2021 | MAIO

NOTA TÉCNICA

10 RECOMENDAÇÕES PARA A INTEROPERABILIDADE DE DADOS NA ADMINISTRAÇÃO PÚBLICA

RECOMENDAÇÕES E BOAS PRÁTICAS PARA O SETOR PÚBLICO BRASILEIRO

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

Realização:

Laboratório de Políticas Públicas e Internet - LAPIN

Autoria:

Cynthia Picolo Gonzaga de Azevedo

Eduarda Almeida

Gustavo Henrique Luz Silva

Henrique Bawden

Isabela Maria Rosal Santos

Revisão:

Amanda Espiñeira

José Renato Laranjeira de Pereira

Imagem de Capa:

arturszczybylo, Getty Images Pro

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

lapin.org.br
@lapin.br
/lapinbr
/lapinbr

Quem somos nós

O Laboratório de Políticas Públicas e Internet (LAPIN) é um think tank de composição multidisciplinar com sede na capital federal brasileira. Seu objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade. Para maiores informações sobre nossa atuação, visite nosso site: lapin.org.br.

Sobre esta Nota Técnica

Esse documento é uma contribuição inicial do LAPIN para a discussão atual sobre novos e melhores modelos de compartilhamento e interoperabilidade de dados pessoais pelo setor público brasileiro. O objetivo é considerar algumas das preocupações relativas ao tratamento de dados pela Administração Pública e, a partir disso, apresentar possíveis soluções a serem consideradas para o endereçamento desses problemas na construção de novos marcos normativos sobre o tema. Não se pretende apresentar exaustivamente todas as medidas que devem ser adotadas pelo setor público, mas incitar o desenvolvimento do tema a partir da consideração de questões relacionadas ao cidadão.

Sumário

I - Introdução **5**

II - Histórico Legislativo: Decreto nº 8789/16, Decreto nº 10.046/19, LGPD e Lei nº 14.129/21 **7**

III - Experiências internacionais **11**

IV - Boas práticas e recomendações para Administração Pública brasileira **21**

Conclusão **32**

I - Introdução

A presente Nota Técnica se insere no contexto de busca por modelos de compartilhamento e interoperabilidade de dados na Administração Pública no Brasil que sejam compatíveis com a privacidade e a proteção de dados. Para os fins deste trabalho, adotamos a definição de interoperabilidade de dados como a capacidade dos sistemas de tecnologia, informação e comunicação, e os processos que estes suportam, de compartilhar dados e trocar informações e conhecimento,[1] a partir de mecanismos de compatibilização de acesso e formato.

Instrumentos de interoperabilidade são adotados por setores públicos ao redor do mundo para garantir a prestação de serviços mais eficientes, aproveitar o conhecimento de outras entidades e facilitar o acesso dos cidadãos a tais serviços. Mas, para garantir que esses processos preservem a segurança da informação, a transparência, a proteção de dados e medidas éticas aplicáveis, é necessário que se adotem métodos de gestão de processos e padrões de segurança adequados para compartilhamentos de dados.[2]

O objetivo principal deste documento é apresentar boas práticas e recomendações para o modelo brasileiro de interoperabilidade de dados que se constrói atualmente, principalmente como alternativas ao Decreto nº 10.046/19 e complementos à Lei nº 14.129/21 (Lei do Governo Digital).

Para tanto, esta Nota explora, inicialmente, o **histórico recente de normas emitidas no cenário brasileiro** sobre o tema, com foco no Decreto nº 8.789/16, no Decreto nº 10.046/19, na Lei Geral de Proteção de Dados e na Lei do Governo Digital. Nesse tópico, são apresentados os pontos que devem servir como exemplo para a regulação sobre o tema e os que não devem ser adotados nessa nova normatização.

Em seguida, são apresentadas experiências internacionais de países com iniciativas já implementadas sobre o governo digital e o compartilhamento de dados,

[1] Banco Interamericano de Desarrollo. **El ABC de la interoperabilidad de los servicios sociales - Marco conceptual y metodológico.** 2019. Disponível em: <https://publications.iadb.org/publications/spanish/document/El_ABC_de_la_interoperabilidad_de_los_servicios_sociales_Marco_conceptual_y_metodol%C3%B3gico.pdf>. Acesso em 18 abr. 2021.
[2] Ibid.

em especial **México, Uruguai, Estônia e Holanda**. Esses países foram escolhidos pelo desenvolvimento da matéria em seus setores públicos, seguindo princípios de transparência, proteção e segurança de dados.

Por fim, esta nota traz **recomendações e boas práticas** para o governo brasileiro, como síntese do que foi levantado em outras experiências internacionais e nacionais, além de contribuições doutrinárias e técnicas voltadas a encontrar um equilíbrio entre a eficiência dos serviços públicos e a proteção de direitos e interesses dos cidadãos.

II - Histórico Legislativo: Decreto nº 8789/16, Decreto nº 10.046/19, LGPD e Lei nº 14.129/21

O ordenamento jurídico brasileiro possui três principais normas que dispõem sobre compartilhamento e interoperabilidade de dados na Administração Pública: o Decreto nº 10.046/19, que revogou o Decreto nº 8.789/16, a Lei Geral de Proteção de Dados e a Lei do Governo Digital. Essas normas trazem diretrizes para o tratamento de dados no setor público e os cuidados que devem ser tomados ao se tratar dados pessoais nesses contextos.

Por mais que não esteja mais em vigor, o **Decreto nº 8.789/16** merece atenção por ter sido uma das primeiras normas no ordenamento jurídico nacional a disciplinar o compartilhamento de dados em larga escala no Estado brasileiro. Com o objetivo de "modernizar a administração pública e gerar maior eficiência do Estado",[3] ele extinguiu a necessidade de acordos de cooperação, convênios e instrumentos congêneres para se realizar compartilhamentos de dados na Administração Pública.

A preocupação sobre como esse compartilhamento seria realizado e quais dados seriam compartilhados já existia em seu texto. No entanto, as medidas de proteção aos dados tratados eram frágeis, e expressavam cuidados apenas com o sigilo bancário e fiscal (art. 1º, §1º, e art. 4º, §3º). Além disso, o Decreto nº 8.789/16 previa mecanismos insuficientes de transparência em relação às atividades da Administração Pública e pouca capacidade de controle do cidadão sobre os seus dados.

Em 2019, o **Decreto nº 10.046/19** (doravante referenciado "Decreto") revogou o Decreto nº 8.789/16 e passou a disciplinar o compartilhamento de dados no âmbito da Administração Pública Federal, instituiu o Cadastro Base do Cidadão (CBC) e criou o Comitê Central de Governança de Dados (CCGD).

Sua aprovação se deu em um contexto em que a Lei Geral de Proteção de Dados Pessoais já havia sido aprovada, apesar de, à época, ainda não estar em plena vigência.

[3] Políticas públicas serão monitoradas com compartilhamento de dados entre órgãos do governo. Disponível em: <http://www.blog.saude.gov.br/index.php/servicos/51255-politicas-publicas-serao-monitoradas-com-compartilhamento-de-dados-entre-orgaos-do-governo>. Acesso em 18 abr. 2021.

Essa situação se refletiu no texto do Decreto, que faz menção à LGPD logo em seu preâmbulo. No entanto, suas disposições pecam em vários pontos em questões de proteção de dados pessoais, de forma tão preocupante que levou ao ajuizamento de uma ADI[4] pedindo a extirpação do Decreto do ordenamento jurídico brasileiro.

Podem ser citados como graves problemas existentes no Decreto os níveis de compartilhamento criados nos artigos 4º e 31,[5] a dissonância entre as categorias de dados trazidas no Decreto e o conceito de dados pessoais da LGPD,[6] as confusões conceituais trazidas com a introdução da figura do gestor de dados e sua relação com a do controlador, a possibilidade de acesso excessivamente facilitado a dados do governo sem demonstração da existência de finalidade específica, além de violar a teoria da separação informacional dos poderes, que postula "ser incompatível com a proteção de dados a possibilidade de Administração Pública e o Estado serem concebidos como uma unidade informacional"[7].

O que está previsto no Decreto 10.046/2019 colide em grande medida com a LGPD, e seu conteúdo pode levar a **tratamentos excessivos, ilegais e abusivos** por parte do Estado. Isso se dá principalmente pelo fato de que suas disposições não cumprem com os **princípios** previstos na lei, principalmente os da finalidade, adequação, necessidade, segurança e transparência. Ainda, faltou à Administração se atentar à concretização dos **direitos** dos titulares previstos na LGPD, o que se percebe da falta de previsão de mecanismos para que os titulares de dados exerçam direitos como acesso, verificação e retificação de dados pessoais incorretos.

Posteriormente, a **Lei Geral de Proteção de Dados Pessoais** entra em vigor e, com isso, suas disposições revelam uma série de requisitos para o compartilhamento

---

[4] Ação Direta de Inconstitucionalidade nº 6649/DF.

[5] O art. 4º categoriza o compartilhamento de dados entre órgãos e entidades da Administração Pública em três níveis: (i) compartilhamento amplo; (ii) compartilhamento restrito; e (iii) compartilhamento específico. Em seguida, o art. 31 dispõe que ato do Comitê Central de Governança de Dados estabelecerá as regras de compartilhamento e segurança e, até que seja editado esse ato, o compartilhamento de dados públicos serão categorizados como amplos e aqueles protegidos por norma serão categorizados como específicos.

[6] O Decreto define conceitos de atributos biográficos e biométricos, fatos da vida e dados cadastrais que não são compatíveis com os conceitos de dados pessoais e dados pessoais sensíveis previstos na LGPD.

[7] IACOMINVS. **Separação de poderes informacional**. 2020. Disponível em: https://near-lab.com/2020/10/04/separacao-de-poderes-informacional/. Acesso em 20 fev. 2021.

de informações dentro da Administração Pública envolvendo dados pessoais, previstos nos artigos 25 ao 27 da lei.

Por exemplo, a LGPD determina, no seu art. 25, que os dados em posse do governo deverão ser mantidos em **formato interoperável e estruturado** para o uso compartilhado pelo Poder Público. Em seguida, o artigo 26 da LGPD deixa claro que o compartilhamento de dados entre a Administração Pública deve se ater às finalidades específicas de execução de políticas públicas e de cumprimento de obrigações legais, devendo ser observados os princípios que regem a LGPD, reforçando a ideia de que a norma deve servir como guia na elaboração de uma política de proteção de dados do Estado.

Nesse sentido, os mecanismos de interoperabilidade a serem implementados devem estar em conformidade com a lei no que tange, dentre outros elementos, aos princípios da finalidade, da necessidade e da minimização, de forma a não ser legítimo o tratamento de dados para fins excessivamente amplos, discricionários e não individualizados.

Por último, a **Lei nº 14.129/21** disciplina, entre outras coisas, o modo como o compartilhamento de dados deve ocorrer dentro da Administração Pública, a partir do seu artigo 38. A preocupação com a proteção de dados pessoais é trazida em algumas passagens e é considerada relevante para o processo de permitir a interoperabilidade de dados. Com isso, nota-se que, mesmo de forma incipiente, a Administração busca observar as diretrizes de proteção de dados e cumprir com o disposto na LGPD.

Dessa forma, para além da utilidade que os dados pessoais podem possuir para a criação de políticas públicas, os tratamentos de dados realizados pela Administração Pública devem ser feitos levando em conta a necessidade de mitigação de riscos a direitos fundamentais.

É com base neste cenário que esta Nota Técnica traz recomendações que o LAPIN entende como necessárias para um bom funcionamento do compartilhamento de dados dentro da Administração Pública, levando em conta o direito à proteção de dados pessoais e a autodeterminação informativa dos cidadãos. Para tanto, a seguir, serão exploradas experiências internacionais no tema, a fim de verificar quais

iniciativas foram implementadas e bem aceitas, possibilitando recomendações compatíveis com a prática internacional.

III - Experiências internacionais

A fim de explorar as melhores práticas internacionais na implementação de sistemas de interoperabilidade no setor público, passa-se ao estudo das iniciativas do **México,** do **Uruguai,** da **Estônia** e da **Holanda.** Esses países foram selecionados para a análise pois incorporaram na Administração Pública robustos mecanismos de interoperabilidade que respeitam princípios de proteção de dados, essenciais para o bom desenvolvimento do tema.

México

Primeiramente, destacamos a iniciativa de dados abertos do **México**, que garantiu que todos os dados públicos estivessem disponíveis para os cidadãos no sítio eletrônico do projeto.[8] Nesse site, é possível navegar por diferentes ferramentas criadas a partir dos dados abertos, que vão desde métricas das contratações realizadas pelo governo até informações sobre o turismo nacional. Os dados são disponibilizados em diversos formatos interoperáveis, como XML ou JSON, sendo possível seu download direto do sítio eletrônico estatal[9]. A partir da disponibilização de tais dados, foram criadas iniciativas e ferramentas, como APIs, para garantir e facilitar a interoperabilidade dos dados.

Isso possibilitou o uso de dados não só por outras entidades do governo mexicano, mas também por empresas privadas, o que gerou um diferencial na economia movida a dados do país, principalmente para as pequenas e médias empresas que não teriam acesso a tantas informações. Esse sistema, que trata tanto dados pessoais quanto informações gerais sobre a Administração Pública, conta com uma robusta arquitetura regulatória,[10] que garante eficiência, segurança e

[8] O endereço eletrônico é o <https://www.datos.gob.mx/>.
[9] Inclusive, a nível nacional, também existe uma plataforma de dados abertos (disponível em: https://dados.gov.br/dataset), com disponibilização de dados em formatos equivalentes aos da iniciativa mexicana. O desenvolvimento dessa plataforma é uma excelente medida para o atual momento do governo.
[10] OCDE. **Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use Across Societies**. Capítulo 5. Policy initiatives enhancing data access and sharing.Disponível em: <https://www.oecd-ilibrary.org/sites/276aaca8-en/1/1/1/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book>. Acesso em 18 abr. 2021.

transparência, desenvolvida especialmente após processo de revisão das ações de governo aberto em 2016, que contou com sugestões da Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

Buscando implementar as recomendações da OCDE, o país adotou medidas para efetivar a segurança das informações tratadas,[11] reforçando as normas legais sobre proteção de dados e privacidade, inclusive com a implementação da lei geral de proteção de dados para entidades públicas (*Ley General de Protección de Datos Personales en posesión de Sujetos Obligados*).[12] Esta norma traz diversas regras ao tratamento de dados realizado pelo setor público, como a impossibilidade do tratamento de dados pessoais sensíveis, salvo com o consentimento expresso de seu titular (art. 7), e a necessidade de observar os princípios da legalidade, finalidade, qualidade, lealdade, proporcionalidade, informação e responsabilidade em todos os tratamentos (art. 16).

Mais tarde, a Autoridade Mexicana de Proteção de Dados aprovou as **Diretrizes Gerais de Proteção de Dados Pessoais para o Setor Público** (Diretrizes), detalhando as bases, princípios e procedimentos para garantir o direito à proteção dos dados pessoais em posse do poder público.[13] O documento, que aborda diversas questões envolvendo o tratamento de dados por atores públicos, reforça a necessidade de observância aos princípios de proteção de dados (art. 7)[14] e o dever de estabelecer e manter medidas de segurança de natureza administrativa, física e técnica (art. 55).

Além disso, as Diretrizes dispõem que, para a realização de tratamento de dados pessoais para finalidades diferentes das que motivaram o seu tratamento original, a entidade deverá considerar (i) a expectativa razoável de privacidade do titular com base

---

[11] OCDE. **Open Government Data in Mexico**. Paris, 2018. Disponível em: <https://read.oecd-ilibrary.org/governance/open-government-data-in-mexico_9789264297944-en#page4>. Acesso em 03 mai. 2021.

[12] Disponível em: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>. Acesso em 03 mai. 2021.

[13] Governo do México. **Lineamientos Generales de Protección de Datos Personales para el Sector Público.** (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*) <https://www.gob.mx/cms/uploads/attachment/file/630677/ACT-PUB-19-12-2017.10.pdf>. Acesso em 4 mai. 2021.

[14] Artigo 7º (em tradução livre): Em todo o tratamento de dados pessoais, o responsável deve observar os seguintes princípios orientadores para a proteção dos dados pessoais: I. Legalidade; II. Finalidade; III. Lealdade; 4. Consentimento; V. Qualidade; VI. Proporcionalidade; VII. Informações e VIII. Responsabilidade.

no relacionamento preestabelecido; (ii) a natureza dos dados pessoais; (iii) as consequências, para o titular, do tratamento posterior; e (iv) as medidas adotadas para que o tratamento posterior cumpra as disposições da lei geral de proteção de dados para entidades públicas e das Diretrizes (art. 10).

Ainda, o governo mexicano instituiu a Unidade de Transparência[15] dentro do Ministério da Função Pública[16] (em espanhol, *Secretaría de la Función Pública*) que, dentre outras funções, recebe, processa e organiza procedimentos internos para responder às solicitações de acesso a informações e a dados pessoais, e coordena a formação contínua em questões de transparência, acesso à informação e proteção de dados pessoais.[17] O chefe da Unidade inclusive figura no Guia de Implementação da Política de Dados Abertos do México como o responsável por (i) assegurar a regulamentação sobre transparência, arquivos, dados pessoais ou confidenciais; (ii) implementar processos de proteção e salvaguarda de informações classificadas como reservadas ou confidenciais; e (iii) solicitar critérios de proteção de dados pessoais à autoridade correspondente quando necessário.[18]

Esses avanços influenciaram para que o projeto mexicano se tornasse, inclusive aos olhos da OCDE, uma relevante referência de iniciativa de governo aberto na América Latina, pelas possbilidades geradas a partir da disponibilidade dessas informações, incluindo a criação de mecanismos de interoperabilidade por diversos agentes públicos ou privados.

---

[15] Maiores informações disponíveis em: https://www.gob.mx/sfp/documentos/unidad-general-de-transparencia#:~:text=Tel%C3%A9fono%3A%202000%203000%20ext.,Insurgentes%20Sur%201735%2C%20Col. Acesso em 14 mai 2021.

[16] O Ministério da Função Pública, subordinado ao Poder Executivo Federal, é o encarregado de coordenar, avaliar e fiscalizar o exercício público do governo federal.

[17] Governo do México. **Unidade de Transparência.** Disponível em: <https://www.gob.mx/sfp/documentos/unidad-general-de-transparencia>. Acesso em 4 mai. 2021.

[18] O Guia de Implementação da Política de Dados Abertos foi publicado em 2017 pela Unidade de Governo Digital do Ministério da Função Pública e traz diversas orientações conceituais e técnicas para ajudar no cumprimento dos regulamentos referentes à publicação e uso de dados abertos. Disponível em <https://www.dof.gob.mx/nota_detalle.php?codigo=5507476&fecha=12/12/2017>. Acesso em 4 mai. 2021.

Principais soluções da iniciativa do México
• A adoção de uma boa estrutura digital pelo governo, conjugada com a disponibilização de dados abertos, alavanca a economia, estimula a transparência e a responsabilidade e democratiza o acesso à informação; • Iniciativas complementares do governo e da autoridade de proteção de dados para nortear o tratamento e compartilhamento de dados pessoais pelo poder público, com a observância de princípios como a finalidade, qualidade e proporcionalidade, trazem segurança jurídica, garantem maior confiança dos cidadãos nas ações do Estado e contribuem para um processo mais seguro e protetivo aos titulares de dados; • A disponibilização de dados em diversos formatos interoperáveis e a criação de APIs para viabilizar a interoperabilidade facilitam o acesso a essas informações. Inclusive, tais medidas podem inspirar recomendações no contexto do art. 25 da LGPD, que determina que os dados deverão ser mantidos em formato interoperável e estruturado.

Uruguai

O **Uruguai** é outro país que tem se destacado na América Latina como um líder regional em governo digital,[19] adotando a equidade como princípio orientador.[20] As iniciativas de desenvolvimento da Administração Pública buscam a transformação digital de forma inclusiva e sustentável, para garantir que mais cidadãos tenham acesso aos benefícios da sociedade da informação em igualdade de condições.

Segundo a *Agencia de Gobierno Electrónico y Sociedad de la Información* (AGESIC)[21], um dos componentes principais da plataforma de dados sujeita à interoperabilidade é a **segurança e privacidade dos dados,** que garante mecanismos para que os cidadãos estabeleçam políticas de acesso aos seus dados pessoais e

[19] Uruguay XXI. **Uruguai ascende posições e se consolida como um líder regional no Governo Digital**. Disponível em <https://www.uruguayxxi.gub.uy/pt/noticias/artigo/uruguai-ascende-posicoes-e-se-consolida-como-um-lider-regional-no-governo-digital/>. Acesso em: 26 abr. 2021.

[20] Como disposto em sua *Agenda Uruguay Digital.* Agencia de Gobierno Electrónico y Sociedad de la Información. **Agenda Digital del Uruguay.** Disponível em: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/programas/agenda-digital-del-uruguay>. Acesso em 18 abr. 2021.

[21] A AGESIC é a agência nacional para governo eletrônico e sociedade da informação, com autonomia técnica, mas dependente da Presidência da República Uruguaia.

implementa processos de auditoria.[22] Então, esse modelo esclarece a necessidade de estabelecer um equilíbrio entre a transparência e a segurança e controle de acesso a dados pessoais. Nesse sentido, a **Política de Dados para Transformação Digital**, elaborada pela AGESIC em 2019, elenca diversos princípios gerais e associados ao ciclo de vida dos dados pessoais, chamando a atenção o **Princípio 7 "Compartilhar e usar"**, que dispõe que (em tradução livre)[23]:

> *Os dados deverão ser compartilhados entre entidades públicas de maneira que sejam facilitados o reuso, fornecimento e troca, cumprindo com os padrões de dados, integração e compartilhamento estabelecidos para este fim. As entidades públicas não deverão estabelecer condições financeiras para o intercâmbio de dados entre elas.*
>
> ***Os dados pessoais não poderão ser usados para fins diferentes ou incompatíveis com aqueles que motivaram sua coleta. As fontes dos dados usados deverão ser explicitadas.***

O documento evidencia a preocupação de se proteger os interesses e direitos dos cidadãos frente à gestão de seus dados pela Administração Pública, contribuindo para o aumento no nível de confiança no governo e, consequentemente, para maior eficácia na implementação de estratégias visando uma transformação digital sustentável no país. Esse cuidado é reforçado pela observância do princípio da finalidade na obrigação de que os dados só podem ser tratados para fim determinado previamente, o que impede tratamentos para objetivos secundários e não explícitos.

Por outro lado, a *Unidad Reguladora y de Control de Datos Personales*, departamento da Autoridade Uruguaia de Proteção de Dados Pessoais (órgão descentralizado da AGESIC), emitiu um guia de boas práticas para a coleta digital de dados por entidades públicas. O documento reforça a necessidade de se coletar dados de maneira segura, respeitando o princípio da finalidade, da necessidade e obtendo o consentimento do titular sempre que cabível. Especificamente sobre interoperabilidade, a autoridade recomenda que esta seja executada por meio de

---

[22] Agencia de Gobierno Electrónico y Sociedad de la Información. **Plataforma de Datos**. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/plataforma-datos. Acesso em 18 abr. 2021.

[23] Agencia de Gobierno Electrónico y Sociedad de la Información. **Uruguay: Política de Datos para la Transformación Digital.** Disponível em: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-politica-datos-para-transformacion-digital>. Acesso em 22 abr. 2021.

canais seguros e com consideração prévia aos fundamentos da comunicação de dados, a fim de garantir a qualidade dos dados coletados[24].

Apesar das recomendações mirarem a fase da coleta em ambiente digital, em última análise, o objetivo é que tais dados sejam compartilhados dentro da Administração Pública, desde que observados os princípios de privacidade e proteção de dados desde o início do tratamento.

Principais soluções da iniciativa do Uruguai
• A observância dos princípios da finalidade, da necessidade e da segurança dos dados minimiza as chances de tratamentos excessivos ou ilegais; • A disponibilização de diretrizes claras e pautadas nos princípios de proteção de dados gera maior confiança da população nos tratamentos realizados pelo setor público; • A equidade deve ser princípio norteador na implementação de mecanismos de interoperabilidade, garantindo acesso a dados não apenas para o setor público mas para toda a sociedade, de acordo com diferentes níveis de acesso, que concomitantemente permitam ao titular de dados restringir o acesso a seus dados pessoais, caso entenda necessário e desde que o compartilhamento não seja obrigatório por lei.

Estônia

Na Europa, a **Estônia** é uma referência quando se trata de interoperabilidade de dados no setor público. O país conta com um **sistema descentralizado** em que vários bancos de dados dos setores público e privado são capazes de interagir, de modo que os dados são armazenados de maneira não duplicada e só precisam ser solicitados ao

[24] Unidad Reguladora y de Control de Datos Personales. **Buenas prácticas en protección de datos personales para el uso de formularios por entidades públicas.** Disponível em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/buenas-practicas-proteccion-datos-personales-para-uso-formularios>. Ver também página destinada à plataforma de interoperabilidade uruguaia em: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/interoperabilidad>. Acesso em 20 abr. 2021.

cidadão uma vez[25] (princípio *once-only*, ou "apenas uma vez").[26] A ferramenta que garante esse compartilhamento de dados dos diversos sistemas de informação é a ***X-Road***, plataforma *open-source* implementada em 2001.[27] Por ser de código aberto, permite também um escrutínio da população quanto ao seu código-fonte, garantindo maior transparência e confiabilidade.

Diversas características fazem desse sistema um ambiente seguro, padronizado, confiável e eficaz para compartilhamento de dados. Por exemplo, (**i**) o usuário do *X-Road* é quem decide quais dados em seu poder serão compartilhados; (**ii**) é possível implementar uma estrutura de autorização para gerenciar direitos de acesso a fim de proteger de acesso não autorizado; (**iii**) a integridade dos dados é mantida graças à tecnologia *blockchain*;[28] (**iv**) terceiros não podem alterar os dados durante o processo de compartilhamento; (**v**) a confidencialidade dos dados é assegurada durante o trânsito por meios de canais criptografados; (**vi**) as mensagens enviadas pelo *X-Road* são padronizadas, protegidas e assinadas digitalmente, podendo inclusive serem usadas como provas em processos judiciais; e (**vii**) todas as alterações de configurações são certificadas, garantindo maior transparência aos usuários.[29] Além disso, o *X-Road* conta com um robusto sistema de segurança, permite interoperabilidade em caráter transfronteiriço e pode ser acessado

---

[25] O Capítulo 5, § 43 (2) da **Lei de Informação Pública da Estônia** inclusive proíbe o estabelecimento de bancos de dados separados para dados já coletados. Disponível em: <https://www.riigiteataja.ee/en/eli/529032019012/consolide>. Acesso em 5 maio. 2021.

[26] Não obstante os benefícios gerados como otimização de tempo e redução de custos, o princípio do "apenas uma vez", por operacionalizar o reuso de informações dos cidadãos pela Administração Pública, desafia o princípio da finalidade, devendo, portanto, ser implementado com as devidas salvaguardas que garantam a proteção de dados pessoais, como gerenciamento de autorização e transparência sobre o uso de dados. TUPAY, Paloma K. **Estonia, the Digital Nation: Reflections of a Digital Citizen's Rights in the European Union**. EDPL, vol. 6, n. 2, p. 294-300. 2020. Disponível em: <https://www.lexxion.eu/wp-content/uploads/2020/07/EDPL_Estonia_extended.pdf>; European Data Protection Supervisor. **Opinion 8/2017 on the proposal for a Regulation establishing a single digital gateway and the 'once-only' principle.** Disponível em: <https://edps.europa.eu/sites/default/files/publication/17-08-01_sdg_opinion_en_0.pdf>. Acesso em 10 mai. 2021.

[27] Autoridade do Sistema de Informação da Estônia (Riigi Infosüsteemi Amet). **X-Road.** Disponível em: <https://www.ria.ee/et/riigi-infosusteem/andmevahetuskiht-x-tee.html>. Estônia e Finlândia criaram, em 2017, o Instituto Nórdico de Soluções de Interoperabilidade (NIIS), que é o atual responsável pelo desenvolvimento do X-Road. Disponível em: <https://www.niis.org/>. Acesso em 18 abr. 2021.

[28] Comissão Europeia. **Case Study Report: e-Estonia.** Disponível em: <https://jiip.eu/mop/wp/wp-content/uploads/2018/10/EE_e-Estonia_Castanos.pdf>. Ver também **e-Estonia Security and Safety.** Disponível em: <https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/>. Acesso em 4 maio 2021.

[29] Autoridade do Sistema de Informação da Estônia (*Riigi Infosüsteemi Amet*). **X-Road.** Disponível em: <https://www.ria.ee/et/riigi-infosusteem/x-tee/miks-eelistada-x-teed.html>. Acesso em 5 mai. 2021.

independentemente da tecnologia usada.[30]

Principais soluções da iniciativa da Estônia
• A utilização de plataforma de código aberto permite maior escrutínio da população, maior transparência e confiabilidade nos tratamentos realizados; • A definição de direitos de acesso garante maior proteção contra acessos não autorizados; • Devem existir mecanismos para assegurar a integridade dos dados, inclusive certificações de alteração de configuração; • Para garantir um bom nível de organização de processos e de gestão da informação, é essencial a padronização e proteção das formas de compartilhamento.

Holanda

A **Holanda,** por sua vez, apresenta um sistema com diversas salvaguardas que minimizam os riscos de compartilhamento de dados. No país, organizações com funções públicas e sociais podem acessar dados pessoais contidos no **Banco de Dados de Registros Pessoais** (*Basisregistratie Personen* - BRP), que é alimentado pelos municípios.[31] O Serviço Nacional de Dados de Identidade (*Rijksdienst voor Identiteitsgegevens* - RvIG), que gerencia o BRP e é responsável pelos sistemas técnicos de armazenamento e intercâmbio de dados pessoais,[32] explica que o BRP é como um sistema de e-mail fechado, em que as organizações devem seguir certos procedimentos para que o RvIG possa verificar se elas atendem aos requisitos legais, técnicos e organizacionais para acesso aos dados.[33]

Além desse controle operacional, o BRP é submetido às regras tanto do Regulamento Geral de Proteção de Dados Europeu (RGPD) quanto da Lei de Registro Básico de Pessoas (Lei BRP), sendo a Autoridade Holandesa de Proteção de Dados a

[30] ibid. Nordic Institute for Interoperability Solutions, **X-Road Technology Overview.** Disponível em: <https://x-road.global/x-road-technology-overview>. Ver também o vídeo institucional **X-Road Introduction**. Disponível em: <https://www.youtube.com/watch?v=9PaHinkJlvA>. Acesso em 18 abr. 2021.
[31] Serviço Nacional de Dados de Identidade (RvIG). **O BRP como um registro básico.** Disponível em: <https://www.rvig.nl/brp/brp-als-basisregistratie>. Acesso em 22 abr. 2021.
[32] O RvIG faz parte do Ministério do Interior e das Relações do Reino da Holanda.
[33] Serviço Nacional de Dados de Identidade (*Rijksdienst voor Identiteitsgegevens* - RvIG). **BRP**. Disponível em: <https://www.rvig.nl/brp>. Acesso em 22 abr. 2021.

responsável pela supervisão e cumprimento dessas normas.[34]

As **diretrizes de funcionamento do BRP** colocam o titular de dados em evidência, **oferecendo diversas garantias à privacidade e à proteção de dados**. Destacam-se, entre elas[35]:

I. Apenas os dados **necessários à finalidade pretendida** pela organização são disponibilizados, sendo necessária uma autorização específica do Ministério do Interior e das Relações do Reino da Holanda para *compartilhamento sistemático* de dados pessoais, que determinará as categorias de dados pessoais, os dados a serem fornecidos e em quais casos isso ocorrerá;[36]
II. A fim de evitar o uso indevido dos dados, é mantido um **registro de quem consulta ou altera os dados** no BRP;
III. Os dados são sempre armazenados **criptografados**;
IV. A Lei BRP, em seu artigo 2.7, **elenca exatamente quais dados são incluídos no sistema** como, por exemplo, nome, data de nascimento, filiação, residência, cônjuge e informações que indiquem onde os dados foram obtidos ou a base jurídica sob a qual os dados foram incluídos no sistema;[37]
V. As autoridades municipais devem conduzir **investigações periódicas** sobre a estrutura, funcionamento e segurança do cadastro de dados, bem como sobre o tratamento dos dados pessoais, e informar a Autoridade Holandesa de Proteção de Dados dos resultados;[38]
VI. **O titular pode solicitar gratuitamente informações** à autoridade municipal sobre quando e quais organizações tiveram acesso aos seus dados, sendo prevista uma resposta em até 4 semanas.[39]

---

[34] Governo da Holanda. **Basisregistratie Personen (BRP)**. Disponível em: <https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/basisregistratie-personen-brp>. Acesso em 22 abr. 2021.
[35] Ibid.
[36] Lei BRP, art. 3.2 (4). Disponivel em: <https://wetten.overheid.nl/BWBR0033715/2019-02-03#Hoofdstuk2>. Já foram emitidas autorizações para, por exemplo, províncias, ministérios, administradores de pensões e hospitais. Ver **BRP Decisions.** Disponível em: <https://publicaties.rvig.nl/Besluiten_en_modelautorisaties/Besluiten/BRP_besluiten>. Acesso em 5 mai. 2021.
[37] Lei BRP, art. 2.7. Disponível em: <https://wetten.overheid.nl/BWBR0033715/2019-02-03#Hoofdstuk2>. Acesso em 22 abr. 2021.
[38] Ibid. Art. 4.3 (2).
[39] Governo da Holanda. **Quem receberá meus dados do Banco de Dados de Registros Pessoais (BRP)?** Disponível em:

Principais soluções da iniciativa da Holanda
● Apenas os dados necessários à finalidade pretendida devem ser disponibilizados; ● O compartilhamento sistemático de dados pessoais exige maior escrutínio; ● Além da autorização para acesso, é importante manter um registro de quem consultou os dados; ● Técnicas de criptografia devem ser utilizadas no armazenamento de dados pessoais; ● É necessário definir concretamente, sem termos vagos, quais dados serão incluídos no sistema interoperável; ● Auditorias precisam ser realizadas para acompanhar os processos de compartilhamento e interoperabilidade, devendo os resultados serem encaminhados à Autoridade de Proteção de Dados competente para apreciação e recomendação de medidas adicionais; ● É imprescindível a disponibilização gratuita de orientações claras que permitam aos titulares de dados o exercício de seus direitos.

<https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/vraag-en-antwoord/wie-krijgen-mijn-persoonsgegevens-uit-brp>. Acesso em 22 abr. 2021.

IV - Boas práticas e recomendações para Administração Pública brasileira

Diante do exposto, passa-se à elaboração de recomendações e boas práticas para a Administração Pública brasileira na interoperabilidade e compartilhamento de dados. Como grande norte para isso, podemos citar a **teoria da privacidade contextual,** que visa superar a noção de que existem dados que *a priori* devem ou não ser protegidos[40] e que isso seria o caminho para que se concretizasse o direito à privacidade.

De acordo com essa noção, o acesso a cada informação deveria levar em conta o **contexto** em que o fluxo informacional estivesse ocorrendo. Com isso, para cada contexto, diferentes regras devem ser levadas em conta para garantir que o processamento de dados seja suficientemente protetivo e seguro, levando em consideração critérios tais como: quem solicita o acesso ao dado; qual a finalidade da solicitação; qual o período de acesso ao dado; políticas de eliminação e descarte, etc . Para tanto, defende-se que a forma mais efetiva de proteção deve assegurar que o fluxo de dados pessoais estabelecido respeite as expectativas de privacidade dos indivíduos e da sociedade. Isso se dá a partir da aplicação das medidas de proteção e segurança adequadas a cada tratamento de dados, demonstrando a necessidade da sua realização para a finalidade desejada como meio de legitimação e avaliando o contexto em que o tratamento se insere.

Nesta visão, o que se deve buscar não é a proibição de compartilhamento de certas categorias de dados, ou uma maneira única a qual possibilitaria que os entes do governo compartilhassem suas informações em si. Pelo contrário, o que se pretende é construir um modelo de compartilhamento que entenda como cada tratamento de dados poderá afetar os direitos de privacidade e autodeterminação informativa dos cidadãos. Nesse sentido, cumpre realizar um juízo sobre qual o risco é aceitável frente aos possíveis danos que podem ocorrer com determinado acesso a dados, levando em conta o contexto em que o tratamento é realizado, os atores, a

[40] NISSENBAUM, Helen. **Privacy as Contextual Integrity**. Washington Law Review, v. 79, 2004. Disponível em: <https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf>. Acesso em 20 fev. 2021.

informação e o modo de transmissão.

Em que pesem as falhas e os riscos elencados nesta Nota Técnica em relação ao Decreto nº 10.046/19, **a interoperabilidade estatal e as iniciativas de Governo Digital não podem ser consideradas problemáticas por si só.** Tais medidas podem auxiliar a transformar e modernizar o governo brasileiro no oferecimento de políticas públicas e serviços essenciais aos cidadãos com maior qualidade, acessibilidade e simplicidade.

Contudo, essas iniciativas devem seguir princípios essenciais à proteção de dados, em especial os princípios da finalidade, adequação, necessidade, transparência e segurança, seguindo boas práticas, como aquelas destacadas das experiências do México, Uruguai, Estônia e Holanda demonstraram ser possível.

O primeiro passo é a construção de um mecanismo de interoperabilidade dentro da Administração Pública mais atento à proteção de dados pessoais e à privacidade dos cidadãos. Essa nova normativa deve servir como tecnologia de construção e operação de políticas públicas,[41] pois a normatização é apenas uma das etapas necessárias para a sua efetividade, não a última.[42]

Logo, para além da construção de normas, é necessário que se adote medidas concretas para a construção de uma política de compartilhamento de dados pessoais dentro do Estado, que devem ser pensadas, implementadas e avaliadas com estrito respeito à legalidade e observância aos direitos fundamentais, em especial à privacidade, à proteção de dados e à autodeterminação informativa.

Recomendação 1: Normativo específico para os entes do art. 4º, III, da LGPD

A **primeira recomendação** é sobre a limitação de escopo do compartilhamento de dados dentro da Administração Pública. O compartilhamento de dados com os entes constantes no art. 4º, inciso III, da LGPD, envolvendo segurança pública, defesa nacional, segurança do Estado e atividades de

[41] COUTINHO, D. **O direito nas políticas públicas**. In: MARQUES, E. A política pública como campo disciplinar. São Paulo: Unesp, 2013. p. 193.
[42] SUXBERGER, A. H. G. **O Direito nas Políticas Públicas: o Déficit de Efetividade dos Direitos é um Problema Normativo ou Institucional**? In: _____ Direitos Humanos e Democracia: estudos em homenagem ao Professor Vital Moreira. Rio de Janeiro: Lumen Juris, 2018. p. 122.

investigação e repressão de infrações penais, incluindo a Agência Brasileira de Inteligência - ABIN, devem ser regidos por normativo específico.

Devem ser aplicadas restrições e medidas de segurança diferenciadas em relação ao resto da Administração Pública, devido à própria natureza da atividade desses agentes. As medidas aqui propostas não são o bastante para lidar com os riscos que podem surgir nas atividades realizadas por essas organizações. É necessário que se crie um modelo específico para o compartilhamento com eles.

Recomendação 2: Implementar uma solução *Privacy By Design*

A **segunda recomendação** a ser dada é que, qualquer que seja o *framework* de interoperabilidade construído pelo Estado Brasileiro, ele deve ser montado tendo em vista a aplicação da metodologia de ***Privacy By Design***, isto é, a adoção dos princípios da privacidade e da proteção de dados desde a concepção do projeto. Isso evitará uma série de problemas na construção do modelo de interoperabilidade, já que a adoção desta metodologia colocará a privacidade dos indivíduos como preocupação central no desenvolvimento do serviço, não sendo apenas um adendo a ser feito posteriormente.

O *Privacy by Design* é composto por sete princípios que devem nortear a construção e o funcionamento de serviços e produtos (e, em último caso, de organizações) na temática de proteção de dados pessoais.[43] Eles são plenamente aplicáveis na concepção do mecanismo de interoperabilidade da Administração Pública.

O primeiro deles é o "Proativo, não reativo, Preventivo, não Remedial", que propõe que as medidas de privacidade sejam integradas de tal modo a evitar futuros problemas, como vazamentos ou uso excessivo de dados. Isso significaria que o mecanismos de interoperabilidade devem ser pensados em uma lógica de impedir que problemas ocorram, não de criar mecanismos que apenas mitiguem o dano caso haja algum tipo de evento adverso envolvendo dados pessoais.

---

[43] CAVOUKIAN, Ann. **Privacy by Design: The 7 Foundational Principles**. Information & Privacy Commissioner, Canada. 2009. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em 05 mai. 2021.

O segundo princípio, que é o "Privacidade como Padrão", conversa inclusive com o que a LGPD dispõe, no art. 46, §2º[44], e com a Lei nº 14.129/21, no art. 38, inciso III[45] e art. 39, parágrafo único.[46] O funcionamento conforme a legislação de proteção de dados pessoais deve ser o modo de funcionamento padrão dessa ferramenta.

Os princípios de "Foco no Usuário" e o "Privacidade dentro do Design de Soluções" correm conjuntamente no caso de mecanismos de interoperabilidade. É necessário trazer o usuário e a sua privacidade como preocupações centrais no processo de elaboração do modelo de interoperabilidade de dados, pensando o design e o funcionamento da ferramenta a partir do cidadão e do cuidado que se deve ter com os dados dele. Uma ferramenta que ao fim e ao cabo permita a violação dos direitos de privacidade e autodeterminação informativa do cidadão não cumpre a sua função final: melhorar a vida do cidadão ao proporcionar um melhor funcionamento da máquina estatal.

A "Segurança de Ponta-a-Ponta" e "Visibilidade e Transparência" são princípios que trazem a necessidade de se pensar a segurança dos produtos e serviços do início ao fim, deixando claro para o usuário como os seus dados são tratados. Pode-se interpretar em dois sentidos esses princípios no caso concreto: a necessidade de que o processo de criação da ferramenta seja transparente do início ao fim, garantindo que a sociedade alerte sobre possíveis falhas no projeto; e a visibilidade de como os dados pessoais dos cidadãos são manipulados, mostrando os riscos e medidas de segurança adotadas em cada compartilhamento, que devem abarcar o

---

[44] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os 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.
(...)
§ 2º **As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.**

[45] Art. 38. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos detentores ou gestores de bases de dados, inclusive os controladores de dados pessoais, conforme estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), deverão gerir suas ferramentas digitais, considerando:
(...)
III - a proteção de dados pessoais, observada a legislação vigente, especialmente a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

[46] Art. 39.(...)
Parágrafo único. Aplicam-se aos dados pessoais tratados por meio de mecanismos de interoperabilidade as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

tratamento como um todo. Nesse sentido, a adoção de uma solução em código aberto, que permita auditoria pela sociedade é uma boa prática a ser adotada. Assim, a implementação desses princípios podem aproximar a arquitetura brasileira da iniciativa da Estônia, que, a partir de mecanismos de transparência, permite maior escrutínio da população e confiabilidade nos tratamentos realizados.

Por fim, complementando todos os anteriores,o princípio de "Visão ganha-ganha da Privacidade". Fazer com que o serviço ou produto cumpra o seu objetivo ao mesmo tempo que garante a segurança dos dados pessoais e a autodeterminação informativa dos indivíduos é a melhor das situações possíveis. No caso de mecanismos de interoperabilidade de dados, isto se reflete em um serviço público prestado com melhor qualidade ao mesmo tempo que respeita os direitos dos cidadãos, promovendo direitos fundamentais e cumprindo com os ditames constitucionais de direito administrativo.

Recomendação 3: Adotar o princípio da prevenção

A **terceira recomendação** pensada é a concretização do princípio da **prevenção**, previsto no art. 6º, inciso VIII, da LGPD, como uma diretriz central para o funcionamento do compartilhamento de dados. Esse fundamento possibilita a compreensão dos riscos de um tratamento e os potenciais malefícios oriundos de tal atividade, o que permite tomada de decisões informadas[47].

A sua concretização passaria pela adoção de protocolos de segurança sempre que necessário, a partir de uma interpretação emprestada do princípio da precaução do Direito Ambiental.[48] Assim, será possível definir casos em que o tratamento de

---

[47] BIONI, B.; LUCIANO, M. **O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada?.** 2019.

[48] De forma analógica, "O direito ambiental e o moderno movimento de proteção ao meio ambiente e defesa da sustentabilidade têm uma grande preocupação com a chamada ética intergeracional e o futuro."; ANTUNES, Paulo de Bessa. **Os princípios da precaução e da prevenção no direito ambiental**. Enciclopédia jurídica da PUCSP, 2020. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/330/edicao-1/os-principios-da-precaucao-e-da-prevencao-no-direito-ambiental>. Acesso em 05 mai. 2021.
Para uma visão do princípio da precaução aplicado à proteção de dados pessoais, vide BIONI, Bruno & LUCIANO, Maria. **O Princípio Da Precaução Na Regulação De Inteligência Artificial: Seriam As Leis De Proteção De Dados O Seu Portal De Entrada?** Disponível em https://brunobioni.com.br/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC%83O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf

dados deve ser evitado, tendo em vista elevado risco de danos irreparáveis à sociedade, mesmo que se implemente medidas robustas de mitigação de risco.

Recomendação 4: Registro de compartilhamentos e elaboração de documentos conforme a LGPD

A **quarta recomendação** versa sobre as integrações com o sistema do Governo Digital. Podemos citar a **obrigatoriedade de mapeamento** dos tratamentos de compartilhamento de dados pessoais e, quando necessária, a elaboração prévia ao tratamento de um Relatório de Impacto à Proteção de Dados Pessoais (**RIPD**), para que seja autorizada a integração com a ferramenta de interoperabilidade, além da existência de um programa de conformidade com a regulação de proteção de dados, com um encarregado já nomeado.

O mapeamento dos fluxos de dados, inclusive de compartilhamentos, é passo essencial para adequação às regras de proteção de dados pessoais e também para a verificação do princípio da finalidade, uma vez que através desse processo será possível definir o fim pretendido com cada coleta de dados. Isso deve ser feito preferencialmente com possibilidade de controle do cidadão por meio de um portal ou aplicativo de fácil manuseio e acesso. Além disso, aproveitando a experiência holandesa, o mapeamento deve ser complementado com auditorias periódicas para confirmar a precisão desse processo. Os resultados devem ser encaminhados para a ANPD para apreciação e avaliação de adoção de medidas adicionais.

Recomendação 5: Adotar regime de transição

Recomendamos também a criação de um **regime de transição**[49] para viabilizar a adequação da Administração Pública e seu bom funcionamento. Tal regime criaria marcos de adequação com a LGPD que a Administração Pública teria que alcançar em data determinada para que possa continuar a realizar o compartilhamento de dados, ainda que em períodos em que não esteja em completa conformidade com a LGPD. Deste modo, seriam implementados gradualmente mecanismos de controle e

[49] Conforme previsto no art. 7º do Decreto nº 9.830/19, "Quando cabível, o regime de transição preverá:
I - os órgãos e as entidades da administração pública e os terceiros destinatários;
II - as medidas administrativas a serem adotadas para adequação à interpretação ou à nova orientação sobre norma de conteúdo indeterminado; e
III - o prazo e o modo para que o novo dever ou novo condicionamento de direito seja cumprido."

segurança, de forma a não alterar bruscamente os processos internos da Administração, impedindo um potencial rompimento das atividades estatais, ao mesmo tempo que se evitariam violações a direitos de titulares de dados e também sanções à Administração Pública pela ANPD. É importante que os passos desse regime de transição sejam publicizados, de modo a garantir transparência no processo de transformação do setor público.

A implementação desses passos de adequação à LGPD deve ser condição indispensável para que entes governamentais possam aderir ao sistema de interoperabilidade e compartilhamento de dados pessoais no âmbito da Administração Pública. **Deve-se garantir que todo órgão cumpra tais procedimentos, sob pena de não poder fazer parte da sistemática de interoperabilidade**. Essa é uma forma interessante para incentivar os órgãos públicos a observarem os instrumentos de segurança da informação e das comunicações a fim de evitar incidentes de segurança, como ataques *hacker* e vazamentos de dados. Além disso, esta previsão gera maior controle sobre quem tem acesso aos dados, ou seja, somente órgãos com autorização, que estejam adequados com a LGPD, poderão acessar os dados.

Recomendação 6: Permitir a fiscalização pela ANPD e pela sociedade

Entende-se necessária também a **inclusão da Autoridade Nacional de Proteção de Dados (ANPD) e de agentes da sociedade civil em todo o processo** de estudo, criação, estruturação, implementação e avaliação da interoperabilidade no âmbito da Administração Pública. A participação desses entes, seja com um papel de supervisão ou de aconselhamento, auxilia no bom desenvolvimento da ferramenta de interoperabilidade.

Recomendação 7: Aplicar práticas de anonimização, quando possível

Além disso, recomendamos a adoção de ferramentas de **anonimização** de dados sempre que a identificação do titular seja dispensável para atingimento da finalidade do tratamento de dados, como uma forma de minimizar os riscos atrelados ao tratamento de dados e os danos de um potencial incidente de segurança. Os dados anonimizados podem ser úteis e suficientes para análises estatísticas e de

formulação de políticas amplas à sociedade brasileira, não sendo necessária a identificação individualizada dos cidadãos.

Ressalta-se que esse processo é diferente de adoção de mecanismos de criptografia e da pseudonomização. Se houver qualquer possibilidade de correlação entre um dado criptografado e outro dado pessoal, estaremos diante de processos de pseudonimização.

Recomendação 8: Obrigatoriedade de treinamento de pessoal

Concomitante a isso, é interessante que seja determinada a obrigatoriedade de realização de **treinamentos e adoção das práticas recomendadas nos guias e documentos** operacionais já publicados de adequação à LGPD, elaborados pela Secretaria de Governo Digital, nas demandas identificadas de interoperabilidade, que, a despeito de poderem ser aprimoradas, servem como um pontapé inicial para a Administração Pública. Além disso, a partir do debate agora em desenvolvimento, outros documentos mais adequados poderão ser publicados, garantindo que essa prática de capacitação dos agentes seja contínua. Com isso, será estabelecida uma cultura de proteção de dados entre os órgãos que acessam dados pessoais por meio de instrumentos interoperáveis.

Essas medidas não são apenas uma burocracia que causa lentidão, que inviabilizaria trocas rápidas de informação dentro da Administração Pública, mas sim recomendações que visam **concretizar os princípios de proteção de dados**, principalmente os de finalidade, adequação e necessidade durante a realização de tratamentos de dados pessoais pelo Estado.

Inclusive, como ilustrado pela arquitetura mexicana, iniciativas de dados abertos podem alavancar a economia, desde que seja garantida transparência, responsabilidade e acesso à informação de forma democratizada. O que se quer coibir aqui são compartilhamentos que violem a Lei Geral de Proteção de Dados Pessoais, evitando, assim, tratamentos de dados discriminatórios e abusivos, e também à Lei de Acesso à Informação, que busca garantir maior transparência ao funcionamento do Poder Público. Essa preocupação em respeitar as regras de proteção de dados colocará o Brasil em destaque no tema de governo digital, uma vez

que isso é uma preocupação da comunidade internacional, inclusive da OCDE, como disposto nesta Nota Técnica.

Recomendação 9: Desenvolver procedimentos para o atendimento dos direitos dos titulares

Ainda, é fundamental que a Administração desenvolva **procedimentos facilitados para o atendimento dos direitos dos titulares**, principalmente de acesso, atualização, retificação e oposição de tratamento de informações pessoais. Esses mecanismos são essenciais para concretização de direitos de cidadãs e cidadãos, garantindo a autodeterminação informativa. Dessa forma, as práticas de interoperabilidade podem ser instrumentos para promoção de eficiência estatal. Porém, se utilizadas de forma isolada e não observados os princípios de proteção de dados, não necessariamente este objetivo será atingido, pois esses dados estarão vulneráveis a incidentes de segurança e ao uso para finalidades inadequadas.

Recomendação 10: Proibir o compartilhamento de dados biométricos

Por fim, recomenda-se a proibição do compartilhamento de dados biométricos até a edição de um Decreto específico para regulamentar e trazer salvaguardas e proibições expressas e específicas sobre o compartilhamento desses tipos de dados sensíveis. Os riscos inerentes ao tratamento de dados biométricos é muito alto, portanto, também propõe-se a elaboração obrigatória e prévia de RIPD para adequadamente documentar e sopesar os riscos envolvidos no compartilhamento.

10 recomendações para a interoperabilidade de dados na Administração Pública	Descrição
1. Normativo específico para os entes do art. 4º, III, da LGPD	O compartilhamento de dados com os entes constantes no art. 4º, inciso III, da LGPD, envolvendo segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, incluindo a Agência Brasileira de Inteligência - ABIN, devem ser regidos por normativo específico.
2. Implementar uma solução *Privacy By Design*	Aplicar os sete princípios de *Privacy by Design* no processo de criação da ferramenta de compartilhamento e interoperabilidade de dados da Administração Pública.
3. Adotar o princípio da prevenção, previsto no art. 6º, inciso VIII, da LGPD	Tornar o princípio da prevenção uma diretriz central para o funcionamento do compartilhamento de dados, inclusive definindo casos em que o tratamento de dados deve ser proibido devido ao risco, mesmo que se implemente medidas para mitigação do risco.
4. Registro de compartilhamentos e elaboração de documentos conforme a LGPD	Mapear todos os compartilhamentos de dados realizados pela Administração Pública, com a elaboração de RIPDs caso se mostre necessário.
5. Adotar regime de transição	Criar um regime de transição que permita a implementação gradual de padrões mínimos de proteção de dados pessoais para viabilizar o compartilhamento de dados.
6. Permitir a fiscalização pela ANPD e pela sociedade	Incluir ANPD e atores da sociedade civil na criação da ferramenta de interoperabilidade para garantir transparência, segurança e *accountability*.
7. Aplicar práticas de anonimização, quando possível	Adotar a anonimização de dados pessoais como prática a ser utilizada sempre que possível.

8. Obrigatoriedade de treinamento de pessoal	Ministrar treinamentos em proteção de dados pessoais na Administração Pública como um todo, de modo a promover, em relação a todo o corpo de servidores, uma mentalidade protetiva a esse direito fundamental.
9. Desenvolver procedimentos para o atendimento dos direitos dos titulares	Construir mecanismos de fácil compreensão e acesso que permitam a concretização dos direitos dos titulares previstos no art. 18 da LGPD em qualquer situação.
10. Proibir o compartilhamento de dados biométricos	Tendo em vista os inerentes altos riscos envolvidos no tratamento de dados biométricos, recomenda-se a edição de um decreto que disponha de salvaguardas e proibições específicas relacionadas ao compartilhamento de dados biométricos.

Conclusão

A interoperabilidade é ferramenta essencial para possibilitar o compartilhamento de dados pessoais na Administração Pública e assim garantir o desenvolvimento de serviços e políticas públicas mais eficientes. Contudo, a criação e a aplicação dos mecanismos necessários para assegurar esse importante passo para a estruturação de um governo digital deve seguir os princípios de proteção de dados, em especial os da finalidade, necessidade, adequação, segurança e transparência.

Além disso, outras técnicas relacionadas à privacidade também devem ser observadas nesse momento, como a adoção de mecanismos de anonimização e procedimentos para concretização dos direitos do titular. Para tanto, é necessário garantir a participação de entidades da sociedade civil e da própria ANPD na evolução do governo digital, para que as técnicas de interoperabilidade adotadas sigam a metodologia do *Privacy By Design* e a ideia de precaução de riscos e danos.