessoais catalogados na BDICN. Para tanto, é necessário que estes tenham algum documento de identificação, o que depende da emissão de uma certidão de nascimento - o "documento fundacional" brasileiro. Ficam excluídos do gov.br, portanto, aqueles que não possuem esse documento, sendo essa fatia da população mais numerosa nas regiões Norte e Nordeste.	Exclusão de acesso a direitos e políticas públicas, como por exemplo os direitos sociais relativos ao trabalho e à seguridade social, como a impossibilidade de emitir a Carteira de Trabalho e Previdência Social (CTPS) e realizar a prova de vida junto ao Instituto Nacional do Seguro Social (INSS), ambos estabelecidos constitucionalmente como direitos sociais no art. 6º.

Exclusão do acesso a serviços públicos de pessoas que possuam algum tipo de inadequação em seus documentos de identidade	A inadequação de documentos de identidade de pessoas trans tem o potencial de exclusão dessa população do acesso ao gov.br e, consequentemente, dos serviços públicos por meio da plataforma acessados. Tal risco decorre da possibilidade de os dados que constituem a BDICN não corresponderem à identidade de gênero da pessoa, seja porque ela ainda não procedeu com a retificação ou porque as bases de dados que compõem a BDICN ainda não foram atualizadas com as informações devidamente retificadas.	Exclusão de acesso a direitos e políticas públicas, como por exemplo os direitos sociais relativos ao trabalho e à seguridade social, como a impossibilidade de emitir a Carteira de Trabalho e Previdência Social (CTPS) e realizar a prova de vida junto ao Instituto Nacional do Seguro Social (INSS), ambos estabelecidos constitucionalmente como direitos sociais no art. 6º.
Exclusão do acesso a serviços públicos de sujeitos hipervulneráveis, como crianças, adolescentes, idosos e pessoas com deficiência	Crianças e adolescentes: **(i)** Em razão da idade, os seus dados não compõem as bases de dados da Justiça Eleitoral e dos Departamentos Estaduais de Trânsito (DETRAN). **(ii)** Por não possuírem dados biométricos registrados na BDICN, podem ser impossibilitados de alcançar o nível máximo de autenticação, que é concedido por meio de validação biométrica dos dados da Justiça Eleitoral e pela validação de dados em certificados digitais. Pessoas idosas: **(i)** A exclusão está associada a dificuldades de uso de computadores, celulares e Internet, decorrentes de analfabetismo e analfabetismo funcional. Pessoas com Deficiência: **(i)** As ferramentas de autenticação disponíveis na plataforma gov.br não são acessíveis e inclusivas a todas as pessoas com deficiência.	Crianças e adolescentes: **(i)** Dificuldade ou inviabilidade de exercer direitos e gozar de políticas e serviços públicos digitais, violando o art. 3º do Estatuto da Criança e do Adolescente. Pessoas idosas: **(i)** Inviabilidade do exercício de direitos sociais relacionados à pessoas idosas, como o acesso à previdência social, estabelecido pelo art. 6º da Constituição Federal. Pessoas com Deficiência: **(i)** Dificuldade ou impossibilidade de acessar serviços públicos digitais, em razão da falta de acessibilidade, violando o art. 4º do Estatuto da Pessoa com Deficiência.

Exclusão do acesso a serviços públicos de pessoas em razão da falta de acesso pleno à Internet	Nessa hipótese, a exclusão se dá em razão da impossibilidade de o cidadão utilizar a plataforma gov.br, seja pela ausência total de acesso à Internet ou pela ausência de um acesso pleno à Internet. Segundo dados recentes, a ausência de acesso pleno à Internet ocorre, mais frequentemente, entre as pessoas de classes sociais mais vulneráveis, que inclusive deixam de acessar serviços públicos por falta de conexão.	Exclusão de acesso a direitos e políticas públicas, como por exemplo os direitos sociais relativos ao trabalho e à seguridade social, como a impossibilidade de emitir a Carteira de Trabalho e Previdência Social (CTPS) e realizar a prova de vida junto ao Instituto Nacional do Seguro Social (INSS), ambos estabelecidos constitucionalmente como direitos sociais no art. 6º.

6.2. Dos riscos e dos direitos: a obrigatoriedade de condução e publicação de Relatório de Impacto à Proteção de Dados Pessoais

Como apontado anteriormente, o relatório de impacto à proteção de dados pessoais é uma importante ferramenta de *accountability* estabelecida pela Lei Geral de Proteção de Dados Pessoais, cuja condução está vinculada à noção de risco aos titulares de dados decorrente de determinada atividade de tratamento de dados.

Apesar de o ordenamento jurídico brasileiro ainda não dispor de uma procedimentalização sobre a condução do RIPD, é possível verificar que, internacionalmente, a sua condução é impulsionada pela existência de um elevado grau de risco para os direitos fundamentais e liberdades civis dos titulares de dados. É para esse mesmo sentido que aponta o Regulamento Geral sobre a Proteção de Dados da União Europeia.

No âmbito nacional, o RIPD está em processo de regulamentação pela Autoridade Nacional de Proteção de Dados e, inclusive, previsto como tema da Agenda Regulatória do órgão para o biênio 2021-2022. Contudo, já é possível identificar direcionamentos por parte da ANPD sobre o que o ordenamento jurídico brasileiro compreende como atividade de tratamento de dados de alto risco - casos nos quais torna-se obrigatória a condução do relatório de impacto à proteção de dados. Conforme apontado na seção 5.3 deste documento, a resolução publicada pela ANPD sobre a aplicação da LGPD para agentes de tratamento de pequeno porte estabelece uma série de critérios, divididos entre critérios gerais e específicos, dos quais a ICN e seu uso no gov.br atendem aos critérios de tratamento de dados em larga escala e utilização de dados pessoais sensíveis e de idosos. Isso já se demonstra o suficiente para seu enquadramento como uma atividade de tratamento de alto risco e, consequentemente, para tornar mandatória a condução de um RIPD.

Em outras palavras, considerando esse cenário normativo-regulatório e as políticas públicas em análise neste *policy paper* – quais sejam, a Identificação Civil Nacional e a utilização da Base de Dados da ICN para a autenticação de usuários na plataforma gov.br –, conclui-se que as atividades de tratamento de dados que constituem tais políticas públicas se enquadram nos critérios de alto risco, uma vez que envolvem, por essência, o tratamento de dados em larga escala e a utilização de dados pessoais sensíveis.

Desse modo, a partir de uma interpretação sistemática do que se encontra disponível no ordenamento jurídico brasileiro, em termos de regulamentações e orientações sobre a classificação de atividade de tratamento de elevado grau de risco aos titulares alto grau de risco e sobre quando se recomenda a condução do RIPD, compreende-se que a sua condução é obrigatória tanto para a implementação da Identificação Civil Nacional quanto para a utilização da Base de Dados da ICN para a autenticação de usuários na plataforma gov.br. Essa obrigatoriedade tem por objetivo auxiliar no processo de enfrentamento do dilema visibilidade-exclusão, imposto pela implementação de um sistema de identidade digital centralizado, de modo a mitigar os seus riscos.

Para além da obrigatoriedade na condução do RIPD, é necessário que o processo de sua elaboração esteja atrelado a uma sólida metodologia científica de análise de riscos. Ademais, é essencial que o Relatório contemple, ao mínimo, os riscos identificados nos capítulos 3 e 4 deste documento, os quais foram sumarizados nas tabelas, uma vez que estes se relacionam com potenciais violações aos direitos fundamentais de acesso a serviços públicos e à identificação civil, a qual se constitui como um dos fundamentos do pleno exercício da cidadania; além do conteúdo mínimo estabelecido pelos art. 5º, inciso XVII e pelo art. 38, parágrafo único, e de outros riscos que, porventura, não foram identificados por este *policy paper*.

E não apenas. O capítulo 5 deste documento apontou o fato de que o RIPD, apesar de contribuir para o processo de conformidade de determinada organização com a legislação de proteção de dados pessoais, não é um documento de conformidade, pois possui como centro gravitacional o titular de dados. É dizer, o relatório de impacto tem por objetivo a garantia dos direitos fundamentais e liberdades civis dos titulares de dados. Além disso, não se pode olvidar que o RIPD deve ser um documento vivo, a ser constantemente revisitado e atualizado, sempre que houver alterações nas atividades de tratamento de dados pessoais que impliquem na emergência de novos riscos aos titulares de dados pessoais.

O RIPD emerge, assim, como uma poderosa ferramenta de *accountability*. E, como tal, um elemento que se apresenta como essencial para que os seus objetivos, como o de proporcionar a efetiva participação da sociedade, sejam cumpridos é sua publicização.

A Lei Geral de Proteção de Dados não estabelece quais as situações que culminariam na publicização do RIPD. Não obstante, é possível verificar que, conforme o art. 32 da LGPD, a publicização desse instrumento possui contornos específicos quando a sua condução se dá a partir de uma atividade de tratamento de dados pessoais executada pelo poder público. Nessa esteira, uma interpretação sistemática dos dispositivos da LGPD e dos princípios constitucionais da Administração Pública - sobretudo o princípio da publicidade - leva à conclusão de que existe um dever de publicização do RIPD por parte do poder público, conforme demonstrado no capítulo 5, subseção 5.3a deste documento.

A publicização por padrão do RIPD pelo setor público tem o condão, assim, de aumentar a transparência, prestação de contas e responsabilização (*accountability*) dos agentes públicos de tratamento de dados. Ademais, permite uma ampliação da participação da sociedade nos processos de construção de políticas públicas que envolvam tratamento de dados pessoais em larga escala, e na possibilidade de fiscalização de políticas públicas pela a sociedade civil - que é afetada diretamente por tais políticas.

Desse modo, conclui-se que a condução de relatórios de impacto à proteção de dados para a implementação da Identificação Civil Nacional e para a utilização da Base de Dados da ICN na autenticação dos usuários na plataforma gov.br é um primeiro passo essencial em direção a políticas públicas de tratamento de dados que sejam transparentes, passíveis de responsabilização e que demonstrem que as medidas necessárias foram tomadas para a mitigação dos riscos aos titulares de dados. Para que isso se concretize, a publicização destes documentos deve ser obrigatória, considerando o seu relevante interesse público.

O relatório de impacto à proteção de dados pessoais, devidamente conduzido e publicizado, deve ser considerado um aliado para o enfrentamento do dilema visibilidade-exclusão. Isso porque a identificação e mitigação dos riscos de um sistema de identidade digital unificado, como se propõe a ICN e a utilização de sua base de dados na plataforma gov.br, são elementos fundamentais para que se ache o correto balanço entre riscos e benefícios destas políticas públicas, as quais são fundantes para o exercício da cidadania no país.

Referências bibliográficas

AGÊNCIA BRASIL.**Governo atinge marca de 1,5 mil serviços digitalizados em 34 meses**. 04 nov. 2021. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/governo-atinge-marca-de-15-mil-servicos-digitalizados-em-34-meses>. Acesso em 11 mai. de 2022.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 650, de 16 de março de 2015**. 01 jun. 2021. Disponível em: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2015/790-resolucao-650>. Acesso em 12 mai. de 2022.

ALMEIDA, Virgílio; GETSCHKO, Demi; AFONSO, Carlos A. The Origin and Evolution of Multistakeholder Models. IEEE Internet Computing, n.19, v. 1, 74–79, 2015. Disponível em: <https://www.computer.org/csdl/magazine/ic/2015/01/mic2015010074/13rRUNvya5I>. Acesso em: 13 mai. 2022.

AMNESTY INTERNATIONAL. Xenophobic machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal, 2021. Disponível em: <https://www.amnesty.org/en/documents/eur35/4686/2021/en/>. Acesso em: 17 mai. 2022.

ARTICLE 19. When bodies become data: Biometric technologies and free expression, 2021. Disponível em: <https://www.article19.org/wp-content/uploads/2021/05/Biometric-Report-P3-min.pdf>. Acesso em: 18 mai. 2022.

ARTICLE 29 DATA PROTECTION WORKING PARTY - WP 29. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. [s.l.], 2014. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Acesso em: 18 mai. 2022.

ANDRADE, Eduardo Goulart *et al.* Dados Virais: Legado da COVID-19 nas aquisições de tecnologias pelo Poder Público. Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: <https://drive.google.com/file/d/1-PmjyYubF65W_8LuOiYR2pw-FQiRWEyZ3/view>. Acesso em: 13 mai. 2022.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. Accountability e Identidade Civil Digital, s.d a. Página projeto Accountability e Identidade Civil Digital. Disponível em: <https://www.dataprivacybr.org/projeto/accountability-e-identidade-civil-digital/>. Acesso em: 09 mai. 2022.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. Apresentação na Turing trustworthy digital identity conference, s.d. b Disponível em: <https://www.dataprivacybr.org/documentos/apresentacao-na-turing-trustworthy-digital-identity-conference/>. Acesso em 09 mai. 2022.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. Oficina sobre Relatório de Impacto à Proteção de Dados e identidade civil digital, s.d c. Disponível em: <https://www.dataprivacybr.org/documentos/oficina-sobre-relatorio-de-impacto-a-protecao-de-dados-e-identidade-civil-digital/>. Acesso em 18 mai. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. Portaria nº 11, de 27 de janeiro de 2021. **Torna pública a agenda regulatória para o biênio 2021-2022**. Brasília, 2021 Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Acesso em: 09 mai. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, 2022. Disponível em: <https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019?utm_source=google--search&utm_medium=cpc&utm_campaign=-totvs_conversao_sql&utm_term[0]=s-institucional_Totvs&utm_term[1]=totvs&utm_content=eta-v4>. Acesso em: 09 mai. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. Guia Orientativo: Tratamento de dados pelo Poder Público. Brasília, jan. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 18 mai. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. 10 mai 2022. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/conselho-nacional-de-protecao-de-dados-pessoais-e-privacidade-cnpd>. Acesso em: 12 mai. 2022.

BANCO MUNDIAL. ID4D: About us, 2022. Disponível em: <https://id4d.worldbank.org/about-us>. Acesso em: 10 mai. 2022.

BANCO MUNDIAL. ID4D: Country Engagement, 2022. Disponível em <https://id4d.worldbank.org/country-engagement>. Acesso em: 10 mai. 2022.

BBC. Aadhaar: 'Leak' in world's biggest database worries Indians. 5 de Janeiro de 2018. Disponível em: <https://www.bbc.com/news/world-asia-india-42575443>. Acesso em: 16 mai. 2022.

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (orgs.). Inteligência Artificial e Direito: ética, regulação e responsabilidade. São Paulo: Revistas dos Tribunais, 2019.

BIONI, Bruno; RIELLI, Mariana. Salvaguardas regulatórias: entre princípio da precaução e relatórios de impacto. *In*: BIONI, Bruno; ZANATTA, Rafael; RIELLI, Mariana (orgs.). Data Privacy Br: Contribuição à consulta pública da Estratégia Brasileira de Inteligência Artificial. São Paulo: Reticências Creative Design Studio, 2020. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/06/E-BOOK-CONTRIBUIÇÃO-DPBR-INTELIGÊNCIA-ARTIFICIAL-FINAL.pdf>. Acesso em: 10 mai. 2022.

BIONI, Bruno *et al.* Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/12/NOTA-TÉCNICA-PROTEÇÃO-DE-DADOS-NO-CAMPO-PENAL-E-DE-SEGURANÇA-PÚBLICA-VF-31.11.2020.pdf>. Acesso em: 11 mai. 2022.

BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 3 ed. Rio de Janeiro: Forense, 2021.

BOCCHINI, Bruno. Pesquisa mostra exclusão de idosos do mundo digital e da escrita. Agência Brasil. São Paulo, 21 ago. 2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-08/pesquisa-mostra-exclusao-de-idosos-do-mundo-digital-e-da-escrita>. Acesso em: 17 mai. 2022.

BRASIL. Lei nº 6.015, de 31 de dezembro de 1973. Dispõe sobre os registros públicos, e dá outras providências.. Brasília, 1973. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l6015compilada.htm>. Acesso em: 18 mai. 2022.

BRASIL. Lei nº 7.116, de 29 de agosto de 1983. Assegura validade nacional as Carteiras de Identidade regula sua expedição e dá outras providências. Brasília, 1983. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/1980-1988/l7116.htm>. Acesso em: 18 mai. 2022.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 11 mai. 2022.

BRASIL. Lei nº 10.741, de 1º de outubro de 2003. Dispõe sobre o Estatuto do Idoso e dá outras providências. Brasília, 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm>. Acesso em: 11 mai. 2022.

BRASIL. Lei nº 13.146, de 6 de julho de 2015. Estatuto da Pessoa com Deficiência. Brasília, 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm>. Acesso em: 11 mai. 2022.

BRASIL. Lei 13.444, de 11 de maio de 2017. Dispõe sobre a Identificação Civil Nacional (ICN). Brasília, 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm>. Acesso em: 17 mai. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 09 mai. 2022.

BRASIL. Lei nº 13.848, de 25 de junho de 2019. Lei das Agências Reguladoras. Brasília, 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13848.htm>. Acesso em: 18 mai. 2022.

BRASIL. Decreto nº 10.900, de 17 de dezembro de 2021. Dispõe sobre o Serviço de Identificação do Cidadão e a governança da identificação das pessoas naturais no âmbito da administração pública federal direta, autárquica e fundacional, e altera o Decreto nº 8.936, de 19 de dezembro de 2016, o Decreto nº 10.543, de 13 de novembro de 2020, e o Decreto nº 9.278, de 5 de fevereiro de 2018. Brasília, 2021a. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.900-de-17-de-dezembro-de-2021-368282514>. Acesso em: 16 mai. de 2022.

BRASIL. Acordo de Cooperação Técnica que firmam entre si a Secretaria-Geral da Presidência da República, o Ministério da Economia e o Tribunal Superior Eleitoral, objetivando a cooperação para implementação da Identificação Civil Nacional. Brasília, 15 mar. 2021b. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/arquivos/act-identificacao-civil-nacional/rybena_pdf?file=https://www.tse.jus.br/imprensa/noticias-tse/arquivos/act-identificacao-civil-nacional/at_download/file>. Acesso em: 18 mai. 2022.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília, 2021c. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm>. Acesso em: 17 mai. 2022.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 3.228, de 20 de set. 2021. Altera a Lei nº 13.444, de 11 de maio de 2017, que dispõe sobre a Identificação Civil Nacional - ICN. Brasília: Câmara dos Deputados, 2021. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2076542>. Acesso em: 17 mai. 2022.

BRASIL. Portaria nº 667, de 9 de fevereiro de 2022. Agenda Legislativa Prioritária do Governo Federal para o ano de 2022. Brasília, 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-667-de-9-de-fevereiro-de-2022-379226707>. Acesso em: 17 mai. 2022.

BRODERSEN, Juan; BLANCO, Pablo Javier. Un cibercriminal que asegura haber robado datos de 45 millones de DNI difundió fotos de políticos, periodistas y famosos en Twitter. Clarín, Buenos Aires, 13 de Outubro de 2021. Disponível em: <https://www.clarin.com/tecnologia/ciberdelincuente-asegura-robado--datos-45-millones-dni-difundio-fotos-politicos--periodistas-famosos-twitter_0_QBD5xKDNM.html>. Acesso em: 16 mai. 2022.

BRODERSEN, Juan; BLANCO, Pablo Javier. "Quizás publique los datos personales de 1 o 2 millones de personas", dijo el usuario que filtró fotos de los DNI de políticos, famosos y periodistas. Clarín, Buenos Aires, 19 de Outubro de 2021. Disponível em: <https://www.clarin.com/tecnologia/-publique-datos-personales--1-2-millones-personas-dijo-usuario-filtro-fotos--dni-politicos-famosos-periodistas_0_SgsEoUeQj.html?utm_term=Autofeed&utm_medium=Social&utm_source=Twitter#Echobox=1634683887>. Acesso em: 16 mai. 2022.

CÂMARA DOS DEPUTADOS. Pandemia acelera o uso de serviços públicos digitais: ao todo, há 4.699 serviços por meio do portal do governo federal, 2021. Disponível em: <https://www.camara.leg.br/noticias/809660-pandemia-acelera-o-uso-de-servicos-publicos-digitais/>. Acesso em: 10 de mai. de 2022.

CARVALHO FILHO, José dos Santos. Manual de Direito Administrativo. 34. ed. São Paulo: Atlas, 2020.

CARIBOU DIGITAL. Identification, identity, and sexuality in Brazil, 2020. Disponível em: <https://medium.com/caribou-digital/identification-identity-and-sexuality-in-brazil--da5464a634d2>. Acesso em: 11 mai. 2022.

CENTRO DE ESTUDOS DE CULTURA CONTEMPOR NEA - CEDEC. Mapeamento das pessoas trans no município de São Paulo: relatório de pesquisa. São Paulo, 2021. Disponível em: <https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/direitos_humanos/LGBT/AnexoB_Relatorio_Final_Mapeamento_Pessoas_Trans_Fase1.pdf>. Acesso em: 17 mai. 2022.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.br). Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros : TIC Domicílios 2020: edição COVID-19: metodologia adaptada, São Paulo: Comitê Gestor da Internet, 2021. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20211124201233/tic_domicilios_2020_livro_eletronico.pdf>. Acesso em: 11 mai. 2022.

CLARKE, Roger. Privacy impact assessment: its origins and development. Computer Law & Security, [s.l], n. 25, 2009. Disponível em: <https://openresearch-repository.anu.edu.au/bitstream/1885/53679/2/01_Clarke_Privacy_impact_assessment%3A_Its_2009.pdf>. Acesso em: 10 mai. 2022.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Regimento Interno do Comitê Gestor da Internet no Brasil**, s.d. Disponível em: <https://www.cgi.br/pagina/regimento-interno-do-comite-gestor-da-internet-no-brasil/308/>. Acesso em: 12 mai. 2022.

CONSELHO NACIONAL DE JUSTIÇA - CNJ. Provimento nº 46, de 16 de julho de 2015. Revoga o Provimento 38 de 25/07/2014 e dispõe sobre a Central de Informações de Registro Civil das Pessoas Naturais - CRC. Brasília, 2015. Disponível em: <https://atos.cnj.jus.br/files//provimento/provimento_46_16062015_16032018111049.pdf>. Acesso em: 18 mai. 2022.

DAHL-JØRGENSEN, Tangni Cunningham, PARMIGGIANI, Elena. Platformization of the public sector: Assessing the space of possibility for participation. Proceedings of the 16th Participatory Design Conference - Participation(s) Otherwise - Volume 2, 2020. Disponível em: <https://dl.acm.org/doi/10.1145/3384772.3385154>. Acesso em: 13 mai. 2022.

DAMASCENO, Victoria. Cadastro do SUS e sistema que emite certificado de vacina impedem uso de nome social. Folha de São Paulo. São Paulo, 28 jan. 2022. Disponível em: <https://www1.folha.uol.com.br/equilibrioesaude/2022/01/cadastro-do-sus-e-sistema-que-emite-certificado-de-vacina-impedem-uso-de-nome-social.shtml?utm_source=twitter&utm_medium=social&utm_campaign=twfolha>. Acesso em: 17 mai. 2022.

DANTCHEVA, Antitza; ELIA, Petros; ROSS, Arun. What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. IEEE Transactions on Information Forensics and Security, vol. 11, n. 3, 2016. Disponível em: <https://ieeexplore.ieee.org/document/7273870>. Acesso em: 18 mai. 2022.

DATA PRIVACY BRASIL. Oficina sobre Relatório de Impacto à Proteção de Dados para o Poder Público. Youtube, 13 de jan. de 2022. Disponível em: <https://www.youtube.com/watch?v=sLBc1nLTcFA&t=2758s>.

DIJCK, José Van; POELL, Thomas; DE WAAL, Martijn. **The Platform Society**. Nova Iorque: Oxford University Press, 2018.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed., São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo; KANASHIRO, Marta. A transformação da identificação e a construção de bancos de dados: o caso do documento único no Brasil. *In*: BRUNO, Fernanda; KANASHIRO, Marta; FIRMINO, Rodrigo (orgs.). Vigilância e visibilidade: espaço, tecnologia e identificação, Porto Alegre: Sulina, 2010, p. 272-296.

ESCÓSSIA, Fernanda Melo da. Invisíveis: Uma etnografia sobre identidade, direitos e cidadania nas trajetórias de brasileiros sem documento. 2019. Tese (Doutorado) - Programa de Pós-Graduação em História, Política e Bens Culturais do Centro de Pesquisa e Documentação em História Contemporânea do Brasil, Fundação Getúlio Vargas, 2019. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27459/Tese%20Fernanda%20da%20Escóssia.pdf?sequence=1&isAllowed=y>. Acesso em: 17 mai. 2022.

EUBANKS, Virginia. Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor. St Martin's Press: 2018.

FAULKNER-GURSTEIN, Rachel; WYATT, David. Platform NHS: Reconfiguring a Public Service in the Age of Digital Capitalism. **Science, Technology, & Human Values**, p. 01-21, 22 nov. 2021. Disponível em: <https://journals.sagepub.com/doi/10.1177/01622439211055697>. Acesso em: 12 mai. 2022.

GARROTE, Marina *et al.* A ICN e o futuro da identidade civil (digital) no Brasil, Jota, [s.l.], 04 out 2021a. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/a-icn-e-o-futuro-da-identidade-civil-digital-no-brasil-04102021>. Acesso em: 16 mai. 2022.

GARROTE, Marina *et al.* ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais, Jota, [s.l.], 13 jun 2021b. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021>. Acesso em: 09 mai. 2022

GELB, Alan.; CLARK, Julia. Identification for Development: The Biometrics Revolution. **SSRN Electronic Journal**, 2013.

GELLERT, Raphaël. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law*, v. 5, n. 1, 2015 p. 3–19. Disponível em: <https://doi.org/10.1093/idpl/ipu035>. Acesso em: 11 mai. 2022.

GELLERT, Raphaël. We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection, European Data Protection Law Review, n. 4, v. 2, 2016. Disponível em: <https://edpl.lexxion.eu/article/edpl/2016/4/7>. Acesso em: 11 mai. 2022.

GOMES, Maria Cecília O. Relatório de impacto à proteção de dados pessoais. Revista do Advogado- AASP, n. 144, 2019. Disponível em: <https://www.academia.edu/41160034/Relatório_de_Impacto_a_Proteção_de_Dados_Pessoais_uma_breve_análise_da_sua_definição_e_papel_na_LGPD>. Acesso em: 19 mai. 2022.

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

GOVERNO FEDERAL. Gov.br - Portal Único do Governo, s.d. Disponível em: <https://www.gov.br/sobre/> Acesso em: 12 mai. 2022.

GOVERNO FEDERAL. **Acordo de Cooperação agilizará a implementação da Identidade Digital**. 16 mai. 2021. Disponível em: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2021/marco/acordo-de-cooperacao-agilizara-a-implementacao-da-identidade-digital-1> Acesso em: 12 de mai. de 2022.

GOVERNO FEDERAL. Digitalização de serviços públicos já atinge mais de 100 municípios, entre eles São Paulo. 19 abr. 2022a. Disponível em: <https://www.gov.br/economia/pt-br/assuntos/noticias/2022/abril/digitalizacao-de-servicos-publicos-ja-atinge-mais-de-100-municipios-entre-eles-sao-paulo>. Acesso em: 17 mai. 2022.

GOVERNO FEDERAL. Fevereiro registra aumento de usuários na plataforma GOV.BR. 04 mai. 2022b. Disponível em: <https://www.gov.br/secretariageral/pt-br/noticias/2022/marco/fevereiro-registra-aumento-de-usuarios-na-plataforma-gov.br>. Acesso em: 19 mai. 2022.

GOVERNO FEDERAL. gov.br atinge 130 milhões de usuários. 06 jun. 2022c. Disponível em: <https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2022/06/gov-br-atinge-130-milhoes-de-usuarios>. Acesso em: 07 jun. 2022.

GRUPO DE PESQUISA EM POLÍTICAS PÚBLICAS PARA O ACESSO À INFORMAÇÃO – GPOPAI. Contribuições à Consulta Pública do Anteprojeto de Lei/APL de Proteção de Dados Pessoais. São Paulo: 02 de julho de 2015. Disponível em: <https://brunobioni.com.br/wp-content/uploads/2019/04/Contribuicao-GPoPAI-Dados-Pessoais_Diagramada.pdf>. Acesso em 23 mai. 2022.

GRUPO DE TRABALHO DO ARTIGO 29 PARA PROTEÇÃO DE DADOS. Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679, 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236/en>. Acesso em: 10 mai. 2022.

HARRIS, Swee Leng. Data Protection Impact Assessments as rule of law governance mechanisms. Data & Policy. 2020. vol. 2,. Disponível em: <https://doi.org/10.1017/dap.2020.3>. Acesso em: 18 mai. 2022.

IGO, Sarah Elizabeth. **The known citizen : a history of privacy in modern America**. Cambridge, Massachusetts : Harvard University Press, 2018.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC; INSTITUTO LOCOMOTIVA. Barreiras e limitações no acesso à internet e hábitos de uso e navegação na rede nas classes C, D e E, 2021. Disponível em: <https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf>. Acesso em: 11 mai. 2022.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. Vazamentos de dados de saúde coloca consumidor em risco; veja o que fazer. 02 de Dezembro de 2020. Disponível em: <https://idec.org.br/noticia/vazamentos-de-dados-de-saude-coloca-consumidor-em-risco-veja-o-que-fazer>. Acesso em 16 mai. 2022.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. Acesso à Internet na Região Norte do Brasil. Instituto Brasileiro de Defesa do Consumidor e Derechos Digitales. Mar. 2022. Disponível em: <https://idec.org.br/pesquisas-acesso-internet>. Acesso em: 18 mai. 2022.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE. Pesquisa Estatísticas do Registro Civil: Nota técnica 01/2020 - Esclarecimentos sobre o Sub-Registro de Nascimentos, 2020. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/periodicos/3099/rc_sev_esn_2018.pdf>. Acesso em: 17 mai. 2022.

JUSTIÇA ELEITORAL. Biometria. [s.l.], s.d. Disponível em: <https://www.justicaeleitoral.jus.br/biometria/>. Acesso em: 18 mai. 2022.

KANASHIRO, Marta Mourão; DONEDA, Danilo. The new Brazilian identification system: Unique features of a general transformation. **Surveillance & Society**, v.10, n.1, p.18–27, 18 jul. 2012. Disponível em: <https://doi.org/10.24908/ss.v10i1.4272>. Acesso em: 11 mai. 2022.

KANG, Margareth; DONEDA, Danilo; 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, agosto 2016. Disponível em: <http://opiniaopublica.ufmg.br/site/files/artigo/4-Margareth-Kang.pdf>. Acesso em: 11 mai. 2022.

KANG, Margareth; LUCIANO, Maria; SANTOS, Maike Wille. Relatório das audiências públicas. In: Análise técnica elaborada pelo Projeto Privacidade Brasil: PLC nº 19/2017 – Identidade Civil Nacional. 2017.

KANG, Margareth; LUCIANO, Maria . Nota técnica. In: Análise técnica elaborada pelo Projeto Privacidade Brasil: PLC nº 19/2017 – Identidade Civil Nacional.

KEANE, Jonathan. Facial Recognition Apps Are Leaving Blind People Behind. Vice, [s.l], 22 mar. 2016. Disponível em: <https://www.vice.com/en/article/ezpzzp/facial-recognition-apps-are-leaving-blind-people-behind>. Acesso em: 17 mai. 2022.

KLOZA, Dariusz. Privacy Impact Assessments as a Means to Achieve the Objectives of Procedural Justice. Jusletter IT. Die Zeitschrift für IT und Recht, 2014. Disponível em: <https://researchportal.vub.be/en/publications/privacy-impact-assessments-as-a-means-to-achieve-the-objectives-o>. Acesso em: 11 mai. de 2022.

KLOZA, Dariusz *et al.* Avaliações de impacto sobre a proteção de dados na União Europeia: complementando o novo regime jurídico em direção a uma proteção mais robusta dos indivíduos. d.pia.lab Policy Brief, 1/2017, 2020.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 445-463.

LIMA, Maria Cristina Oliveira de. "Por causa de um papel eu não podia voltar pra casa com meu bebê". Revista Piauí, 22 fev. 2022. Disponível em: <https://piaui.folha.uol.com.br/por-causa-de-um-papel-eu-nao-podia-voltar-pra-casa-com-meu-bebe/>. Acesso em: 18 mai. 2022.

LISTER, Charles. Privacy and large-scale personal data systems. **The Personnel and Guidance Journal**, v. 49, n.3, p. 207–211, nov. 1970. Disponível em: <https://doi.org/10.1002/j.2164-4918.1970.tb03433.x>. Acesso em: 16 mai. 2022.

LOBO, Ana Paula. Serpro leva contrato de R$ 72 milhões para fazer a identificação civil nacional. Convergência Digital, 10 jan. 2022. Disponível em: <https://www.convergenciadigital.com.br/Governo/Serpro-leva-contrato-de-R%24-72-milhoes-para-fazer-a-identificacao-civil-nacional-59110.html>. Acesso em: 17 mai. 2022.

LOPEZ, Oscar. Reported murders, suicides of trans people soar in Brazil. Reuters, [s.l.], 8 de setembro de 2020. Disponível em: <https://www.reuters.com/article/us-brazil-lgbt-murders-trfn-idUSKBN25Z31O>. Acesso em: 11 mai. 2022.

LYON, David. **Identifying citizens: ID Cards as Surveillance**. Cambridge: Polity Press, 2009.

MARÉCHAL, Nathalie. First They Came for the Poor: Surveillance of Welfare Recipients as an Uncontested Practice. **Media and Communication**, v. 3, n. 3, p. 56–67, 20 out. 2015. Disponível em: <https://www.cogitatiopress.com/mediaandcommunication/article/view/268>. Acesso em: 10 mai. 2022.

MARTIN, Aaron. Aadhaar in a Box? Legitimizing Digital Identity in Times of Crisis. **Surveillance & Society**, [s.l.], v.19, n.1, p. 104-108, 5 mar, 2021. Disponível em: <https://doi.org/10.24908/ss.v19i1.14547>. Acesso em: 10 mai. 2022.

MASIERO, Silvia.; SHAKTHI, S. Grappling with Aadhaar: Biometrics, Social Identity and the Indian State. **South Asia Multidisciplinary Academic Journal**, n. 23, 15 set. 2020. Disponível em: <https://journals.openedition.org/samaj/6279>. Acesso em: 10 mai. 2022.

MASIERO, Silvia; BAILUR, Savita. Digital identity for development: The quest for justice and a research agenda. **Information Technology for Development**, v. 27, n. 1, p. 1–12, 2 jan. 2021. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/02681102.2021.1859669>. Acesso em: 10 mai. 2022.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe. **Technology and Privacy: The New Landscape**. Cambridge, MA: The MIT Press. p.219-242.

MINISTÉRIO DA EDUCAÇÃO. Portaria nº 33 de 18 de janeiro de 2018. Brasília, 2018. Disponível em: <http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=72921-pcp014-17-pdf&-category_slug=setembro-2017-pdf&Itemid=30192>. Acesso em: 17 mai. 2022.

MINISTÉRIO DA ECONOMIA. Do Eletrônico ao Digital, 25 nov. 2019. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>. Acesso em: 23 mai. 2022.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Escritório de Projetos e Processos do RIC- EPP, s.d. Disponível em: <https://www.justica.gov.br/Acesso/governanca/escritorio-de-projetos-e-processos-do-ric-2013-epp>. Acesso em: 11 mai. 2022.

MINISTÉRIO DA SAÚDE. Portaria nº 1.820, de 13 de agosto de 2009. Brasília, 2009. Disponível em: <https://conselho.saude.gov.br/ultimas_noticias/2009/01_set_carta.pdf>. Acesso em: 17 mai. 2022.

MULHOLLAND, Caitlin; MATERA, Vinicius. O tratamento de dados pessoais pelo Poder Público. *In*: MULHOLLAND, Caitlin (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, p. 217-236.

MURAKAMI WOOD, David.; FIRMINO, Rodrigo. Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of 'identity fraud'. **Identity in the Information Society**, v. 2, n. 3, p. 297–317, dez. 2009. Disponível em: <http://link.springer.com/10.1007/s12394-010-0038-y>. Acesso em: 10 mai. 2022.

MURAKAWA, Fabio. 'Ninguém está totalmente preparado', diz Heleno sobre ataque hacker a sites do governo. Valor, Brasília, 13 de Dezembro de 2021. Disponível em: <https://valorinveste.globo.com/mercados/brasil-e-politica/noticia/2021/12/13/ninguem-esta-totalmente-preparado-diz-heleno-sobre-ataque-hacker-a-sites-do-governo.ghtml>. Acesso em: 16 mai. 2022.

NAÍSA, Letícia. Falha no sistema do Inep expõe dados de 5 milhões de estudantes; entenda. Uol, São Paulo, 10 de Setembro de 2021. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/09/10/falha-no-sistema-do-inep-vaza-dados-de-5-milhoes-de-estudantes.htm>. Acesso em: 16 mai. 2022.

NATION. Judge orders State to regularise Huduma Namba roll out, 2021. Disponível em: <https://nation.africa/kenya/news/judge-orders-state-to-regularise-huduma-namba-roll-out-3582906>. Acesso em: 10 mai. 2022.

NISSENBAUM, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. California: Stanford University Press, 2010.

OCDE. **OECD Reviews of Digital Transformation: Going Digital in Brazil**. [s.l.] OCDE, 2020.

OPEN SOCIETY FOUNDATIONS. Nubian Rights Forum *et al.* v. the Honourable Attorney General of Kenya *et al.* ("NIIMS case"), 2022. Disponível em: <https://www.justiceinitiative.org/litigation/nubian-rights-forum-et-al-v-the-honourable-attorney-general-of-kenya-et-al-niims-case>. Acesso em: 10 mai. 2022.

POELL, Thomas.; NIEBORG, David.; VAN DIJCK, José. Platformisation. **Internet Policy Review**, v. 8, n. 4, 29 nov. 2019. Disponível em: <https://policyreview.info/node/1425>. Acesso em: 12 mai. 2022.

PRIVACY COMPANY. New DPIA for the Dutch government and universities on Microsoft Teams, OneDrive and SharePoint Online. 21 fev. 2022. Disponível em: <https://www.privacycompany.eu/blogpost-en/new-dpia-for-the-dutch-government-and-universities-on-microsoft-teams-onedrive-and-sharepoint-online>. Acesso em: 19 mai. 2022.

PUPO, Amanda. Nove milhões tiveram problemas ao usar biometria, revela TSE. Exame, 27 out. 2018. Disponível em: <https://exame.com/brasil/nove-milhoes-tiveram-problemas-ao-usar-biometria-revela-tse/>. Acesso em: 18 mai. 2022.

QUELLE, Claudia. Does the Risk-Based Approach to Data Protection Conflict with the Protection of Fundamental Rights on a Conceptual Level? Tilburg Law School Research Paper, 2015.

REPUBLIC OF KENYA IN THE HIGH COURT OF KENYA AT NAIROBI CONSTITUTIONAL & JUDICIAL REVIEW DIVISION CONSOLIDATED PETITIONS NO. 56, 58 & 59 OF 2019, 30 jan 2020. Disponível em: <https://www.khrc.or.ke/publications/214-judgement-on-niims-huduma-namba/file.html>. Acesso em: 16 mai. 2022.

ROUBICEK, Marcelo. Desigualdade de gênero e raça: o perfil da pobreza na crise. Nexo, 25 abr. 2021. Disponível em: <https://www.nexojornal.com.br/expresso/2021/04/25/Desigualdade-de-gênero-e-raça-o-perfil-da-pobreza-na-crise>. Acesso em: 17 mai. 2022.

SAWHNEY, Ria Singh.; CHIMA, Raman Jit Singh.; AGGARWAL.; Naman M. **Busting the dangerous myths of Big ID Programs: cautionary lessons from India**. Access Now Publication, 2021.

SILVA, Priscila Regina. Os direitos dos titulares de dados. *In*: MULHOLLAND, Caitlin (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, p. 195-2015.

SIMITIS, Spiros. (1987). Reviewing Privacy In An Information Society. University Of Pennsylvania Law Review, v. 135, n. 3, 1987. Disponível em: <https://doi.org/10.2307/3312079>. Acesso em: 17 mai. 2022.

SOLANO, Joan Lopez *et al.* Digital disruption or crisis capitalism? Technology, power and the pandemic. Tilburg Institute for Law, Technology, and Society, 2022. Disponível em: <https://globaldatajustice.org/wp-content/uploads/2022/05/Global-Data-Justice-Digital-disruption-or-crisis-capitalism-03-2022.pdf>. Acesso em: 25 mai. 2022.

SPINA, Alessandro. A Regulatory Mariage de Figaro: risk regulation, data protection, and data ethics. European Journal of Risk Regulation , n. 8, v. 1, 88-94, 2017.

SUDRÉ, Lu. At least 124 trans people killed in Brazil in 2019: report. Brasil de Fato, São Paulo, 30 de Janeiro de 2020. Disponível em: <https://www.brasildefato.com.br/2020/01/30/at-least-124-trans-people-killed-in-brazil-in-2019-report>. Acesso em: 11 mai. 2022.

SUPREMO TRIBUNAL FEDERAL - STF. Decisão Mandado de Segurança 36.150 Distrito Federal, 17 dezembro 2021. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15349322719&ext=.pdf>. Acesso em: 18 mai. 2022.

TELESÍNTESE. Transformação digital do governo em desequilíbrio, diz TCU. 06 dez. 2021. Disponível em: <https://www.telesintese.com.br/transformacao-digital-do-governo-em-desequilibrio-diz-tcu/>. Acesso em: 19 mai. 2022.

THORSTENSEN, Vera; ZUCHIERI, Amanda Mitsue. Governo Digital no Brasil: o Quadro Institucional e Regulatório do País sob a Perspectiva da OCDE. Working Paper 529 – CCGI Nº 24 - FGV, 2020. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/29177/TD%20529%20-%20CCGI_24.pdf?sequence=1&isAllowed=y>. Acesso em: 11 mai. 2022

TRIBUNAL DE CONTAS DA UNIÃO - TCU. **TCU avalia governança das estratégias de transformação digital da Administração Pública Federal**. 04 ago.2021. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-avalia-governanca-das-estrategias-de-transformacao-digital-da-administracao-publica-federal.htm>. Acesso em 12 de mai. de 2022

TRIBUNAL SUPERIOR ELEITORAL - TSE. Biometria. [s.l.], s.d. Disponível em: <https://www.tse.jus.br/eleitor/biometria>. Acesso em: 18 mai. 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. Guia orientativo : aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral, Brasília: Tribunal Superior Eleitoral, 2021a. Disponível em: <https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/guia-orientativo-aplicacao-da-lgpd.pdf>. Acesso em: 18 mai. 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. **Aviso de Pauta: assinatura de acordo visa implementar a Identificação Civil Nacional (ICN)**. 15 mar. 2021b. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/2021/Marco/aviso-de-pauta-assinatura-de-acordo-visa-implementar-a-identificacao-civil-nacional-icn>. Acesso em: 12 mai. 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. TSE institui comissão para gerir o tratamento de inconsistências biométricas do Cadastro Eleitoral. [s.l.], 03 set. 2021c. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/2021/Setembro/tse-institui-comissao-para-gerir-o-tratamento-de-inconsistencias-biometricas-do-cadastro-eleitoral>. Acesso em: 18 maio 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. TSE e CNJ realizam primeira ação para identificar pessoas sem documento nas prisões. [s.l.], 19 out. 2021d. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/2021/Outubro/tse-e-cnj-realizam-primeira-acao-para-identificar-pessoas-sem-documento-nas-prisoes>. Acesso em: 18 mai. 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. Contrato TSE nº85/2021. Contrato de prestação de serviços que entre si celebram o Tribunal Superior Eleitoral e o Serviço Federal de Processamento de Dados - SERPRO. 31 dezembro 2021e. Disponível em: <https://www.tse.jus.br/transparencia-e-prestacao-de-contas/licitacoes-e-contratos/contratacoes-diretas-2021/serpro/ct-85-2021-serpro/rybena_pdf?file=https://www.tse.jus.br/transparencia-e-prestacao-de-contas/licitacoes-e-contratos/contratacoes-diretas-2021/serpro/ct-85-2021-serpro/at_download/file>. Acesso em: 18 mai. 2022

TRIBUNAL SUPERIOR ELEITORAL - TSE. TSE lança nesta terça (8) nova etapa de implementação do Documento Nacional de Identidade (DNI). [s.l], 07 fevereiro 2022a. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/2022/Fevereiro/tse-lanca-nesta-terca-8-nova-etapa-de-implementacao-do-documento-nacional-de-identidade-dni>. Acesso em: 18 mai. 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. Biometria atual por UF. [s.l.], 17 maio 2022b. Disponível em: <https://www.tse.jus.br/eleitor/biometria/biometria-atual-uf>. Acesso em: 18 maio 2022.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 17 mai. 2022.

UNIVERSIDADE DE BRASÍLIA. Relatório técnico: Características e Questões de Pesquisa sobre Gestão de Identidade, 2015. Disponível em: <https://www.justica.gov.br/Acesso/governanca/pdfs/infraestrutura-trecnologica/20150228-mj-ric-rt-caracteristicas-e-questoes-de-pesquisa-sobre-g-i.pdf/view>. Acesso em: 17 mai. 2022.

UNITED NATIONS. A/HRC/39/29: The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights, 03 agosto 2018. Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement>. Acesso em: 18 mai. 2022.

UNITED NATIONS. A/74/48037: Report of the Special rapporteur on extreme poverty and human rights, 11 outubro 2019. Disponível em: <https://www.ohchr.org/Documents/Issues/Poverty/A_74_48037_AdvanceUneditedVersion.docx>. Acesso em: 18 mai. 2022.

VILAS BÔAS, Bruno. Sub-registro de nascimentos cede, mas ainda é desafio no Norte, diz IBGE. Valor, 04 dez. 2019. Disponível em: <https://valor.globo.com/brasil/noticia/2019/12/04/sub-registro-de-nascimentos-cede-mas-ainda-e-desafio-no-norte-diz-ibge.ghtml>. Acesso em: 18 mai. 2022.

WANGHAM, Michelle S, *et al*. Gerenciamento de Identidades Federadas. *In.*: Livro de Minicursos do X Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, 2010, p.1-52. Disponível em: <https://doczz.com.br/doc/384142/mc1--gerenciamento-de-identidades-federadas>. Acesso em: 16 mai. 2022.

WIMMER, Miriam. Limites e Possibilidades para o Uso Secundário de Dados Pessoais no Poder Público: Lições da Pandemia. REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS (RBPP), v. 11, p. 123-143, 2021a. Disponível em: <https://www.publicacoes.uniceub.br/RBPP/article/view/7136>. Acesso em: 18 mai. 2022.

WIMMER, Miriam. Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luis (Org.). Tratado de Proteção de Dados Pessoais. 1ed. Rio de Janeiro: Forense, 2021b, p. 271-288.

ZANATTA, Rafael. A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?. Anais do I Encontro da Rede De Pesquisa Em Governança Da Internet, 2017. Disponível em: <http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf>. Acesso em: 10 mai. 2022.