ORGANIZAÇÃO
Bruno Bioni, Hana Mesquita, Johanna K. Monagreda e Rafael Zanatta

CONSTRUINDO CAMINHOS PARA A JUSTIÇA DE DADOS NO BRASIL: O PAPEL DAS DEFENSORIAS PÚBLICAS NA PROTEÇÃO DE DADOS PESSOAIS

EDITORA
Associação Data Privacy Brasil de Pesquisa

DataPrivacyBR Research

Organização:
Bruno Bioni, Hana Mesquita, Johanna K. Monagreda, Rafael Zanatta

Construindo caminhos para a justiça de dados no Brasil: o papel das Defensorias Públicas na proteção de dados pessoais

São Paulo
1ª edição
2022

Editora: ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA

Editora: ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA
São Paulo
1ª edição
2022
ISBN: 978-65-997956-0-2

Projeto gráfico e Edição: Roberto Junior
Revisão: Eduardo Mendonça, Hana Mesquita e Johanna K. Monagreda
Capa: Roberto Junior

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Construindo caminhos para a justiça de dados no Brasil [livro eletrônico] : o papel das defensorias públicas na proteção de dados pessoais / organização Bruno Bioni ... [et al.]. -- 1. ed. -- São Paulo : Associação Data Privacy Brasil de Pesquisa, 2022.
PDF.

Outros organizadores : Hana Mesquita, Johanna K. Monagreda, Rafael Zanatta.
Vários autores.
Bibliografia.
ISBN 978-65-997956-0-2

1. Direito à privacidade - Brasil 2. Proteção de dados - Direito - Brasil 3. Proteção de dados - Leis e legislação 4. Proteção de dados pessoais I. Bioni, Bruno. II. Mesquita, Hana. III. Monagreda, Johanna K. IV. Zanatta, Rafael.

22-112792 CDU-342.721(094.56)

Índices para catálogo sistemático:

1. Proteção de dados pessoais e da privacidade : Leis : Comentários : Direito 342.721(094.56)

Aline Graziele Benitez - Bibliotecária - CRB-1/3129

FICHA TÉCNICA

O **Data Privacy Brasil** é um espaço de intersecção entre a escola Data Privacy Ensino e a Associação Data Privacy Brasil de Pesquisa. Este livro digital foi produzido exclusivamente pela Associação Data Privacy Brasil de Pesquisa, entidade civil sem fins lucrativos sediada em São Paulo.

A organização dedica-se à interface entre proteção de dados pessoais, tecnologia e direitos fundamentais, produzindo pesquisas e ações de incidência perante o sistema de Justiça, órgãos legislativos e governo. A partir de uma Política de Financiamento Ético e Transparência, a associação realiza pesquisas de interesse público que buscam reforçar a gramática de direitos fundamentais e ampliar a cultura de proteção de dados pessoais no Brasil e no Sul Global. A Associação integra a Coalizão Direitos na Rede, a Rede-Iberoamericana de Proteção de Dados Pessoais e o Conselho Consultivo da Sociedade Civil da Sociedade da Informação (CSISAC) da Organização para Cooperação e Desenvolvimento Econômico (OCDE). A Associação Data Privacy Brasil de Pesquisa também representa a sociedade civil perante o Conselho Nacional de Proteção de Dados Pessoais da Autoridade Nacional de Proteção de Dados (ANPD).

Este livro digital faz parte do projeto “Expandindo o papel das Defensorias Públicas na proteção de dados pessoais”, executado com apoio da Fundação Ford.

Para mais informações sobre a organização, impacto de seus projetos e como pesquisas são apoiadas, visite www.dataprivacybr.org.

PROJETO

Expandindo o papel das defensorias públicas na proteção de dados pessoais no Brasil

ORGANIZAÇÃO

Bruno Bioni, Hana Mesquita, Johanna K. Monagreda e Rafael Zanatta

APOIO

Fundação Ford

DIRETORES

Bruno Bioni e Rafael Zanatta

COORDENADORAS GERAIS DE PROJETO

Mariana Rielli e Marina Meira

LÍDER DE PROJETO

Johanna K. Monagreda

EQUIPE DE PESQUISA

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

ANALISTA DE INCIDÊNCIA

Vinícius Silva

ADMINISTRATIVO E COMUNICAÇÃO

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

IMPRENSA

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

SUMÁRIO

APRESENTAÇÃO

O livro digital *"Construindo caminhos para a justiça de dados no Brasil: o papel das Defensorias Públicas na proteção de dados pessoais"* representa um dos exitosos frutos colhidos ao longo da caminhada de dois anos do projeto "Expandindo o papel das Defensorias Públicas na proteção de dados pessoais no Brasil".

Iniciado em 2020, com o apoio da Fundação Ford, o projeto nasceu a partir do reconhecimento de que as Defensorias Públicas desempenham um papel fundamental na concretização de direitos. Em um país profundamente marcado por desigualdades sociais e assimetrias de poder como o Brasil, a missão constitucional das Defensorias Públicas significa um compromisso real com a população socioeconomicamente vulnerável.

Tendo em mente este compromisso, a Associação Data Privacy Brasil de Pesquisa atuou ao lado da instituição com o objetivo de fortalecer as Defensorias Públicas com conhecimentos e instrumentos para proteger dados pessoais, tanto *internamente*, através de fortes programas de governança de dados, quanto *externamente*, através da atuação individual e em litígios estratégicos envolvendo direitos coletivos.

Encerrada a primeira fase do projeto, o presente livro digital marca uma virada na compreensão da proteção de dados pessoais como um instrumento de justiça, sendo necessário incorporar, nas reflexões sobre proteção de dados e direitos digitais, preocupações sobre equidade, emancipação, justiça social e transformação estrutural.

Esperamos que aproveitem a leitura.
Associação Data Privacy Brasil de Pesquisa

PREFÁCIO

LUCIANA GROSS CUNHA[1]

O modelo de assistência jurídica no sistema de justiça brasileiro, adotado pela Constituição Federal, se destaca pela ousadia de ter um órgão *permanente e essencial à função jurisdicional do Estado cuja finalidade é a promoção dos direitos humanos e a defesa dos direitos individuais e coletivos, de forma integral e gratuita*[2]. Assumir essa responsabilidade de forma tão abrangente, em um país marcado por relações patriarcais, racistas, com enormes desigualdades sociais e altíssimas concentrações de renda, não é pouca coisa. A ousadia dos constituintes foi ainda mais longe quando, em 2009 o Legislativo, ao definir as regras de criação das Defensorias Públicas nos estados, previu *a Ouvidoria-Geral como órgão auxiliar da Defensoria Pública do Estado, de promoção da qualidade dos serviços prestados pela Instituição*[3]. Diante de tais dispositivos, não há dúvidas de que a finalidade na persecução do interesse público das Defensorias Públicas, da forma como descrita pela Lei Geral de Proteção de Dados (LGPD) é a proteção dos direitos dos seus usuários[4]. Mas o que isso quer dizer quando os serviços prestados pela Defensoria Pública envolvem os dados pessoais dos seus usuários, ao mesmo tempo que o funcionamento da Defensoria Pública e a melhoria da qualidade dos seus serviços dependem desses dados?

1 Professora da Fundação Getúlio Vargas (FGV) Direito SP. Mestre e Doutora em Ciência Política pela Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo FFLCH/USP. Membra do Conselho Consultivo da Ouvidoria Geral da Defensoria Pública do Estado de São Paulo. Desenvolve pesquisas sobre a performance das instituições do sistema de justiça e sua conexão com o ambiente político, administração da justiça e acesso à justiça.

2 Constituição Federal, artigo 134, *caput*.

3 Lei Complementar nº 132/2009, artigo 105-A, *caput*.

4 Lei nº 13.709/2018, o artigo 23, *caput*.

Esses são alguns dos desafios enfrentados pelas Defensorias Públicas diante da necessidade de se adequar à LGPD. Responder a essas perguntas é buscar conciliar os objetivos da administração pública no âmbito da administração da justiça, tendo como mote a defesa e proteção dos dados de cidadãos brasileiros, que em sua maioria se encontram em situação de exclusão social, econômica e digital. Assim como as demais instituições do sistema de justiça brasileiro, a Defensoria Pública desde a metade da década de 2000, vem passando por avanços consideráveis no que diz respeito à produção de informação e na transparência e responsividade dos serviços prestados. Esse processo tem sido organizado a partir de dois pressupostos: de um lado, o reconhecimento de que a informação é uma ferramenta de gestão fundamental na avaliação e construção de projetos de melhoria da prestação do serviço público de justiça; de outro, é que esse processo depende de um diálogo contínuo com a sociedade civil, seja quanto às demandas dos movimentos sociais, seja na prestação de contas, por meio da publicidade dos mecanismos de tomada de decisão e dos dados resultantes acerca das suas atividades.

Tais pressupostos foram impactados de maneira significativa pela LGPD, em vigor desde 2020. Do lado da produção de informação e sua utilização na gestão para a melhoria da qualidade do serviço público foi impactado pela maior responsabilidade das Defensorias como órgão da administração pública, no uso de dados pessoais para a execução da política pública da justiça e a necessidade de adequação aos requisitos impostos pela LGPD no tratamento desses dados. Isso quer dizer que a coleta, o tratamento, leitura e uso das informações contendo dados pessoais, que importam nos atendimentos dos usuários das Defensorias Públicas, assim como aconteceu nos demais órgãos da administração pública que também fazem uso de dados pessoais, tiveram que ser reestruturados no sentido de garantir os direitos preservados pela LGPD. Disso depende não somente a revisão e reestruturação desses processos, mas também o treinamento e capacitação de todos os atores envolvidos, desde o corpo administrativo que atua nas atividades-meio da Defensoria Pública, até os atendentes, defensores públicos e integrantes dos órgãos diretivos da instituição.

Os princípios e as regras que organizam a proteção de dados, de acordo com a LGPD, também impactaram as instâncias e os mecanismos de diálogo com a sociedade civil, no que diz respeito à transparência das atividades desenvolvidas pela Defensoria Pública, principalmente levando-se em conta o compromisso da instituição ao assumir a participação da Ouvidoria, como instância mediadora das

demandas da sociedade civil e dos movimentos sociais direcionadas para a Defensoria, e como espaço de sugestões, reclamações e elogios aos serviços prestados por ela. Isso sem falar na atividade fim da Defensoria Pública, de defesa judicial e extrajudicial de uma população cada vez mais numerosa, de excluídos em um país assolado pela crise econômica, social e política, que ganhou contornos de tragédia humanitária com a chegada da pandemia de Covid-19.

Dentro da perspectiva da justiça de dados, na linha proposta por Linnet Taylor, de que a proliferação e difusão de informações pessoais em uma sociedade digitalizada tem como resultado uma maior (in)visibilidade e discriminação de diferentes setores da sociedade[5], a atuação especializada da Defensoria Pública nessa área é complexa e urgente. Complexa, pois trata-se de uma área na qual ainda temos pouco conhecimento sobre quais e como funcionam os instrumentos capazes de coletar e classificar essas informações. Urgente, pois na ausência de diagnósticos sobre como esses instrumentos operam, estamos diante da possibilidade de geração de maior (in)visibilidade e discriminação de grande parte da população.

A Ação Civil Pública na qual as Defensorias Públicas do Estado de São Paulo e da União, em conjunto com associações da sociedade civil organizada, pediram a suspensão da implantação do reconhecimento facial pela Companhia do Metropolitano de São Paulo, com base na LGPD, entre outros diplomas legais, é ilustrativo da insegurança jurídica e do potencial de violações que a manipulação de dados pode gerar, e a importância da atuação das Defensorias na proteção da privacidade e do livre desenvolvimento da personalidade, além do exercício da cidadania[6]. Nesta ação, que teve a liminar concedida em parte, o tribunal reconheceu que o uso de dados biométricos, sem o consentimento dos seus titulares e o conhecimento dos *critérios, condições e propósitos da implementação do sistema de reconhecimento facial*, pode causar prejuízos irreversíveis, atingindo os direitos fundamentais dos cidadãos. Tratando-se dos usuários das Defensorias Públicas que, em sua maioria fazem parte a grupos já vulnerabilizados pelas suas condições sociais e econômicas, este exemplo é ainda mais significativo já que o uso de dados pessoais significa também intensificar discriminações raciais e de gênero, a partir

5 Taylor, L. What is data Data Justice? The Case for Connecting Digital Rights and Freedoms Globally (June 26, 2017). Disponível em **http://dx.doi.org/10.2139/ssrn.2918779**. Acessado em março, 2022. A tradução desse artigo realizada por Gabriela Vergili, Hana Mesquita e Pedro Saliba, está disponível na presente publicação.

6 Ação Civil Pública nº 1010667-97.2022.8.26.0053.

de imagens de controle[7].

Ter sido convidada para prefaciar o livro organizado pela Associação Data Privacy Brasil de Pesquisa, resultado do projeto Defensorias e Proteção de Dados é uma oportunidade de falar do tema do acesso à justiça que pauta os meus trabalhos, desde o início da minha trajetória acadêmica, ainda nos anos 1990, levando em consideração obstáculos e desafios que não vislumbrava. Os avanços tecnológicos, a digitalização da justiça e os atendimentos e processos que passaram a ser digitais, principalmente depois da nossa experiência de confinamento social, diante da pandemia de Covid-19, entre 2020 e 2021, representam uma nova realidade na administração da justiça e, de forma ainda mais intensa no exercício do acesso à justiça. Como direito fundamental básico, que garante os demais direitos, o acesso à justiça sob a perspectiva da justiça de dados, mesmo com os avanços que passamos quanto à gestão de dados pelas instituições do sistema de justiça, ganha novos contornos para os quais essa obra que agora, o leitor tem acesso, de maneira muito instigante e elucidativa, ilumina.

Trazendo dois artigos acadêmicos fundamentais – O que é justiça de dados? Conectando direitos digitais e liberdades globalmente, de Linnet Taylor, com tradução de Gabriela Vergili, Hana Mesquita e Pedro Saliba; e Presa na rede de proteção social: Privacidade, gênero e justiça de dados no Programa Bolsa Família, de Mariana Valente, Natália Neris e Nathalie Fragoso -, passando pelo material coletado e analisado durante o desenvolvimento do projeto –Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD, de Bruno Bioni, Marina Kitayama e Rafael Zanatta; e Relatório de Discussões da Oficina Prática de Adequação à LGPD – Defensorias Públicas e Proteção de Dados, de Bruno Bioni, Hana Mesquita e Rafael Zanatta -; e tratando de temas como o papel central desempenhados pelas Defensorias no sistema de justiça, no que diz respeito à LGPD; a necessidade do consentimento no uso de dados pessoais por parte dos usuários da Defensoria, dentro de uma política de promoção da cultura de proteção de dados; e da prerrogativa de requisição das Defensorias no âmbito da Justiça de dados, essa publicação é na minha perspectiva, que venho acompanhando a evolução dos estudos sobre acesso à justiça e o processo de institucionalização das Defensorias no país, uma ótima chance para darmos visibilidade e quem sabe promover maior igualdade por meio do Direito. Muito obrigada pelo convite e boa leitura a todos e todas.

7 Collins, P. H. Pensamento Feminista Negro. Conhecimento, Consciência e a Política do Empoderamento. São Paulo: Ed. Boitempo, 2019.

O QUE É JUSTIÇA DE DADOS?

CONECTANDO DIREITOS DIGITAIS E LIBERDADES GLOBALMENTE

O QUE É JUSTIÇA DE DADOS? CONECTANDO DIREITOS DIGITAIS E LIBERDADES GLOBALMENTE

LINNET TAYLOR[1]

TRADUÇÃO

Gabriela Vergili, Hana Mesquita e Pedro Saliba[2]

REVISÃO

Mariana Rielli[3] e Johanna K. Monagreda[4]

1 Linnet Taylor é Professora de Governança Internacional de Dados no Tilburg Institute for Law, Technology and Society (TILT), onde lidera o projeto de justiça Global de Dados financiado pelo European Research Council (ERC), procurando compreender as diferentes perspectivas a nível mundial sobre o que constitui um tratamento justo através das tecnologias de dados. A sua pesquisa gira em torno da utilização de novas fontes de dados digitais na governança e de questões de desenvolvimento humano e econômico. Anteriormente foi bolsista de pesquisa Marie Curie na faculdade de Desenvolvimento Internacional da Universidade de Amsterdã, e pesquisadora de pós-doutorado no Oxford Internet Institute. É doutora em Desenvolvimento Internacional pelo Instituto de Estudos de Desenvolvimento, da Universidade de Sussex.

2 Gabriela Vergili é bacharela em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Advogada e pesquisadora no Data Privacy Brasil desde 2019, e com a formalização da Associação Data Privacy Brasil de Pesquisa, atuou no projeto Os Dados e o Vírus, e atualmente integra o projeto Novas Fronteiras dos Direitos Digitais, gabriela@dataprivacybr.org. **Hana Mesquita** é advogada e pesquisadora na área de proteção de dados e novas tecnologias. Graduada pela Pontifícia Universidade Católica do Rio de Janeiro e integrante do grupo de pesquisa Legalite - PUC-Rio. É pesquisadora da Associação Data Privacy Brasil de Pesquisa desde junho de 2021, hana.mesquita@dataprivacybr.org. **Pedro Saliba** é advogado e sociólogo, mestre em Sociologia e Antropologia pelo PPGSA/UFRJ. Pesquisas na interseção entre proteção de dados pessoais e poder público, especialmente na área de segurança e vigilância. Foi pesquisador do Laboratório de Estudos Digitais (LED/UFRJ) e atualmente trabalha como pesquisador na Associação Data Privacy Brasil desde setembro de 2020, pedro.saliba@dataprivacybr.org.

3 Mariana Rielli é advogada e pesquisadora com trajetória no terceiro setor, especificamente nas áreas de direitos digitais e direitos humanos em geral. Graduada em Direito pela Universidade de São Paulo (USP), desenvolveu diversos projetos de pesquisa e extensão relacionados a essas temáticas, como o Laboratório de Liberdades da Faculdade de Direito da USP, do qual foi coordenadora. Atuou como assessora de pesquisa e advocacy no Centro de Referência Legal da ARTIGO 19 Brasil entre 2014 e 2018 e foi consultora da Alianza por la Libre Expresión e Información. Integra no Data Privacy Brasil desde março de 2019 e, a partir da formalização da Associação Data Privacy Brasil de Pesquisa, passou a coordenar o projeto Observatório da Privacidade e Proteção de Dados e também a integrar a Coordenação geral de projetos da ONG, mariana@dataprivacybr.org.

4 Johanna K. Monagreda é Doutora e Mestre em Ciência Política pela Universidade Federal de Minas Gerais. Licenciada em Ciência Política e Administrativa pela Universidad Central de Venezuela. Líder de projeto na Associação Data Privacy Brasil de Pesquisa. Sua área de atuação inclui pesquisas em direitos humanos, políticas de igualdade racial e políticas para mulheres na América Latina, johanna.monagreda@datprivacybr.org.

RESUMO

A crescente disponibilidade de dados digitais como reflexo do desenvolvimento econômico e humano - e em particular a disponibilidade de dados derivados da utilização de dispositivos e serviços tecnológicos - tem implicações políticas e práticas para a forma como as pessoas são vistas e tratadas pelo Estado e pelo setor privado. No entanto, a revolução dos dados é até agora majoritariamente técnica: o poder dos dados de classificar, categorizar e intervir ainda não foi explicitamente ligado a uma agenda de justiça social pelas autoridades envolvidas. Enquanto isso, embora a discriminação orientada por dados avance num ritmo semelhante ao das tecnologias de processamento de dados, os mecanismos para combatê-la e a conscientização da sociedade a respeito não têm acompanhado. Este artigo postula que, assim como uma ideia de justiça é necessária para estabelecer o Estado de direito, uma ideia de justiça de dados – justeza na forma como as pessoas são visibilizadas, representadas e tratadas como resultado da produção de dados digitais - é necessária para determinar caminhos éticos num mundo datificante. Ao reunir as emergentes perspectivas acadêmicas sobre este tema, proponho três pilares como fundamento de uma noção internacional de justiça de dados: (in) visibilidade, (des)engajamento com a tecnologia e não-discriminação. Esses pilares integram direitos e liberdades positivos com direitos e liberdades negativos e, ao fazê-lo, desafiam tanto a base das atuais regulações de proteção de dados quanto a crescente presunção de que ser visível através dos dados que produzimos faz parte do contrato social contemporâneo.

PALAVRAS-CHAVE

Privacidade, ética, desenvolvimento, discriminação, representação, vigilância

Introdução: A questão da justiça de dados

À medida que ocorre a disponibilização de dados digitais sobre populações que anteriormente eram invisíveis digitalmente, agentes públicos, políticos e pesquisadores de todo o mundo estão se beneficiando do que a ONU denominou "revolução dos dados" (Nações Unidas, 2014). A crescente disponibilidade de dados digitais que refletem o desenvolvimento econômico e humano, em particular a chamada "fumaça dos dados" ou *data fumes* (Thatcher, 2014) - isto é, dados produzidos como subproduto da utilização de dispositivos e serviços tecnológicos - está provocando uma mudança de paradigma na elaboração de políticas públicas, que deixam de ser informadas por dados (*data informed*) para se tornarem orientadas por dados (*data driven*) (Kitchin, 2016). Essas fontes granulares de dados, que permitem a pesquisadores inferir os movimentos, atividades e comportamento das pessoas apresentam implicações éticas, políticas e práticas para a forma como as pessoas são vistas e tratadas pelo Estado e pelo setor privado (ou ambos agindo conjuntamente).

Esta visibilidade distribuída tem implicações sociais e políticas ainda mais claras no caso de populações de baixa renda, sobre as quais a capacidade das autoridades públicas de coletar e reunir dados estatísticos costumava ser limitada. No entanto, a revolução dos dados é até agora primariamente técnica: o poder dos dados para classificar, categorizar e intervir ainda não foi explicitamente vinculado a uma agenda de justiça social pelas agências e autoridades que coletam, geram e utilizam dados. Tampouco existe um nível de conscientização elevado entre agentes de políticas públicas sobre como as novas tecnologias orientadas por dados podem não ser neutras em termos de acesso, utilização ou impactos, conforme demonstram pesquisas sobre este fenômeno (Dalton *et al.*, 2016). Na realidade, enquanto a discriminação orientada por dados avança em um ritmo semelhante ao de tecnologias de processamento de dados, a conscientização e os mecanismos para combatê-la não.

Duas tendências tornam urgentemente necessário o desenvolvimento de uma perspectiva global de utilização justa de dados digitais: uma é o aumento exponencial da adoção de tecnologia em todo o mundo, e a outra é a correspondente globalização de *data analytics*[5]. Dos sete bilhões de telefones celulares no mundo,

5 N.T.: De acordo com o *Information Commissioner's Office* (ICO), autoridade independente do Reino Unido para a defesa de proteção de dados, "*data analytics*" representa o processo de análise de dados

5,5 bilhões estão em países de baixa e média renda (LMICs), nos quais 2,1 bilhões de pessoas também estão online (UIT, 2015). A Índia e a China encomendaram a criação de centenas de cidades inteligentes (smart cities) que vão habilitar o monitoramento e rastreamento de cidadãos e cidadãs em todos os aspectos das suas vidas (Greenfield, 2013), registros digitais e biométricos estão se tornando a nova norma até mesmo nos países mais pobres, e as práticas de ajuda internacional e humanitária e desenvolvimento cada vez mais empregam grandes quantidades de dados digitais para mapear, organizar e intervir massivamente nas regiões de baixa renda (Taylor, 2015). O alcance do mercado global de dados também mudou para levar em conta estas novas fontes de dados, com empresas multinacionais competindo para traçar os perfis de bilhões de potenciais novos consumidores (Taylor, 2016a). Enquanto isso, pesquisa e prática sobre como a datificação pode servir à cidadania, liberdade e justiça social são ínfimas em comparação com a habilidade das empresas e do Estado de utilizar os dados para intervir e influenciar.

Este artigo postula que, assim como uma ideia de justiça é necessária para estabelecer o Estado de direito, uma ideia de *justiça de dados* é necessária para determinar caminhos éticos em um mundo datificado. Diversos enquadramentos de justiça de dados estão emergindo em diferentes áreas e têm o potencial de se aprimorar reciprocamente. Assim, analisarei o trabalho já produzido sobre justiça de dados e posicionarei os diferentes pontos de vista em diálogo entre si para, em seguida, argumentar que, ao encontrarmos princípios comuns, nós podemos uni-los em um único enquadramento para debate e pesquisa posteriores.

Este artigo estrutura-se da seguinte forma: primeiramente, irei delinear os motivos para preocupação com as novas interfases público-privado no uso de *Big Data*, nomeadamente a natureza disciplinar e frequentemente discriminatória de grandes bases de dados empregadas a nível populacional. Depois, utilizarei exemplos empíricos para demonstrar que tais preocupações não são apenas ampliadas, mas fundamentalmente diferentes em um contexto de *Big Data*. Irei então explorar os atuais enquadramentos de justiça e dados e identificar quais aspectos decorrentes do *Big Data* eles se propõem a endereçar. A seguir, proporei um conceito de justiça de dados abrangente que possa conectar as abordagens existentes e formar uma base de diálogo entre elas. Finalmente, defenderei a Abordagem das

que ocorre por meio da utilização de software para identificar automaticamente padrões em conjuntos de dados (quando esses conjuntos de dados contêm dados pessoais) e utilizá-los para fazer previsões, classificações ou classificações de risco. Disponível em: **https://ico.org.uk/for-organisations/toolkit-for--organisations-considering-using-data-analytics/**. Acessado em 07 de fevereiro de 2022.

Capacidades (*Capabilities Approach*) de Sen e Nussbaum como um enquadramento teórico para esta proposta de conceito, com o objetivo de fornecer uma abordagem ecossistêmica que possa endereçar instituições, mercados, sistemas jurídicos e o debate público.

Uma nota sobre a metodologia: as premissas teóricas e empíricas da formulação aqui proposta são baseadas em um projeto de pesquisa que compreende trabalho de campo, observação e entrevistas conduzidas durante o período de 2012 a 2016. Este projeto incluiu 200 entrevistas formais e informais e períodos de observação conduzidos com pesquisadores acadêmicos, organizações humanitárias e de desenvolvimento, desenvolvedores de tecnologia independentes, organizações ativistas no campo de dados e direitos, grandes empresas de tecnologia e agentes públicos dos Estados Unidos, União Europeia e de diversos países da África e da Ásia. A parte de observação da pesquisa foi conduzida em eventos internacionais relevantes para o movimento "*Responsible Data*", por meio da participação em grupos consultivos e de discussões públicas sobre ética de dados. As entrevistas foram conduzidas nestes eventos e, adicionalmente, por meio de trabalho de campo realizado durante 2014-2016 em operadoras multinacionais de redes telefônicas na França e na Noruega e em um projeto de datificação do setor público em Bangalore, Índia.

O problema: dados na interfase público-privado

Por que procurar maneiras de relacionar preocupações com justiça social e datificação, e vice versa? Por que não, por exemplo, priorizar a garantia de que a inovação comercial e digital possa prosseguir sem restrições, visto que há argumentos sobre os seus benefícios para a sociedade, ou que dados apoiem a eficiência no setor público, servindo aos interesses da cidadania e da segurança pública? Ambos questionamentos foram feitos por atores do setor privado (Fórum Econômico Mundial, 2011) e setor público (Comissão Europeia, 2016) em discussões de alto nível. O que há em relação aos impactos sociais de dados digitais que sugere que uma agenda de justiça social é importante? Por um lado, os impactos de *Big Data* são muito diferentes dependendo da posição socioeconômica de uma pessoa. O trabalho de Gilliom (2001) e, mais recentemente, de acadêmicos como Eubanks (2014) e Masiero (2016) mostram que o grande fardo da vigilância

de dados (vigilância que utiliza meios digitais) sempre foi suportado pelos pobres. Sistemas burocráticos projetados para assegurar que pessoas não façam mau uso de fundos estatais de bem-estar social e outros auxílios fornecidos pelo poder público são parte do aparelho de governamentalidade (Lemke, 2001); a aplicação da lei orientada por dados foca de forma desigual em bairros pobres que vivenciam certos tipos de criminalidade (O'Neil, 2016); e migrantes sem registro são rastreados e abordados por meio de sistemas digitais de maneiras mais invasivas do que viajantes com alta renda (Taylor, 2015).

Para além do status socioeconômico, marcadores de gênero, etnia e local de origem também auxiliam a definir a quais bases de dados pertencemos, como estes sistemas usam nossos dados e que tipos de influência eles podem ter sobre nós. A obra de Kang sobre tráfico (2015), por exemplo, mostra como a vigilância dos comportamentos e movimentos de mulheres por autoridades internacionais contra o tráfico e trabalho sexual tem sido historicamente moldada por metodologias e tipos de expertise muitos distintos, a depender da origem e grupo étnico de cada sujeito, de forma que tipos diferentes de dados alimentam o sistema internacional de diferentes regiões, com variação correspondente na conceituação de quem deveria ser o sujeito foco das medidas anti-tráfico e programas de controle e disciplina contra o trabalho sexual. Do mesmo modo, a pesquisa de Moore e Currah (2015) sobre como pessoas transgêneras têm sido tratados em bases de dados populacionais nos Estados Unidos mostra que a habilidade de se identificar legalmente como um gênero diferente depende significativamente de sua fonte de renda. A obra de Jiwani (2015) sobre cidadania e conformidade também demonstra as formas como a vigilância como um "processo social ativo" reforça barreiras sociais e estruturais.

Ademais, estes problemas se interseccionam e multiplicam nas fronteiras criadas pela conexão e surgimento de conjuntos de dados. Esta interseccionalidade (Cho *et al.*, 2013) nos efeitos da datificação é um componente importante do argumento a favor de uma perspectiva de justiça social. Uma variedade de características interligadas - raça, etnia, religião, gênero, localização, nacionalidade, *status* socioeconômico - determinam como indivíduos se tornam sujeitos de direito por meio do uso de seus dados e, consequentemente, como estes dados podem ser empregados por agentes decisórios, empresas ou ambos para definir ações que os impactam. Por sua vez, a possibilidade de uma pessoa ser identificada como alvo de vigilância multiplica-se dependendo do número de categorias de interesse a que ele pertença.

Por exemplo, uma adolescente parte de uma família imigrante, vivendo em uma região de baixa renda, cujos pais são pobres e que pertence a uma minoria étnica e religiosa, está exponencialmente mais suscetível a ser alvo de vigilância, tanto por autoridades protetivas (serviços sociais), quanto preventivas (polícia). E, provavelmente, também terá menos oportunidades de resistir a essa vigilância ou a intervenções do que suas amigas que moram em regiões economicamente favorecidas e que pertencem à maioria étnica da região.

Sistemas de dados serem discriminatórios não é novidade. Muito menos que eles tendem a reforçar desvantagens em relação àqueles já marginalizados ou excluídos socialmente, ou que estas mesmas pessoas são as que encontram maiores obstáculos ao buscar reparação. A evidência disto está bem documentada e não necessariamente demanda uma nova conceituação de justiça de dados - todos têm direito a ser tratados de forma justa por todas as autoridades públicas (e privadas). Contudo, com relação às atuais implicações da datificação para a justiça social, o que exige uma atenção especial é a particular dinâmica contemporânea em que métodos de coleta e análise de dados não são mais facilmente separáveis entre "voluntários" (pesquisas diretas ou outra forma de coleta de dados administrativos em que a pessoa está ciente de que seus dados estão sendo agrupados) *versus* "outros" (vigilância digital via aparelhos e sensores). Para a adolescente vigiada descrita no exemplo anterior, o problema se multiplica quando as funções de coleta e análise de dados passam a ser divididas entre autoridades públicas e empresas privadas que fornecem seu celular, seu acesso à internet ou os aplicativos que ela usa. A ''economia da vigilância'' também tem implicações sobre questões de representação justa e acesso a serviços, dado que o acesso à tecnologia crescentemente determina quem pode ser visto: Shearmur (2015) alertou que aqueles que usam *Big Data* para estudar comportamentos ou modelar políticas públicas não veem a sociedade, mas "usuários e mercados".

A interfase público-privado é importante porque muito do que entendemos como funções do setor público (contar, categorizar e servir às necessidades de cidadãos e cidadãs) são, na verdade, realizadas pelo setor privado, com implicações correspondentes para transparência e prestação de contas (*accountability*). O número de cientistas de dados no poder público equipados para analisar *Big Data* é pequeno em comparação com o número de burocratas interessados no que o Big Data pode informar, o que faz com que a datificação do governo seja (e sempre será) executada primariamente pelo setor privado. Ilustrativamente, o delator Edward Snowden foi funcionário da empresa de consultoria Booz Allen

Hamilton quando executava serviços de vigilância para as agências de inteligência dos Estados Unidos. Isto sugere que os mercados são um fator central para estabelecer e ampliar as assimetrias de poder relacionadas aos dados digitais, e que novas estratégias e enquadramentos podem ser necessários para endereçar a interfase público-privado e determinar se as tecnologias baseadas em dados nos servem ou nos controlam.

Em resposta a este problema, dentro de diferentes campos tem emergido a defesa de uma conceituação dos nossos direitos relacionados a dados que seja mais ampla e orientada pela justiça social. Conforme dados populacionais se tornam subprodutos do capitalismo informacional, surgem consequências tanto em relação às maneiras pelas quais podemos ser monitorados, quanto às possibilidades de reparação se formos submetidos a tratamento injusto. Isto porque as ferramentas legais e de representação democrática que proporcionam a possibilidade de reparação quando dados são utilizados de forma inadequada são cada vez menos aplicáveis conforme os dados começam a fluir mais livremente entre os atores do setor privado e público. Responsabilização e prestação de contas (*accountability*) se tornam vagas, por um lado, porque cada ator pode deslocar a responsabilidade para os demais e, por outro, porque a vigilância se torna indireta e invisível, fazendo com que as pessoas sejam menos capazes de identificar as relações entre danos sofridos e dados.

A interfase público-privado envolvida na coleta de dados em larga escala, e o seu engajamento inevitável com o mercado global de dados, levanta questões fundamentais sobre como direitos podem ser assegurados ao longo de diferentes fronteiras e sistemas jurídicos, e até sobre se direitos individuais devem ser o único instrumento usado para combater danos causados por dados (Taylor *et al.*, 2017). Uma importante mudança é que a relação de vigilância (ou monitoramento) - que sustenta várias outras funções dos dados, frequentemente positivas - não ocorre mais ‘’de um para um’’, com um alvo e geografia fixos, mas sim de ‘’muitos para muitos’’, de forma virtual e com objetivos que podem mudar de estatais para privados, e vice versa. Um panóptico (Foucault, 1977) em que a vigilância contínua leva as pessoas a modularem seu próprio comportamento não é mais a metáfora mais útil para a vigilância contemporânea datificada, que é invisível e plural, operando por meio de uma infinidade de plataformas. Ao invés de censurar nosso comportamento para satisfazer os nossos observadores, acidentalmente nos tornamos visíveis, por meio do nosso comportamento diário, a uma enorme variedade de atores, desde corporações que criam os dispositivos e sistemas que usamos,

os prestadores de serviços que facilitam a criação e disseminação de conteúdo, até *data brokers* que rastreiam nossa atividade nestes dispositivos e sistemas, e a infinidade de consumidores dos seus produtos, que incluem governos, empresas de marketing, agências de inteligência e partidos políticos. Mesmo quando a autocensura é um objetivo de um sistema tecnológico (como é o caso do esquema de crédito social chinês, desenhado para criar comportamentos dos cidadãos e cidadãs que se alinhem com as prioridades governamentais (Creemers, 2016), pode ser argumentado que não é realista que as pessoas permaneçam constantemente em um estado de luta contra um abrangente sistema de vigilância. Contrariamente, evidências demonstram que a necessidade crescente por tecnologias baseadas em dados no dia a dia faz com que as pessoas se conformem a essa visibilidade distribuída ao invés de se engajar politicamente (Turow *et al*., 2015).

Até agora, no Norte Global, as liberdades e necessidades em relação às tecnologias de dados têm sido abordadas por meio de um recorte de direitos fundamentais que inclui proteção de dados, privacidade informacional[6] e liberdade de expressão e comunicação. Contudo, esse enquadramento apresenta dois problemas quando aplicado ao mercado global de dados. Primeiro, o recorte individual liberal dos Direitos Humanos requer que abusos sejam claros e visíveis, de modo que os prejudicados possam responder, e, segundo, ele assume que a reparação será buscada no nível individual. Isso é problemático ao se considerar a natureza invisível e "de muitos para muitos" do "ver" por meio de tecnologias de dados, mas também pelo fato de que muitos dos impactos negativos dos dados ocorrem no nível coletivo tanto quanto no nível individual (Taylor *et al*., 2017).

Ao invés de um recorte de direitos fundamentais cuja aplicação demanda violações identificáveis, essa nova situação requer uma abordagem mais multifacetada, que possa endereçar a variedade de atores e possibilidades inerentes à contemporânea coleta e uso de dados. Ao se identificar as novas maneiras em que o poder está gravado nos dados digitais em larga escala, podemos debater melhor o que nós queremos e não queremos em relação às informações que emitimos sobre nós mesmos. A próxima seção vai explorar dois exemplos da interfase público-privado de datificação que ilustram formas pelas quais cada uma pode ser um *locus* de discriminação estrutural (que permeia instituições, regras e

6 N.T.: O termo "privacidade informacional" frequentemente é empregado de forma intercambiável com proteção de dados pessoais. Entretanto, sua origem é estadunidense, como um termo amplo para abordar diferentes campos de privacidade relacionados a informações sobre indivíduos, separadas de seus corpos físicos ou propriedades.

práticas) que é também interseccional (multiplicando desvantagens sobre pessoas em decorrência de aspectos interseccionais de sua identidade).

Identificando injustiça de dados

Irei explorar o problema da discriminação orientada por dados utilizando dois casos ilustrativos. Ambos demonstram que uma articulação específica de justiça de dados é agora exigida no que diz respeito às tecnologias de dados contemporâneas. O primeiro caso se refere à base de dados biométricos da Índia, conhecida como sistema Aadhaar. A base de dados é a maior do mundo, com mais de um bilhão de registros, e foi lançada em 2009 com o expresso objetivo de combater as fraudes no sistema de bem-estar social ao permitir que aqueles abaixo da linha pobreza provem sua identidade por meio de impressão digital ou *scanner* de íris no momento de coletar seus benefícios. Entretanto, o desenho das tecnologias que habilitam a inclusão no sistema - scanner de íris e impressão digital, além das redes, com ou sem fios, que traduzem a inclusão de dados (*inputs*) em identidades verificadas (*outputs*) - na verdade assegura que os mais pobres sejam os mais mal servidos pelo Aaadhar.

O desenho do sistema não reconhece a materialidade da pobreza, sendo incapaz de "autenticar aqueles que trabalham com pedras, cimento, calcário e aqueles acima de 60" (Yadav, 2016), uma vez que essas pessoas comumente não apresentam impressão digital em razão do trabalho braçal, ou íris escaneável devido a desnutrição. O sistema também desconsidera a precariedade do dia a dia da população pobre, uma vez que permite o registro de somente um único requerente por família para receber os bens racionados[7], de modo que se o requerente estiver doente, trabalhando ou não puder ir ao fornecedor dos bens racionados, a família não terá acesso ao seu direito (Priya e Priya, 2016). Além disso, o sistema de autenticação por *backup* funciona por meio do envio de uma senha para o telefone celular do requerente, excluindo assim as pessoas mais pobres que não podem pagar por um dispositivo celular ou qualquer pessoa que simplesmente não tenha

7 N.T.: No original, a autora utiliza o termo "*rations*" que se traduzido literalmente para o português, temos "ração". Como a palavra remete à alimentação de animais de um modo geral, optou-se por adaptar para "bens racionados".

anotado o número que tinham quando se cadastraram no sistema (Yadav, 2016).

O sistema também agrava a carga burocrática da pobreza, tendo em vista que, apesar da obrigatoriedade de participação no programa, não há formas para as pessoas corrigirem as entradas na base de dados a nível local. Não existe uma supervisão independente para fins de correção de falhas tecnológicas: o sistema de reparações remete as pessoas de volta à Autoridade Única de Identificação da Índia - agência que controla o Aadhaar -, porém não existe nenhuma obrigação legal de para que a autoridade forneça uma solução para os problemas de autenticação, deixando as lojas locais de bens racionados e as pessoas se resolverem sozinhos (Thikkavarapu, 2016). Apesar da falta de resposta aos registrados, a base dados permite que as pessoas mais pobres se tornem consumidores: o presidente do Aadhaar afirmou que o sistema apresenta um forte potencial de marketing direto para a população (Nilekani, 2013) e que estão em andamento planos de parceria com a *Google* para que a empresa possa alcançar e traçar o perfil dos seus "próximos bilhões de usuários " (Aulakh e Surabhi Agarwal, 2016).

O problema do peso/fardo desigual do Aadhaar sobre as pessoas pobres foi demonstrado pela desmonetização do governo em 2016, que levou a uma situação de caos os elementos da economia indiana baseados em dinheiro vivo (*cash-based elements*) e, consequentemente também a vida das pessoas mais pobres e marginalizadas. A desmonetização impôs exigências aos sistemas de pagamento automático de forma discriminatória contra as pessoas pobres, uma vez que elas tinham menos acesso a telefones celulares, sistemas de poupança formais e bancos em geral, e aplicações que poderiam ajudá-los a superar a crise de liquidez que se seguiu - e pagaram o preço mais alto caso as tecnologias relacionadas ao Aadhaar não os identificassem corretamente (Masiero, 2017).

Aadhaar é o que Johnson (2014), no seu trabalho sobre justiça informacional, denomina de um "sistema disciplinar". Ele suscita uma série de questões ligadas à justiça que são específicas do uso de tecnologias de dados, especificamente a forma como registra, armazena e processa os dados pessoais dos registrantes. Primeiramente, no ponto de coleta e processamento de pedidos, o sistema força os registrantes a confirmar um "padrão de normalidade" (Johnson, 2014), ao exigir que apresentem impressões digitais e íris legíveis, telefones celulares, uma família estável na qual o mesmo registrante possa retirar os bens racionados semanalmente, entre outros critérios. Esses critérios apontam para um padrão de normalidade de classe média e não para a precariedade e imprevisibilidade da vida dos pobres.

Segundo, o sistema traz problemas de justeza[8] distributiva (*fairness*). Embora se afirme que o sistema Aadhaar promove a justiça distributiva ao reduzir a corrupção nas transações de programas sociais, dando às pessoas pobres acesso a serviços e representação anteriormente inacessíveis, na verdade ele oferece possibilidades radicalmente diferentes a depender dos recursos e *status* socioeconômico de cada um. Terceiro, o sistema amplifica desigualdades: para as pessoas ricas, é uma forma de suavizar sua passagem pelo mundo. É possível adquirir um telefone ou uma conta de luz ou água, provar sua identidade nas transações cotidianas e simplificar as relações com a burocracia. Para as pessoas mais pobres, frequentemente de casta inferior e/ou do sexo feminino, é um meio de formalizar a precariedade. Para aquelas pessoas cujos corpos o sistema não consegue processar ou cuja identidade é mal interpretada, não há um caminho aparente de retorno à legibilidade administrativa. Finalmente, o sistema não permite a reparação justa de abusos ou reclamações. O procedimento de reclamações não foi concebido para emergências: ao invés de acesso a um funcionário local, o problema deve ser direcionado por telefone ou e-mail para um centro de processamento "sem prazos, sem oficiais de reparação designados, sem registros de recebimento datados por escrito, sem compensação para os reclamantes e sem penalizações para os funcionários em falta" (Sabhikhi, 2016). Embora sejam apenas as pessoas pobres que não têm escolha sobre a utilização do sistema, ele está alinhado com os corpos e estilos de vida das classes média e alta. Enquanto isso, há relatos de crescente subnutrição entre as famílias excluídas pela base de dados (Priya e Priya, 2016).

Um segundo exemplo se refere a um sistema que no momento de escrita deste artigo ainda se encontrava em desenvolvimento, mas que demonstra como a incerteza algorítmica (Kwan, 2016) – a lacuna entre a informação espacial virtual e a verdade física do terreno – pode traduzir-se na incorporação de injustiças. Uma proposta recente feita por uma empresa de consultoria comercial para a Agência Espacial da União Europeia tinha como objetivo monitorar os movimentos dos migrantes em direção às fronteiras do sul da União Europeia. Utilizando aprendizagem de máquina empregada em imagens de satélite que mostram grupos a se prepararem para embarcar para a travessia do Mediterrâneo, dados de mídias sociais e reportagens locais online, a empresa se propôs seguir os migrantes e prever a sua origem e direção de movimento. Originalmente, os consultores planejaram utilizar

8 N.T.: No original, a autora utiliza o termo "*fairness*". Optou-se por traduzi-lo enquanto "justeza" para evidenciar não apenas a conformidade com a justiça, mas apontar como o caráter de exatidão e precisão sobre os procedimentos e sistemas e arquiteturas de redes podem afetar direitos fundamentais.

os rastros do uso dos telefones celulares dos migrantes, mas foram dissuadidos em razão da dificuldade de obter bases de dados atuais, que são rigorosamente guardadas por operadoras telefônicas devido a preocupações com a privacidade (Taylor, 2016c). O objetivo do projeto proposto foi descrito como o de viabilizar a visualização de migrantes rumo à Europa, identificando pequenos grupos em praias individuais ou encostas e prevendo quem iria atravessar qual fronteira e quando. As previsões, vendidas às autoridades de controle de fronteira e migração, potencialmente permitiriam a essas autoridades usar a triagem algorítmica para identificar os migrantes "indesejados" e controlar os números de migrantes aptos a apresentar pedidos de asilo por meio da implementação de medidas para prevenir que chegassem ao solo europeu.

Essa proposta era problemática por várias razões. Primeiro, o aprendizado de máquina adotado permitiria ao projeto categorizar migrantes com base no comportamento e características registradas remotamente, e segundo, os resultados dessa análise seriam direcionados para instituições que decidem se permitem ou não a entrada desses migrantes. O primeiro objetivo é arriscado porque envolve a utilização de outros atributos como *proxies*[9] para os comportamentos ou características alvo - por exemplo, assumindo que pessoas que se reúnem em uma determinada praia em determinado momento, ou que têm postado determinadas palavras-chave ou termos nas redes sociais, podem estar planejando migrar ou pedir asilo em um determinado local. Por sua vez, esses *proxies* para local de origem e direção da viagem são concebidos com o objetivo de prever a probabilidade de um grupo de migrantes vir a ter um pedido de asilo válido.

Na realidade, contudo, é possível ser uma pessoa migrante sem registro de qualquer parte do planeta e ter um pedido de asilo válido. Isso ocorre porque qual-

9 N.T.: Em redes informáticas, um servidor *proxy* é uma aplicação de servidor que atua como intermediário entre um usuário que solicita um recurso e o servidor que fornece esse recurso. *Big data* também depende de *proxies*. Há coisas que simplesmente não podem ser facilmente medidas, ou medidas de forma alguma, tornando difícil fornecer um modelo de valor ou comportamento. Mas, num esforço para tentar prever os melhores resultados, um número deve ser atribuído de alguma forma. Por isso, utiliza-se os proxies. Vale frisar que estudiosos de dados se dedicam aos impactos da discriminação por *proxy* ou *proxy discrimination*. De acordo com o *National Council of Insurance Legislators* (NCOIL Property/Casualty Insurance Modernization Act), discrminação por *proxy* significa substituição intencional de um fator neutro por um fator baseado na raça, cor, credo, origem nacional, ou orientação sexual para o objetivo de discriminar um consumidor para impedir que este obtenha um seguro ou uma taxa mais vantajosa devida à raça, cor, origem nacional, ou orientação sexual. A discriminação por *proxy* tem por vezes sido utilizada intencionalmente para contornar as regras que proíbem a discriminação em empréstimos, habitação ou emprego. Para saber mais, conferir Prince, Anya and Schwarcz, Daniel B., *Proxy Discrimination in the Age of Artificial Intelligence and Big Data* (August 5, 2019). 105 Iowa Law Review 1257 (2020), Available at SSRN: **https://ssrn.com/abstract=3347959**.

quer pessoa pode estar em risco mesmo em um ambiente "seguro". Por exemplo, durante a tentativa do governo dos Estados Unidos de impor uma proibição de viagem aos muçulmanos em 2016, o governo canadense considerou a possibilidade de desclassificar os EUA como um país seguro para refugiados (Kassam, 2017). As pessoas de países democráticos que não estão em guerra podem estar em risco em razão da sua sexualidade, gênero, religião, etnia, filiação política ou qualquer outra característica. As condições de risco para as pessoas são contingentes, mutáveis e sutis, para além do que pode ser previsto através da captura e ponderação de *proxies* de local de origem e comportamento migratório. Tal modelo, baseado na já desacreditada ideia de "agir de forma suspeita", acabará quase que inevitavelmente sendo utilizado para produzir uma resposta de "sim/não" que, aplicada a nível de grupo, determina a vida ou a morte de migrantes individuais.

Um sistema como esse serve para demonstrar como as possibilidades de controle por meio de tecnologias de dados "co-evoluem" com possibilidades de cuidado (Lyon, 2007). Pessoas refugiadas utilizam tecnologias semelhantes para guiá-los pelo seu caminho na Europa, mas de forma a proteger suas identidades e dar-lhes algum grau de controle sobre sua trajetória. Elas compartilham os dados de GPS do celular com parentes e voluntários, utilizam o *Google Maps* para encontrar seu caminho e as redes sociais para decidir como fazer sua viagem (BBC News, 2015; Ram, 2015). Quando utilizadas por pessoas e grupos "no terreno", as mesmas tecnologias de GPS e cartografia baseadas em satélite que podem ser usadas por agências de fronteira para controlar e apagar a migração também ajudam pessoas migrantes a preservar a autonomia, a segurança humana e seu direito de fugir do perigo.

Existe um forte incentivo para que analistas comerciais, nesse caso, destaquem a precisão das suas previsões automatizadas, haja vista que isso aumenta o seu valor para os compradores do setor público. Um bom sistema utilizável, como observam Bowker e Star (1999: 33), torna-se tão conveniente que desaparece a um ponto que só os seus resultados permanecem visíveis. No contexto da vigilância remota em larga escala para fins de políticas públicas, a probabilidade da precisão dessas respostas serem testadas diminui. O'Neil (2016) alertou que os modelos algorítmicos devem ser constantemente recalibrados utilizando o *feedback* dos eventos que supostamente devem prever. No entanto, é difícil imaginar como um modelo que se vale da vigilância remota para prever os objetivos e origem de migrantes sem registro também possa incorporar dados corretos sobre os desfechos reais desses movimentos migratórios.

Para além da provável inexatidão de tal sistema, o exemplo nos leva ao maior problema: que os direitos fundamentais - incluindo os direitos à privacidade e autonomia, à reparação eficaz dos danos, e muitos outros relacionados à utilização de dados em um sistema de predição da migração - não são efetivamente tratados como fundamentais porque não ultrapassam fronteiras. O problema dos direitos de pessoas migrantes vai muito além dos dados, mas os sistemas de dados sustentam a forma como elas podem ser incluídos ou excluídos e, por conseguinte, a sua capacidade de reivindicar seus direitos (Broeders, 2009). Sistemas de dados que são de natureza transnacional exigem direitos e mecanismos de reparação igualmente transnacionais, porém isso é atualmente impossível no caso de processos remotos de detecção, análise e tomada de decisão. Alguém que é vigiado de forma remota não saberá por que está sendo categorizado e, em qualquer caso, aqueles que são territorialmente excluídos como resultado desses processos não poderão recorrer das decisões. Entretanto, se o funcionamento de leis nacionais e da soberania significa que uma pessoa tem certos direitos fundamentais quando está de um lado da fronteira da União Europeia, mas não do outro, isso é profundamente problemático por razões que não podem ser solucionadas por meio de reivindicações de soberania (Brock, 2009). A justiça de dados une-se a uma classe de problemas multidimensionais complexos como a justiça climática, o terrorismo e a pobreza, que foram classificados como "*super-perversos*"[10] (Levin *et al.*, 2012), sendo necessário endereçá-los de uma forma sistêmica, a fim de lidar com suas interdependências.

Justiça de dados através de domínios e sistemas

Atualmente, existem (pelo menos) três principais abordagens para conceitualizar a justiça de dados: a primeira endereça os modos nos quais os dados usados para governança podem sustentar assimetrias (Johnson, 2014); a segunda foca nos modos nos quais as tecnologias de dados podem proporcionar maior justiça distributiva, tornando pessoas pobres visíveis (Heeks e Renken, 2016); por fim, há uma abordagem interessada em como as práticas de vigilância de dados podem

10 N.T.: Tradução livre do inglês "*super-wicked*".

impactar o trabalho de organizações que trabalham por justiça social (Dencik et al., 2016). Ainda que estas linhas de pesquisa aparentemente apontem em diferentes direções, irei argumentar que existe valor em reuní-las.

Johnson (2014) conecta a justiça de dados primariamente a dados abertos. Ele escreve sobre a necessidade de "englobar a questão dos dados abertos sob a questão maior de justiça informacional", mas avança ao oferecer conclusões que têm relevância para o uso de dados enquanto ferramenta para governança (e governabilidade) de forma mais ampla. Ele advoga pelo estabelecimento de um conceito de "justiça informacional" que possa se contrapor aos modos pelos quais a produção administrativa de dados incorpora privilégios sociais e cria um conjunto desigual de oportunidades devido às diferentes capacidades da cidadania versus usuários e usuárias comerciais. Ele argumenta que há nos sistemas uma tendência à função disciplinadora porque o modo como os dados são coletados e estruturados constitui uma forma de coerção normativa (um exemplo disso é o problema vivenciado por pessoas transgêneres ao tentarem modificar seus registros de nascimento, conforme citado acima). Como uma forma de endereçar o problema, Johnson (2016: 29) advoga por "tornar a política explícita" em relação às tecnologias de dados, mediante pesquisas colaborativas envolvendo especialistas da filosofia da tecnologia, ciência de dados e ciências sociais.

Em seguida, Heeks e Renken (2016) fornecem uma rica análise sobre os possíveis enquadramentos da justiça de dados sob a perspectiva e prioridades do campo do desenvolvimento internacional, deslocando a questão da justiça informacional para o nível explicitamente global e questionando como ela deve ser proposta quando aplicada a questões de desenvolvimento humano. O artigo parte da noção de que os Objetivos de Desenvolvimento Sustentável estão na vanguarda tanto de "dados" quanto de "justiça" e que, portanto, o campo/área do desenvolvimento deve se engajar com ambos enquanto conceitos interseccionais pela primeira vez. Os autores defendem uma abordagem estrutural que não se limite às funções dos dados nesse setor, mas que seja enquadrada com referência a "códigos de justiça social e política mais amplos" (p. 5). Eles utilizam a Declaração Universal dos Direitos Humanos (Organização das Nações Unidas, 1948) para sustentar que os direitos de titulares como controle, acesso e representação são fundamentais em termos de justeza e justiça. O artigo defende uma perspectiva em rede, apontando os sistemas de dados como conectores a níveis local e global, nos quais interesses antagônicos estão, por definição, em jogo.

Por fim, Dencik *et al.* (2016) identificam a necessidade de conceitualizar a

justiça de dados devido ao modo como o capitalismo de vigilância constrange a cidadania e o ativismo. Defendem, portanto, a introdução da terminologia "justiça de dados" para descrever uma resistência à vigilância estatal baseada nos princípios da justiça social. Sua ideia de justiça de dados presta atenção aos modos pelos quais as escolhas de sistemas de dados, fornecedores e públicos alvo carregam consigo tipos específicos de poder e interesses. Sob este enquadramento, justiça de dados é um conceito que pode auxiliar na colaboração entre ativismo anti-vigilância e de justiça social, orientando o primeiro a articular preocupações mais amplas sobre liberdades e garantias, e o segundo a envolver-se com a dimensão técnica da vigilância e da resistência. Este enquadramento foca especificamente no ativismo social, mas se conecta tanto com o chamado de Johnson a explorar a política da datificação, quanto à atenção à economia política dos dados: "A referência à 'justiça de dados' reconhece a economia política do sistema que dá suporte às possibilidades de vigilância massiva, ao passo que chama atenção à agenda política que orienta sua implementação" (Dencik *et al.*, 2016: 10)

Essas três interpretações contrastantes da ideia de justiça de dados estão conectadas pelo seu foco na política e no poder, além de suas formulações de justiça social. As diferenças entre os conceitos, no entanto, são úteis porque levantam algumas questões essenciais.

Primeiramente, como a conceitualização de justiça de dados em escala global pode invocar fundamentos importantes como direitos, justiça e justeza sem se tornar relativista? Heeks e Renden (2016, p. 7) apontam que cada região ou país irá julgar o que considera justo de acordo com seus próprios conceitos, baseados em suas próprias tradições e história, e que por isso procuram 'passar ao largo das noções interpretativas, de baixo para cima' em direção a códigos mais amplos como a Declaração Universal dos Direitos Humanos.

Como é possível, porém, formular princípios de justiça de dados sem permitir que eles sejam moldados pela comunidade global de produtores de dados? Uma visão de justiça de dados que leve em consideração o poder e a política deve, necessariamente, também ser enraizada em experiências locais. Se os países têm diferentes objetivos quanto ao potencial do uso de dados digitais, e diferentes ideias do que se considera seu uso indevido, como deve ser sua contribuição para o enquadramento do que seria justo? Por exemplo, já se argumentou que as pessoas recipientes de políticas de desenvolvimento efetivamente têm um dever de visibilidade frente às autoridades que trabalham no combate à pobreza (Taylor, 2016c). Robert Kirkpatrick, da iniciativa de ciência de dados Global Pulse, da ONU, disse, a

respeito de cidadãs e cidadãos de países em desenvolvimento que "privacidade é seu direito. Mas acesso a comida, água e ajuda humanitária também são. O desafio é que nós vemos uma série de sistemas regulatórios nos quais não há um teste decisivo"[11-12]. Sua fala sugere que agências de desenvolvimento têm direito sobre os dados das pessoas sob uma lógica utilitarista, e que se opor ao tratamento de dados nesse contexto não deveria ser uma escolha porque irá impactar os direitos da coletividade.

Até aqui, utilizei palavras como "direitos" e "liberdades" para denotar conceitos que parecem essenciais como métricas para o uso justo das tecnologias. O exemplo da Global Pulse, no entanto, indica a necessidade de uma abordagem relacional (oposta à abordagem relativista) que possa integrar direitos e necessidades em um único enquadramento, mais do que demandar uma escolha puramente utilitária entre eles. Na verdade, a gramática dos direitos pode não ser a ferramenta correta para definir uma formulação global de justiça. Brock (2009), em seu relato cosmopolita sobre a justiça global, argumenta que questionar quais são as necessidades das pessoas, ao invés dos direitos que podem reivindicar, possibilita pensar através de enquadramentos culturais e regionais de justiça. A noção liberal de sujeito de direitos não é adotada em diversas sociedades que, não obstante, têm fortes tradições filosóficas e jurídicas sobre noções de justiça e justeza (Panikkar, 1982). Muitos Estados e regiões, por exemplo, adotam uma perspectiva sobre direitos que os enquadra como inseparáveis dos deveres correspondentes, além de endereçar o indivíduo como parte de um coletivo maior (Sen, 2005).

Datificação é, frequentemente, um território tanto para a formalização, quanto para a negociação de direitos. Por exemplo, no caso de diversos Estados africanos, Makulilo (2016) afirma que, com a chegada da era digital, a crescente economia de dados vem situando a noção de *Ubuntu* (a humanidade em direção ao coletivo) em uma complexa interação com a noção de privacidade. Argumentando ser possível encontrar certas liberdades identificadas como importantes em diferentes sociedades na região, mesmo sem sua formalização como direitos humanos, Makulilo cita Nwauche, acadêmico nigeriano, que afirma que apesar da inexistência de um direito formalizado, "a privacidade é importante na Nigéria porque há seres humanos". Com base nisso, pode ser mais útil pensar em termos de necessidades básicas relacionadas a dados que podem ser formalizadas de

11 NT.: Por teste decisivo, aqui o autor citado se refere à criação de métricas sólidas para balizar a compreensão sobre direitos e o equilíbrio entre eles.

12 Robert Kirkpatrick, UN Global Pulse, entrevistado em 18 de agosto de 2014.

modo diverso em diferentes locais.

Também a dissuadir contra o uso de um enquadramento baseado em direitos individuais para moldar a justiça de dados vem o fato de que as injustiças de dados tendem a ocorrer de forma coletiva. Novas tecnologias de dados tendem a classificar, perfilar e informar ações baseadas em características e comportamentos de grupos, mais do que individuais (Taylor *et al.*, 2017), de modo que, para operacionalizar qualquer conceito de justiça de dados, inevitavelmente será necessário abordar a questão para além do nível individual. Alguns sistemas jurídicos já têm formalizada essa relação entre vigilância e coletividade: a lei mexicana, por exemplo, prevê esse caráter coletivo da privacidade informacional ao incluir a família na esfera do indivíduo em relação à proteção de dados (Tribunales Colegiados del Circuito, 2015). Sen (2005), cujo trabalho é central para a contribuição de Heeks e Renken sobre justiça de dados, equilibra o individual e coletivo quando aponta que a justiça social não pode ocorrer em um vácuo, exigindo ação coletiva para que seja efetivada. A abordagem estrutural é a chave aqui: se considerarmos a necessidade do estabelecimento formal do que é justo (liberdades de processo) e da necessidade de agência (liberdades de oportunidade) (Sen, 2005), a justiça de dados parece se encaixar melhor em uma perspectiva ampliada de capacidades que abranja variações sobre como a justeza deve ser determinada e se a justiça pode ser realizada.

A segunda questão que emerge dos três enquadramentos acima listados é sobre o que a justiça de dados deve tentar alcançar. As três perspectivas focam em direções muito diferentes: Johnson questiona como o desenho das bases de dados pode melhor incorporar princípios de anti-discriminação; Heeks e Renken focam especificamente em como os dados devem ser distribuídos de modo a alcançar níveis de acesso, participação e representação mais justos. Dencik *et al.*, por sua vez, se preocupam com as condições nas quais os dados não devem ser distribuídos (através da vigilância), de modo a proteger o trabalho de ativistas que trabalham em prol da justiça social. Uma outra perspectiva contrastante pode ser encontrada no trabalho de Mann (2016), que afirma ser importante um foco em quem consegue processar os benefícios econômicos da economia de dados, e que, na promoção da justiça social relacionada aos dados digitais, deve-se buscar incorporar princípios de justiça no modo como os mercados de dados são estruturados.

Essas perspectivas são contrastantes ou incompatíveis? Será que nós precisamos separar os enquadramentos, de modo a desenvolver melhores defesas

contra a discriminação, ampliar as resistências à vigilância e possibilitar o exercício do direito de ser contabilizado para fins de políticas públicas, ou seria mais útil encontrar um argumento abrangente sobre justiça de dados, capaz de incorporar esses princípios e, dessa forma, realizar uma contribuição maior do que endereçá-los separadamente? Na próxima seção defenderei tal enquadramento mais abrangente, de modo a promover uma reconciliação entre os objetivos citados, cada qual promovendo uma liberdade diferente, mas essencial, em relação a dados.

Uma proposta de enquadramento para justiça de dados

Um enquadramento que pudesse conciliar as diferentes perspectivas discutidas acima teria de fazer várias coisas. Em primeiro lugar, teria que levar em conta a novidade e complexidade das formas como os (grandes) sistemas de dados podem discriminar, disciplinar e controlar, como demonstrado nos exemplos do Aadhaar e do sistema de monitoramento da migração. Em segundo lugar, teria que considerar tanto o potencial positivo como o negativo das novas tecnologias de dados - a sua capacidade de facilitar o que Nussbaum e Sen (1993) chamam de "florescimento humano", que constitui o principal objetivo do desenvolvimento humano - e também o seu potencial de prejudicá-lo. Finalmente, teria que fazê-lo utilizando princípios que fossem úteis em diferentes contextos sociais, e assim, remediar o atual padrão duplo em relação à privacidade e ao valor da visibilidade em países mais pobres *versus* países mais ricos, como ilustrado pela Global Pulse e seu balanceamento utilitarista entre privacidade e outras necessidades.

Assim, é necessária uma conceituação que leve em conta a necessidade do indivíduo estar representado, mas também a possibilidade de optar pela não coleta ou tratamento de dados, a necessidade de preservar a autonomia em relação às tecnologias de produção de dados e a necessidade de ser protegido contra e de desafiar a discriminação orientada por dados. Isto sugere uma abordagem baseada em três pilares: visibilidade, (des)engajamento com a tecnologia e combate à discriminação orientada por dados (ver Figura 1), mas que faça mais do que estabelecer quais direitos são necessários. Essa abordagem deve também prever um compromisso metodológico com a economia política dos dados, a fim de determinar não só *o quê*, mas também *quem* é importante e como ambos se

relacionam com os resultados desejados.

Como mostra a Figura 1, os elementos de justiça de dados aqui enunciados são propositadamente mais amplos do que os enquadramentos internacionais disponíveis, tais como os Princípios de Práticas Informacionais Justas (*Fair Information Practice Principles*), que constituem a base dos direitos de informação em muitos países da OCDE, ou o direito à privacidade, tal como estabelecido nos diversos instrumentos de direitos humanos. Estes enquadramentos são valiosos e muitas vezes eficazes, mas visam o problema a um nível prático e não conceitual. Ao invés de delimitar o que deve ou não ser feito com dados, os elementos de justiça de dados aqui propostos representam uma forma de pensar para além de domínios e aplicações particulares, e, em vez disso, abordar as tecnologias de dados principalmente na medida em que elas se relacionam às necessidades humanas.

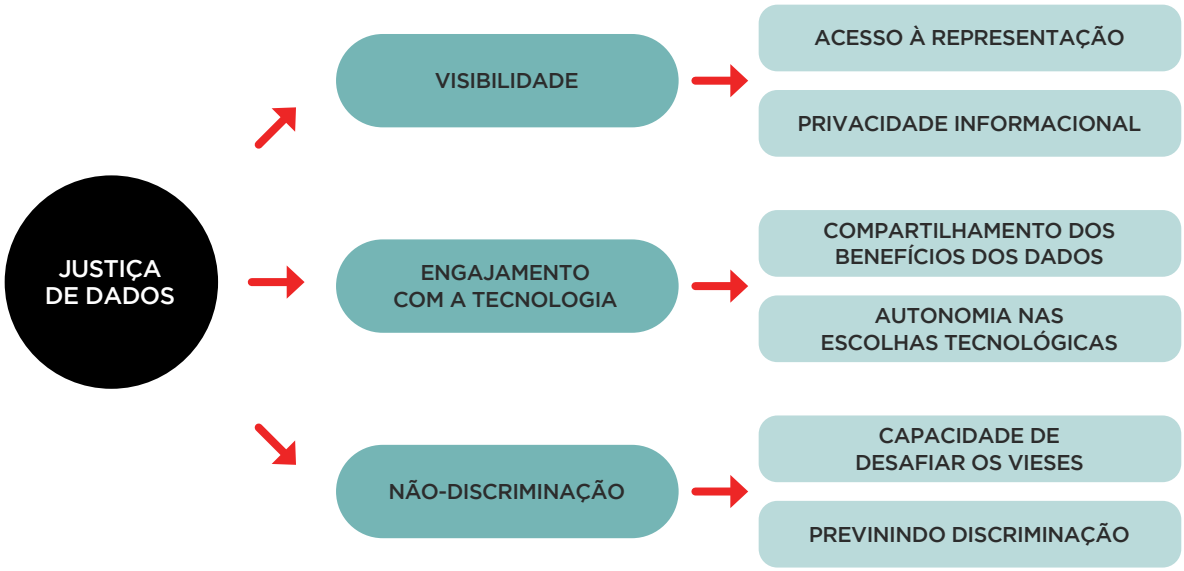


Figura 1. Os três pilares da justiça de dados

O primeiro pilar, a visibilidade, trata tanto da privacidade quanto da representação. Aqui podem ser extraídas linhas de raciocínio comuns aos campos dos estudos de desenvolvimento internacional, da geografia humana e da doutrina jurídica. Um enquadramento mais detalhado das necessidades paralelas de visibilidade e privacidade informacional deve ter em conta trabalhos em andamento sobre a privacidade nas margens sociais (Arora, 2016; Gilliom, 2001; Jayaram, 2014), sobre os riscos para a privacidade de grupo criados por práticas de perfilamento coletivo (Taylor, 2016b; Floridi, 2014; Raymond, 2016) e sobre até que ponto os dados podem ser considerado um bem público (Taylor, 2016d).

O engajamento com a tecnologia é o segundo pilar desta tentativa de enquadramento conceitual. Embora a TIC para o desenvolvimento[13] - a promoção do engajamento com as tecnologias digitais nos países de baixa ou média renda - tenha estabelecido claramente ligações entre a promoção do desenvolvimento humano e o acesso às TICs (Heeks, 2010; Unwin, 2009), este campo está se adaptando, tal como outros, à evolução das novas tecnologias de produção de dados e *analytics* e começa, agora, a abordar de forma crítica a liberdade de não utilizar tecnologias específicas, e em particular de não se tornar parte de bases de dados comerciais como subproduto de intervenções pró desenvolvimento (Taylor & Broeders, 2015; Gagliardone, 2014). A liberdade de controlar os termos do seu engajamento com os mercados de dados é um componente essencial de qualquer enquadramento de justiça de dados, já que embasa o poder de compreender e determinar a sua própria visibilidade. Argumentos sobre a importância da autonomia das pessoas no que diz respeito à tecnologia podem ser encontrados em teorias pós-coloniais, uma vez que a forma como os dados são processados e analisados nos mercados de dados nacionais e globais posiciona os indivíduos como subalternos (Spivak, 1988) em relação àqueles que processam os seus dados. Eles não conseguem definir por si próprios como os seus dados são utilizados, a quem são revendidos ou os tipos de perfis e intervenções que esses dados podem permitir. Nesse sentido, Mann (2016) argumenta que uma abordagem de *dados para o desenvolvimento econômico*, e não apenas de dados para o desenvolvimento *per se*, concentra a atenção nos potenciais benefícios da coleta e análise de dados para as pessoas de baixa renda, independentemente das grandes empresas de tecnologia, e na forma como os retornos dos dados podem ser capturados e processados a nível local.

O terceiro pilar da formulação proposta é a não-discriminação. Ele é composto por duas dimensões: o poder de identificar e desafiar os vieses na utilização de dados, e a liberdade de não ser discriminado. É esperado que a capacidade das pessoas para identificar e desafiar o enviesamento na tomada de decisões orientadas pelos dados diminua à medida que a complexidade da produção e processamento de dados aumenta (Kroll *et al.*, 2016). À medida que as redes neurais e a aprendizagem profunda (*deep learning*[14]) se tornam mais comuns, a capacida-

13 N.T.: TICs são Tecnologias da Informação e Comunicação e podem ser entendidas como um conjunto de recursos tecnológicos, utilizados de forma integrada, que proporcionam, por meio das funções de *hardware*, *software* e telecomunicações, a automação e comunicação de processo.

14 N.T.: A noção de *deep learning* está associada ao conceito de *machine learning* ou a aprendizagem de máquina. O aprendizado de máquina utiliza algoritmos para organizar dados, detectar padrões e fazer com que computadores realizem tarefas, aprendam com elas e ainda gerem soluções inteligentes sem que sejam pro-

de até mesmo dos próprios designers de sistemas de compreender como vieses podem ser incorporados no processamento de dados é reduzida. Isto significa que devem ser concebidos métodos que permitam a governança de processos e decisões baseadas em algoritmos, e também que a responsabilidade de desafiar a discriminação por parte dos indivíduos terá de ser acompanhada pela capacidade de identificar e criar sanções por parte dos governos (Kroll *et al*., 2016).

Parte da contribuição do quadro conceitual proposto para a justiça de dados é ajudar a enquadrar as questões necessárias, bem como a apontar o caminho para respostas. Tal como na tabela periódica, qualquer mapeamento de relações e posições também mapeia os elementos ausentes. Por exemplo, a *liberdade de não se envolver com os mercados de dados ou de não estar representado em bases de dados comerciais* ainda não foi devidamente teorizada: mesmo os estudos de privacidade partem do princípio de que tal envolvimento é inevitável. Contudo, existem indícios históricos e contemporâneos de que tais liberdades são necessárias: De manifestantes luditas do século XIX, que desenvolveram uma nova política de direitos e resistência dos trabalhadores no contexto das novas tecnologias industriais (Binfield, 2015) a ativistas anti-censo dos anos 70 e 80 nos Países Baixos e na Alemanha (Hannah, 2010; Holvast, 2013), tem havido um debate sobre onde as tecnologias que podem contar e controlar se encaixam dentro do contrato social e quanta visibilidade cidadãos e cidadãs devem ao Estado. Este debate está subjacente às formulações de Heeks e Renken e Johnson: o direito a ser visto e representado é central para a justiça de dados, mas o mesmo acontece com o direito de se retirar das bases de dados, quer seja detida pelo Estado, empresas comerciais ou ambas, como no caso do sistema Aadhaar.

Talvez a questão central levantada pelo conceito de justiça de dados aqui exposto seja como equilibrar e integrar a necessidade de ser visto e representado adequadamente com as necessidades de autonomia e integridade. Quais são as implicações de deixar as pessoas optarem por não participar da coleta de dados? Deverão as pessoas, por exemplo, ser capazes de se auto-excluir de bases de dados comerciais se essas bases de dados tiverem alto potencial de utilização pelo Estado para complementar ou substituir dados administrativos ou de censos? Quais são os princípios de boa governança para a utilização de *Big Data* num contexto

gramados especificamente para isso. Já a aprendizagem profunda é uma tecnologia que utiliza algoritmos mais complexos do que a aprendizagem de máquina e baseia-se no princípio das redes neurais, buscando imitar o cérebro humano com ainda mais fidelidade, no que tange à forma de compreender novas informações e gerar resultados a partir delas. Em outras palavras, a aprendizagem de máquina geralmente funciona de forma linear, enquanto a aprendizagem profunda utiliza camadas encadeadas hierarquicamente.

democrático, e quem deve ser responsável por determiná-los?

O censo é, simultaneamente, um dos momentos mais invasivos na relação entre indivíduo e Estado e um dos direitos mais importantes da cidadania em uma sociedade democrática. Se os dados do Estado serão, em breve, pelo menos parcialmente compostos por dados coletados comercialmente (Keeter, 2012) e atualizados em tempo real, e se esses dados podem dizer aos governos não só fatos convencionais sobre a população mas, em vez disso, quase tudo, onde termina a observação legítima para começar a vigilância ilegítima?

Uma abordagem ecossistêmica baseada nas capacidades

Conforme Heeks e Renken sugerem, a Abordagem das Capacidades de Sen (1999) e Nussbaum (2006) oferece uma via para a integração dos princípios da justiça de dados em um enquadramento operacionalizável, assim como o faz a Ferramenta das Escolhas[15] de Kleine, que conceitualiza oportunidades oferecidas pela tecnologia em um contexto de desenvolvimento. A Abordagem das Capacidades engloba tanto o que Sen chama de *liberdades de oportunidade*, descritas por Alkire (2011) como a oportunidade real de alguém alcançar aquilo a que dá valor, quanto o que ele chama de *liberdades de processo*, que denotam agência – a capacidade de agir em nome do que importa (Alkire, 2011). Em consonância com o foco da justiça de dados na prevenção da marginalização e na promoção de um modelo socialmente justo para o tratamento de dados, tal abordagem não parte de uma consideração da "pessoa média", mas questiona que tipo de princípios organizadores para a justiça podem atingir pessoas em situação de vulnerabilidade e marginalização na mesma medida em que atingem quaisquer outras pessoas (veja a Figura 2).

O diagrama demonstra como a justiça de dados pode se encaixar na Abordagem das Capacidades enquanto uma estrutura conceitual abrangente, dentro da qual pesquisas e debates podem identificar quais liberdades as pessoas valorizam em relação às tecnologias de dados e como materializá-las. Ele está posicionado dentro da estrutura de liberdades de oportunidades e liberdades de processos que

15 N.T.: Tradução livre de "*choice framework*".

determina o que os "funcionamentos" das pessoas ('fazeres' ou 'seres')[16] podem ser quando se trata da sua relação com tecnologias de dados. Por sua vez, esses funcionamentos podem ser traduzidos por meio de *fatores de conversão social*, como apoio político, jurídico e educacional, em *capacidades*, como a participação na cadeia de valor dos dados, o acesso a dados que afetam um indivíduo (por exemplo, por meio de legislações sobre o acesso à informação ou pelo acesso direto a instalações de dados setoriais), e a inclusão na tomada de decisão sobre quais tecnologias deverão ser utilizadas em contextos específicos.

Se seguirmos o conselho de Sen sobre o envolvimento com o domínio do raciocínio público para determinar o que as pessoas querem em relação às tecnologias de dados, isso também nos leva a considerar seu argumento geral para um enquadramento das Capacidades: que ela ajuda pessoas a decidirem quais funcionamentos mais valorizam, e quais capacidades desejam priorizar. Assim, a tarefa de um enquadramento conceitual para a justiça de dados passa a ser aprofundar essa abordagem, a fim de entender quais são os princípios comuns que podem auxiliar a sua operacionalização. Tais princípios são necessários em relação à natureza global do mercado de dados, uma vez que legislações nacionais têm dificuldade em regular processos transnacionais, como é o caso, por exemplo, de *data brokers*[17] e grandes provedores de serviços online, como o *Google* e o *Facebook*.

A tarefa de construir e pensar sobre a operacionalização desse tipo de enquadramento da justiça de dados requer, portanto, um conjunto de ferramentas teóricas e metodológicas diferentes de, por exemplo, pesquisas sobre privacidade informacional. Isso se encaixa em uma tendência atual na qual estudiosos em todo o mundo estão pedindo mudanças sobre como os impactos sociais dos dados são pesquisados (Cohen, 2012; Dalton *et al.*, 2016; Floridi, 2016; Kleine, 2010; Schwartz e Solove, 2011). Cohen (2012), em particular, defendeu uma análise interdisciplinar e socialmente situada sobre informação, poder e privacidade, capaz de criar novas formas de organização para a prosperidade humana que sejam relevantes para a ascensão do "eu em rede". Tal pesquisa precisaria adotar uma abordagem

16 N.T.: A ideia de "funcionamentos" ou "*functionings*" para Sen se traduz em estados de "ser" e "fazer" - exemplos comuns são "estar bem-nutrido" ou "ter um teto". Os conjuntos de funcionamentos a que os indivíduos efetivamente têm acesso conformam as suas capacidades.

17 N.T.: *Data brokers* são empresas que compilam dados pessoais, realizam seu tratamento e vendem informações a terceiros. Um exemplo do uso é para fins de publicidade, de modo a categorizar consumidoras e consumidores para campanhas de *marketing* direcionado. Outro exemplo corrente são empresas do campo financeiro, que realizam pontuação de crédito (ou *score* de crédito), determinando, com base em atividades de indivíduos, quem teria mais probabilidade de honrar seus compromissos financeiros.

ecossistêmica global, que pudesse olhar para além de fronteiras. Ela ofereceria a possibilidade de fazer uma ponte entre diferentes níveis de envolvimento com a tecnologia e diferentes conceitos de desenvolvimento relacionado à tecnologia, e também entre sistemas morais e filosóficos diversos. Uma ferramenta importante nesse processo seria o campo emergente dos Estudos Críticos de Dados[18], bem como o das geografias digitais de modo mais amplo, os quais têm demonstrado que o conhecimento necessário para estabelecer uma abordagem socialmente justa do uso de dados digitais já existe, mas tende a não ser incorporado em políticas públicas, legislação ou práticas no nível necessário para ser operacionalizável (Dalton *et al.*, 2016). A conexão desse conhecimento com a política e as leis, especialmente no que tange às responsabilidades políticas transnacionais de provedores de serviço online (Taylor *et al.*, 2017), inevitavelmente faria parte do trabalho de materializar a justiça de dados, assim como acontece com os movimentos de justiça social de forma mais ampla.

As questões levantadas pelo enquadramento da justiça de dados aqui apresentado operam tanto no nível mais alto – onde o contrato social é moldado e negociado – quanto no mais básico, nas práticas da vida digital cotidiana. Estes níveis, como Heeks e Renken apontam, serão diferentes em cada sociedade ou região. Portanto, o principal desafio na construção do conceito será descobrir como esses princípios abrangentes podem ganhar tração em diferentes contextos: alguns países ou grupos irão identificar benefícios na vigilância, enquanto outros vão reagir fortemente contra ela como uma prática opressiva. Alguns afirmam que a inovação do setor privado desempenha um papel central na realização dos benefícios da ciência de dados, enquanto outros afirmam que tornar o setor público mais responsável pelo controle de dados alcançará resultados mais justos. O núcleo conceitual precisaria ser traduzido e negociado em todos os contextos, assim como seus componentes já foram (por exemplo, proteção de dados ou a ética em pesquisa). Ideias como justiça, igualdade e não discriminação informam regimes tão variados quanto tributação e regulação de mercado, de modo que a justiça de dados precisaria operar como outro ramo desses princípios básicos de governança. No entanto, ao invés de serem centralizados (o "centro" inevitavelmente seria um local com muita renda e alta tecnologia), essas traduções e negociações teriam que ocorrer de forma distribuída dentro do que Sen (2005) denominou "o domínio do raciocínio público". Sob esta premissa, cada sistema jurídico e social desenvolve-

18 N.T.: Tradução livre do inglês *Critical Data Studies*.

ria por si mesmo como os princípios da justiça de dados seriam aplicados. Isso é importante porque os princípios aqui estabelecidos estão em desarranjo, de uma forma ou de outra, com todos os regimes já estabelecidos para a governança de dados no planeta (por exemplo, o direito de não ser registrado em bancos de dados), e enfrentarão desafios diferentes a depender de onde a discussão seja feita.

Figura 2.

Conclusão

O conceito de justiça de dados apresentado acima representa um desafio para a maioria das atuais formulações de governança de dados. Ele o faz porque incorpora a suposição de que qualquer enquadramento que não absorva tanto os aspectos benéficos quanto negativos das tecnologias de dados não pode ganhar força no domínio do raciocínio público. Os enquadramentos utilizados atualmente ou enfatizam os riscos e danos, ou defendem que os dados e o poder de analisá-los sejam tão amplamente acessíveis quanto possível. A tarefa de reconciliar essas perspectivas é enorme, política e teoricamente. A proposta que busca reconciliar a visibilidade e invisibilidade da datificação, além do engajamento ou desengajamento tecnológico, irá desafiar diversas normas já estabelecidas, notadamente em áreas que promovem a inovação e o desenvolvimento econômico, além do direito estabelecido do Estado de contar e intervir sobre seus cidadãos e cidadãs. Os princípios aqui apontados não são obstáculos à inovação, nem devem constituir uma barreira a processos democráticos nos governos. Contudo, eles colocam questões difíceis que exigem uma reconciliação significativa entre valores distintos. É importante expor essas questões porque elas apontam para as interfases dinâmicas entre indivíduos e Estado, entre setores público e privado, bem como entre a ciência e a população. Além disso, elas demarcam o território desconfortável no qual ocorrem atritos em torno da privacidade, da responsabilização e da prestação de contas.

Esses espaços de atrito merecem nossa atenção. São os lugares onde estamos negociando tanto a evolução da governança, quanto de como desejamos conviver lado a lado nas sociedades do conhecimento. A mudança não deve ocorrer nessas interseções sem repararmos nisso, tampouco devemos considerá-la inevitável. A inovação e a evolução da tecnologia são constantes e desejáveis, mas as formas como as tecnologias são usadas para nos monitorar e governar são negociáveis. Devemos ser capazes de determinar nossas interações com a tecnologia debatendo e, se necessário, resistindo e propondo caminhos diferentes. Se não podemos imaginar modos de recobrar o tipo de privacidade que gostaríamos, ou como permitir que as pessoas optem por não serem vigiadas através de seus dados – ou mesmo produzir esses dados em primeiro lugar – talvez tenhamos que, além de renegociar, também reinventar.

Isso também pode envolver demandas diferentes a autoridades - sejam comerciais ou governamentais - com relação a governança de, e por meio das, tecnologias de dados. Operacionalizar o enquadramento aqui proposto implica um deslocamento da responsabilização dos indivíduos pela compreensão sobre o mercado de dados, tornando as autoridades nacionais e internacionais responsáveis por sua governança. Isso também demandaria a distinção entre o uso *responsável* de dados – a expressão da moda nas áreas de governança de dados e política de inovação – e *prestação de contas* a respeito dos dados, algo muito mais difícil de alcançar, na medida em que exige mudanças estruturais, ao invés de apenas permitir que nossos vigilantes vigiem a si mesmos.

Os vários enquadramentos de justiça de dados propostos desde o advento do *Big Data* indicam que, em todo o mundo, acadêmicos e formuladores de políticas públicas estão tentando conciliar princípios de justiça social com a realidade da datificação. Suas contribuições vão de grandes dimensões, como o Manifesto Onlife, até outras mais específicas, como o trabalho de Greenfield "*Against the Smart City*" (2013). O próximo desafio é integrar essas perspectivas e princípios mundiais em uma visão mais ampla que possa abordar a globalização das tecnologias de dados e os seus impactos. O enquadramento aqui apresentado é uma resposta ao desafio de dar sentido à vida em sociedades datificadas. Ele visa a oferecer um roteiro para uma análise mais aprofundada, a especificação de metas e objetivos particulares e, eventualmente, a sua operacionalização em contextos nacionais e internacionais múltiplos e diversos.

DECLARAÇÃO DE CONFLITO DE INTERESSES

A autora declarou não haver potenciais conflitos de interesses em relação à pesquisa, autoria e/ou publicação deste artigo.

FINANCIAMENTO

A pesquisa foi conduzida no Oxford Internet Institute e na Universidade de Amsterdam, neste último com uma bolsa de pós-doutorado Marie Curie (624583 D4D).

Referências[19]

Alkire S (2011) The capability approach and human development. University of Oxford. Available at: <http://www.ophi. org.uk/wp-content/uploads/OPHI-HDCA-SS11-Intro-to-the-Capability-Approach-SA.pdf>. (accessed 23 June 2017).

Arora P (2016) Bottom of the data pyramid: Big data and the global south. *International Journal of Communication* 10: 19.

Aulakh G and Surabhi Agarwal N (2016) Google in talks with government to partner for Aadhaar, UPI. The Economic Times. Available at: <http://economictimes.india-times.com/opinion/interviews/google-in-talks-with-government-to-partner-for-aadhaar-upi-caesar-sengupta-vice-president-next-billion-users-at-google/articleshow/54556320.cms>. (accessed 28 September 2016).

BBC News (2015) Migrant crisis: "We would be lost without Google maps." Available at: <https://www.youtube.com/watch?v Zcr-GWv3Qbs>. (accessed 22 June 2017).

Binfield K (2015) Introduction. Writings of the Luddites.

Baltimore, MD: Johns Hopkins University Press.

Bowker GC and Star SL (1999) Sorting Things Out: Classification and Its Consequences. Cambridge: MIT Press. Brock G (2009) Global Justice: A Cosmopolitan Account. Oxford: Oxford University Press.

Broeders D (2009) Breaking Down Anonymity: Digital Surveillance of Irregular Migrants in Germany and the Netherlands. Amsterdam: Amsterdam University Press.

19 N.T.: As referências foram reproduzidas integralmente, mantendo-se a padronização e títulos conforme o artigo original.

Broeders D and Taylor L (2017) Does great power come with great responsibility? The need to talk about corporate polit- ical responsibility. The Responsibilities of Online Service Providers. New York: Springer, pp. 315–323.

Cho S, Crenshaw KW and McCall L (2013) Toward a field of intersectionality studies: Theory, applications, and praxis. Signs: Journal of Women in Culture and Society 38(4): 785–810.

Cohen JE (2012) Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. New Haven, CT: Yale University Press.

Creemers R (2016) What could China's "social credit system" mean for its citizens? Foreign Policy. Available at: <http://foreignpolicy.com/2016/08/15/what-could-chinas-social- credit-system-mean-for-its-citizens/>. (accessed 26 June 2017).

Dalton CM, Taylor L and Thatcher J (2016) Critical data studies: A dialog on data and space. Big Data & Society 1–9. doi: 10.1177/2053951716648346.

Dencik L, Hintz A and Cable J (2016) Towards data justice? The ambiguity of anti-surveillance resistance in political activism. Big Data & Society 3(2): 1–12.

Eubanks V (2014) Want to predict the future of surveillance? Ask poor communities. The American Prospect, pp. 1–4. Available at: <http://prospect.org/article/want-predict-future- surveillance-ask-poor-communities#.VXbsO_Oh2k8.twitter>. (accessed 9 October 2017).

European Commission (2016) Digital Agenda for Europe. Available at: <https://europa.eu/european-union/file/1497/ download_en?token KzfSz-CR>.

Floridi L (2014) Open data, data protection, and group priv- acy. Philosophy and Technology 27: 1–3.

Floridi L (2016) On human dignity as a foundation for the right to privacy. Philosophy and Technology 1(6). Available at: <https://www.youtube.com/watch?v=CD5zfBcAHms>. (accessed 9 October 2017).

Foucault M (1977) Discipline & punish – Panopticism. Discipline and Punish: The Birth of the Prison. New York: Vintage, pp. 195–228.

Gagliardone I (2014) "A country in order": Technopolitics, nation building, and the development of ICT in Ethiopia. Information Technologies and International Development 10(1): 3–19.

Gilliom J (2001) Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy. Chicago, IL: University of Chicago Press.

Greenfield A (2013) Against the Smart City: A Pamphlet. Do Projects.

Hannah M (2010) Dark Territory in the Information Age: Learning from the West German Census Controversies of the 1980s. Burlington, NJ: Ashgate.

Heeks R (2010) Development 2.0: The IT-enabled transformation of international development. Communications of the ACM2 53(4): 22–24.

Heeks R and Renken J (2016) Data Justice for Development: What Would It Mean? Manchester. Available at: <https://www.gdi.manchester.ac.uk/research/publications/other-working-papers/di/di-wp63/>. (accessed 9 October 2017).

Holvast J (2013) De Volkstelling van 1971. Amsterdam: Uitgeverij Paris.

ITU (2015) Key ICT indicators for developed and developing countries and the world (totals and penetration rates). Available at: <https://www.itu.int/en/ITU-D/Statistics/.../2014/ITU_Key_2005-2014_ICT_data.xls>. (accessed 9 October 2017).

Jayaram M (2014) India's big brother project. Boston Review. Available at: <http://www.bostonreview.net/world/mala-vika-jayaram-india-unique-identification-biometrics>. (accessed 1 January 2016).

Jiwani Y (2015) Violating in/visibilities: Honor killings and interlocking surveillance(s). In: Dubrovsky RE and Magnet SA (eds) Feminist Surveillance Studies. Durham, NC and London: Duke University Press, pp. 79–92.

Johnson J (2014) From open data to information justice. Ethics and Information Technology 16(4): 263–274.

Johnson J (2016) The question of information justice. Communications of the ACM 59(3): 27–29.

Kang LHY (2015) Surveillance and the work of anti-traffick- ing: from compulsory examination to international coord- ination. In: Dubrofsky RE and Magnet SA (eds) Feminist Surveillance Studies. Durham, NC and London: Duke University Press, pp. 39–57.

Kassam A (2017) Refugees crossing into Canada from US on foot despite freezing temperatures. The Guardian. Available at: <https://www.theguardian.com/world/2017/feb/07/us-refugees-canada-border-trump-travel-ban>. (accessed 26 June 2017).

Keeter S (2012) Survey research, its new frontiers, and dem- ocracy. Public Opinion Quarterly 76(3): 600–608.

Kitchin R (2016) The ethics of smart cities and urban science. Philosophical Transactions of the Royal Society A 374(2083): 1–15.

Kleine D (2010) ICT4WHAT? – Using the choice framework to operationalise the capability approach to development. Journal of International Development 22(5): 674–692.

Kleine D (2011) The capability approach and the "medium of choice": Steps towards conceptualising information and communication technologies for development. Ethics and Information Technology 13(2): 119–130.

Kroll JA, et al. (2016) Accountable algorithms. University of Pennsylvania Law Review 165(633): 633–705.

Kwan M (2016) Algorithmic geographies: Big data, algorithmic uncertainty, and the production of geographic know- ledge. Annals of the American Association of Geographers 106(2): 274–282.

Lemke T (2001) "The birth of bio-politics": Michel Foucault's lecture at the College de France on neo-liberal governmentality. Economy and Society 30(2): 190–207.

Levin K, et al. (2012) Overcoming the tragedy of super wicked problems: Constraining our future selves to ameliorate global climate change. Policy Sciences 45(2): 123–152.

Lyon D (2007) Surveillance Studies: An Overview. Cambridge: Polity Press.

Makulilo AB (2016) "A person is a person through other persons" – A critical analysis of privacy and culture in Africa, Beijing Law Review 7: 192–204.

Mann L (2016) Corporations left to other peoples' devices: A political economy perspective on the big data revolution in development. Development and Change. Epub ahead of print. doi: 10.1111/dech.12347.

Masiero S (2016) Digital governance and the reconstruction of the Indian anti-poverty system. Oxford Development Studies 818: 1–16.

Masiero S (2017) Will Aadhaar help the poor become cash- less? LiveMint. Available at: <http://www.livemint.com/Opinion/Mj3KgqCK1cZ2hbZYwbvE9H/Will-Aadhaar-help-the-poor-become-cashless.html> (accessed 15 February 2017).

Moore LJ and Currah P (2015) Legally sexed: Birth certificates and transgender citizens. In: Dubrovsky RE and Magnet SE (eds) Feminist Surveillance Studies. Durham, NC and London, pp. 58–78.

Nilekani N (2013) Technology to leapfrog development: The Aadhaar experience. Available at: <http://www.cgdev.org/sites/default/files/nandan-nilekani-sabot-lecture-tran-script-technology-leapfrog-development.pdf>. (accessed 9 October 2017).

Nussbaum M and Sen A (1993) The Quality of Life. Oxford: Oxford University Press.

Nussbaum MC (2006) Frontiers of Justice: Disability, Nationality, and Species Membership. Cambridge, MA: Harvard University Press.

O'Neil C (2016) Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Crown Publishing Group.

Panikkar R (1982) Is the notion of human rights a western concept? Diogenes 30(120): 75–102.

Priya S and Priya A (2016) Even in Delhi, basing PDS on Aadhaar is denying many the right to food. The Wire. Available at: <https://thewire.in/75359/right-to-food-how-aadhaar-in-pds-is-denying-rights/>. (accessed 8 February 2017).

Ram A (2015) Smartphones bring solace and aid to desperate refugees. Wired. Available at: <https://www.wired.com/ 2015/12/smartphone-syrian-refugee-crisis/>. (accessed 22 June 2017).

Raymond NA (2016) Beyond "do no harm" and individual consent: Reckoning with the emerging ethical challenges of civil society's use of data. In: Taylor L, Floridi L and van der Sloot B (eds) Group Privacy: New Challenges of Data Technologies. Springer International, pp. 67–82.

Sabhikhi IA (2016) Aadhaar in MGNREGA is likely to be hugely disruptive for workers. The Wire. Available at: <https://thewire.in/102103/aadhaar-mgnrega-errors-corruption/>. (accessed 8 February 2017).

Schwartz PM and Solove DJ (2011) The PII problem: Privacy and a new concept of personally identifiable information. New York University Law Review 86: 1814.

Sen A (1999) Development as Freedom. New York: Random House.

Sen A (2005) Human rights and capabilities. Journal of Human Development 6(2): 151–166.

Shearmur R (2015) Dazzled by data: Big Data, the census and urban geography. Urban Geography 36(7): 965–968.

Spivak GC (1988) Can the subaltern speak? In: Nelson C and Grossberg L (eds) Marxism and the Interpretation of Culture. University of Illinois Press, pp. 271–313.

Taylor L (2016a) From zero to hero: How zero-rating became a debate about human rights. IEEE Internet Computing 20(4): 79–83.

Taylor L (2016b) No place to hide? The ethics and analytics of tracking mobility using

mobile phone data. Environment and Planning D: Society and Space 34(2): 319–336.

Taylor L (2016c) Safety in numbers? Group privacy and big data analytics in the developing world. Group Privacy: New Challenges of Data Technologies. Dordrecht: Springer.

Taylor L (2016d) The ethics of big data as a public good: Which public? Whose good? Philosophical Transactions of the Royal Society A 374: 1–13.

Taylor L and Broeders D (2015) In the name of development: Power, profit and the datafication of the global South. Geoforum 64(4): 229–237.

Thatcher J (2014) Living on fumes: Digital footprints, data fumes, and the limitations of spatial big data. International Journal of Communication 8: 19.

Thikkavarapu PP (2016) The Aadhaar bill is yet another legislation that leaves too much power with the govern- ment at the centre. The Caravan. Available at: <http://www. caravanmagazine.in/vantage/aadhaar-bill-another-legistlation-leaves-power-centre>. (accessed 22 June 2017).

Tribunales Colegiados del Circuito. Gaceta del Seminario Judicial de la Federación, De cima Época, Tomo II, Libro 20, July 2015, p.1719, Tesis 11.1o.29 P (10a), Registro 2009626.

Turow J, Hennessy M and Draper N (2015) The tradeoff fallacy: How marketers are misrepresenting American con- sumers and opening them up to exploitation. Epub ahead of print 2015. DOI: 10.2139/ssrn.2820060. Available at: <http://dx.doi.org/10.2139/ssrn.2820060>. (accessed 9 October 2017).

UN General Assembly (1948) Universal declaration of human rights. United Nations, 1–6.

United Nations (2014) A world that counts: Mobilising the data revolution for sustainable development. New York. Available at: <http://www.undatarevolution.org/wp-content/uploads/2014/12/A-World-That-Counts2.pdf>. (accessed 9 October 2017).

Unwin PTH (2009) ICT4D: Information and Communication Technology for Development. Cambridge: Cambridge University Press.

World Economic Forum (2011) Personal data: The emergence of a new asset class. New York. Available at: <http://www3.weforum.org/docs/WEF_ITTC_ PersonalDataNewAsset_Report_2011.pdf>. (accessed 9 October 2017).

Yadav A (2016) In Rajasthan, there is "unrest at the ration shop" because of error-ridden Aadhaar. Scroll.in. Available at: <http://scroll.in/article/805909/in-rajasthan- there-is-unrest-at-the-ration-shop-because-of-error-ridden-aadhaar> (accessed 9 October 2017).

O DESAFIO DA LGPD PARA AS **DEFENSORIAS PÚBLICAS** NO BRASIL

O DESAFIO DA LGPD PARA AS DEFENSORIAS PÚBLICAS NO BRASIL[1]

RAFAEL A. F. ZANATTA[2]
MARINA S. KITAYAMA[3]

Introdução

O presente ensaio tem, como objetivo, discutir o impacto da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) para as Defensorias Públicas, levando em consideração três aspectos centrais: (i) a aplicação da LGPD para as atividades de tratamento de dados realizadas pelas Defensorias, (ii) os cuidados com os dados pessoais de seus usuários e (iii) as oportunidades do uso de dados pessoais para atividades-fim e atividades-meio das Defensorias Públicas.

O enfoque nas Defensorias Públicas é importante por três motivos. O primeiro ponto a ser considerado é a própria missão e atribuição legal do órgão, encarregado pela defesa de direitos daqueles que se encontram em situação de vulnerabilidades[4]. As Defensorias são guardiãs de uma quantidade vultosa de dados

1 O presente ensaio foi produzido a partir do projeto "Defensorias Públicas e LGPD", coordenado por Bruno R. Bioni e Rafael A. F. Zanatta pela Associação Data Privacy Brasil de Pesquisa. O projeto é financiado pela Fundação Ford por um período de dois anos (2020-2022). Para elaboração deste ensaio, nos beneficiamos das discussões com Adriana Britto, Bruno Bioni, Estela Guerrini, Florisvaldo Fiorentino Junior, Luiz Fernando Baby, Juliana Belloque, Rafael Pitanga, Rodrigo Pacheco, Maria Tereza Sadek, Thomaz Fiterman Tedesco e os participantes do evento "Proteção de dados pessoais e o papel das Defensorias", realizado em 02 de setembro de 2020 pelas Defensorias do Estado de São Paulo e Rio de Janeiro, em parceria com a Associação Data Privacy Brasil de Pesquisa. Somos gratos aos debates e discussões que iluminaram este ensaio. A responsabilidade pelos erros e ausências de clareza é exclusivamente nossa. Originalmente publicado em ZANATTA, Rafael; KITAYAMA, Marina. Os desafios da LGPD para as Defensorias Públicas no Brasil, in: Lei Geral de Proteção de Dados e o Poder Público / organizadores: Daniela Copetti Cravo; Daniela Zago Gonçalves da Cunda; Rafael Ramos. – Porto Alegre : Escola Superior de Gestão e Controle Francisco Juruena ; Centro de Estudos de Direito Municipal, 2021, p. 172-185.

2 Doutorando pelo Instituto de Energia e Ambiente da USP. Mestre em Direito pela USP. Mestre em Direito e Economia Política pela Universidade de Turim. Diretor da Associação Data Privacy Brasil de Pesquisa.

3 Graduanda em Direito pela USP. Pesquisadora da Associação Data Privacy Brasil de Pesquisa.

4 RIBEIRO, Marcia Carla Pereira; DE PAULA MACHADO, José Alberto Oliveira. Acesso à Justiça e a Defensoria Pública na América Latina: democratização de direitos como desenvolvimento. Direito e Desenvolvimento, v. 8, n. 1, p. 89-106, 2017.

pessoais, muitos dos quais, sensíveis. O perfil do público atendido corresponde, também, ao perfil daqueles que mais sofrem das lesões causadas pelo uso abusivo de dados pessoais, seja em virtude de processos de tomada de decisões automatizadas discriminatórias, seja em virtude do assédio de empresas que colocam a privacidade de seus consumidores em detrimento do acesso "gratuito" de serviços. A população assistida, tipicamente marcada por desigualdades e exclusão[5], tende a ser afetada de forma mais severa pela digitalização da sociedade. Como argumentado por Virginia Eubanks, populações socialmente vulneráveis são alvo de mais vigilância e controle, alimentando um "feedback looping" de automação e injustiças[6]. Esse quadro exige uma reflexão renovada para as Defensorias sobre as condições de igualdade e uma ordem jurídica justa[7].

Um segundo motivo advém da sua constituição, enquanto órgão do poder público e integrante do sistema de justiça, o que, por lei, traz uma série de implicações sobre sua forma de atuação. Notoriamente, tais particularidades trazem impactos diretos sobre o modo como as Defensorias terão que lidar com o tratamento dos dados pessoais que lhes são confiados. Contudo, até o presente momento, pouco material foi produzido no que diz respeito à proteção de dados e as especificidades do poder público, com exceção dos trabalhos de Miriam Wimmer, que reconhece que "no setor público, o tratamento de dados pessoais não se inicia, em geral, a partir de uma decisão voluntária do titular, mas como decorrência das exigências do próprio pacto social"[8].

O terceiro motivo que justifica o enfoque é o recente protagonismo das Defensorias Públicas nas discussões de proteção de dados pessoais. Isso é notável em razão da quantidade de eventos sobre LGPD organizados por Defensorias Públicas, o anúncio de estruturação de "encarregados pela proteção de dados pessoais" dentro das Defensorias e a participação ativa de Defensorias em ações civis públicas que questionam uso abusivo de dados pessoais, na prestação de serviços públicos. Esse engajamento demandará um compromisso interno com a LGPD, considerando

5 SILVA, Michelle Valéria Macedo et al. Direitos humanos. Acesso à justiça. Defensoria pública. Pobreza. Exclusão social. Revista da Defensoria Pública da União, n. 06, 2013.

6 EUBANKS, Virginia. Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press, 2018.

7 SADEK, Maria Tereza. A Defensoria Pública no sistema de justiça brasileiro. São Paulo: APADEP em Notícias, p. 2-2, 2008. SADEK, Maria Tereza. Acesso à justiça: um direito e seus obstáculos. Revista USP, n. 101, p. 55-66, 2014.

8 WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades. Revista dos Advogados da AASP, n. 144, nov., 2019, p. 127.

que sua vigência teve início em setembro de 2020 em caráter definitivo.

Organizamos o ensaio em três partes. Na primeira, explicamos o escopo de aplicação da LGPD. Na segunda, analisamos a importância da proteção de dados pessoais para atividade meio. Na terceira, analisamos como a LGPD afeta as atividades-fim das Defensorias. Argumentamos que é preciso enfrentar a complexidade da tarefa de conformidade com a LGPD dentro das Defensorias Públicas e a importância dessa agenda para uma visão renovada do acesso à justiça e fortalecimento da cidadania no Brasil[9].

O escopo da aplicação da LGPD para as Defensorias Públicas

A primeira razão que torna essencial a discussão da Lei Geral de Proteção de Dados no âmbito das Defensorias Públicas brasileiras é o próprio escopo de aplicação da normativa. Como remete seu nome, a Lei 13.709/2018 se propõe a abraçar de forma ampla as atividades de tratamento de dados pessoais, transformando o paradigma legal anterior, em que a matéria encontrava-se regulamentada de forma esparsa através de microssistemas setoriais[10].

Conforme disposto pela própria LGPD, esta se aplica sobre todo o tipo de tratamento de dados pessoais realizado por pessoa física ou jurídica, de direito público ou privado[11], independentemente do meio, dentro de território nacional ou com o objetivo de gerar oferta de bens e serviços neste. O texto traz poucas exceções de aplicação da Lei, previstas de forma taxativa em seu art. 4º, a LGPD se coloca como não aplicável às atividade de tratamento para fins exclusivamente particulares e não econômicos (art. 4º, I), fins jornalísticos e artísticos (art. 4º, II),

9 Nos referimos, evidentemente, aos trabalhos de Maria Tereza Sadek e acadêmicos do campo do acesso à justiça no Brasil. Ver nota acima.

10 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Forense, 2020, p. 103.

11 Ao analisar a redação da LGPD, Wimmer argumenta que "a lei incorre em graves imprecisões técnicas, utilizando de maneira aparentemente intercambiável termos como Administração Pública, Poder Público e pessoas jurídicas de Direito Público". Para Wimmer, "o conceito de Poder Público é mais amplo que o de Administração Pública, visto que engloba também os Poderes Legislativo e Judiciário". WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades, Revista dos Advogados da AASP, n. 144, nov., 2019, p. 130.

ou exclusivos de segurança pública e do Estado, defesa nacional e atividades de investigação criminal (art. 4º, III)[12].

Observada a amplitude de aplicação da normativa, percebe-se que, assim como a enorme maioria das instituições públicas e privadas, as Defensorias estão, inevitavelmente, submetidas aos ditames da LGPD, ficando sujeitas à fiscalização por parte da ANPD e à imposição do poder jurisdicional de outros entes competentes à julgar a matéria.

A constatação traz implicações profundas às Defensorias Públicas considerando sua complexidade de organização funcional e administrativa, assim como pela quantidade de dados pessoais por ela tratados. Enquanto órgão integrante do sistema de justiça, as Defensorias tem atuação sob a égide da legalidade e estão vinculadas a princípios diversos, o que, por si, já resulta na necessidade de um tratamento de dados específico. Sujeita à prestação de contas, por exemplo, além das finalidades principais da coleta, o órgão tem que levar em consideração seus usos secundários, como produção de relatórios, ou seja, nem sempre será possível eliminar informações logo que encerrada a finalidade primeira do tratamento.

Fora isso, em um país marcado por profundas desigualdades, a atribuição das Defensorias, sendo a de defesa de direitos daqueles em situação de vulnerabilidade, torna inevitável que o órgão detenha uma quantidade massiva de dados pessoais, como já observado por Defensores Públicos que escreveram sobre a LGPD[13]. Considerando que, diante a escassez de recursos, as Defensorias têm que criar critérios que determinem quem receberá atendimento, a grande maioria daqueles que buscam seus serviços tem de passar pelo procedimento de triagem socioeconômica, o que implica na coleta de enormes quantidades de dados de renda do indivíduo e de integrantes de seu núcleo familiar.

Este importante papel institucional desempenhado pelas Defensorias traz, para além dos trabalhos de se adequar à LGPD, o desafio de se consolidar enquanto ente apto a defender as disposições legais nele previstas, uma jornada dupla e de alta complexidade.

12 Conforme disposto no art. 4º, §1º, a hipótese será regulamentada por legislação específica, devendo observar os princípios gerais de proteção de dados e os direitos dos titulares previstos na Lei 13.709/18.

13 SILVA, Franklyn R. Alves. A LGPD e o tratamento de dados dos assistidos pela Defensoria Pública. Consultor Jurídico, março de 2020. Disponível em: <**https://www.conjur.com.br/2020-mar-31/tribuna defensoria-lgpd-tratamento-dados-assistidos-defensoria**>. FEICHAS, Roger. Principais Regras da LGPD para a Defensoria Pública. JusBrasil, maio de 2020. Disponível em: <https://professorrogerfeichas.jusbrasil.com.br/artigos/847086836/principais-regras-da-lgpd-para-a defensoria-publica>. Acesso em> 13 set. de 2020.

Do atendimento aos dados sensíveis: preocupações com atividade-meio das Defensorias Públicas

Tomando como o ponto de partida a própria adequação das Defensorias Públicas às previsões da LGPD, a complexidade da tarefa se evidencia pela robustez e importância do ente. O Brasil possui um sistema legal com muitos elementos que o tornam único. Para além de uma longa tradição no que diz respeito a direitos coletivos, criados durante os movimentos sociais da década de 80[14], o judiciário brasileiro é um dos poucos do mundo equipado com um ente público, cuja função é a defesa de direitos da população em situação de vulnerabilidade social ou econômica. A maioria dos estados desenvolveu as estruturas de suas Defensorias Públicas, a partir dos anos 50, sendo a primeira delas a do estado do Rio de Janeiro. Hoje, há dezenas de unidades espalhadas pelo país, as quais, juntas, representam uma camada extremamente importante da justiça social do sistema jurídico brasileiro.

De acordo com cientistas políticos[15], existem três razões principais que tornam as Defensorias Públicas brasileiras um órgão de relevância especial. A primeira delas é o fato de o Brasil ser um dos poucos países da América-Latina a possuir a instituição constitucional de um serviço público que promova assistência jurídica à população vulnerável. Em segundo lugar, dado os altos índices de desigualdade social, quase 90% da população brasileira está enquadrada dentro dos critérios da justiça gratuita, sendo o principal deles o de renda familiar de até três salários mínimos (IBGE, 2010)[16]. A terceira razão é a existência recente da instituição, de modo que, apesar de ser um órgão relativamente jovem (segunda metade do século XX), já se apresenta como um relevante ator político, especialmente no sistema de justiça.

Considerando o cenário brasileiro de desigualdades sociais e regionais gritantes a expectativa de que sejam altos os números de atendimentos realizados pelas Defensorias se confirma. Completando apenas dez anos em 2016, a De-

14 ZANATTA, Rafael. Tutela coletiva e coletivização da proteção de dados pessoais, In: PALHARES, Felipe (org.), Temas Atuais de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2020, p. 345-374.

15 MADEIRA, Lígia Mori. Institutionalisation, Reform and Independence of the Public Defender's Office in Brazil. Brazilian Political Science Review, v. 8, n. 2, p. 48-69, 2014.

16 Disponível em: <https://migalhas.uol.com.br/quentes/318863/parana-e-o-estado-com-menos_defensores-publicos-por-habitante-no-brasil>. Acesso em: 15 set. de 2020.

fensoria Pública Estadual de São Paulo já havia realizado mais de 10 milhões de atendimentos, com média atual de 1,5 milhões de atendimentos por ano[17].

Defensorias Públicas de estados com índices demográficos menores também apresentam números que denotam a magnitude da quantidade de informações tratadas diariamente por esses órgãos, a DPE-RS, apenas entre os dias 18 de março e 30 de junho de 2020, período pandêmico, realizou mais 200 mil atendimentos, sua grande maioria, de forma remota[18].

Afora a quantidade massiva de atendimentos e, consequentemente, de dados pessoais tratados, ainda deve-se somar o processo de digitalização da sociedade. Acelerado pela crise do COVID 19, esse processo acentua uma série de desigualdades e torna extremamente desafiador o trabalho das Defensorias Públicas, no Brasil, sendo uma das consequências imediatas do isolamento social a necessidade de digitalização de seu atendimento. A instituição, sem ferramentais tecnológicos próprios para tanto, se viu obrigada a encontrar soluções alternativas disponíveis no mercado, as quais eram, muitas vezes, financeiramente bancadas pelos próprios defensores. Tornaram-se ferramentas padrão para o trabalho das Defensorias o armazenamento em nuvem, uso de drives compartilhados e de meios de comunicação por aplicativos. Apesar de ser a solução disponível em tempo, é notório que esta não se configura como a ideal na perspectiva de longo prazo, considerando a quantidade e a qualidade de dados pessoais tratados pelo ente.

Em síntese, as preocupações com a atividade-meio giram em torno de alguns problemas comuns: (i) os processos de atendimento automatizados e novas intermediações na relação entre Defensores e usuários, (ii) a utilização de sistemas integrados para fluxo de dados e compartilhamento de dados entre Defensorias[19], (iii) a necessidade de categorização de dados sensíveis e criação de regras de segurança de informação, garantindo princípios de "*need to know*" e necessidade do tratamento de dados pessoais para viabilizar acessos a determinados sistemas por servidores, estagiários, voluntários, e outros profissionais, (iv) a obtenção de

17 Disponível em: <**https://www.conjur.com.br/2016-jan-09/15-milhao-atendimentos-ano-defensoria-sp faz-10-anos**>. Acesso em: 20 set. de 2020.

18 Disponível em: <**http://www.defensoria.rs.def.br/mais-de-200-mil-atendimentos-e-aumento-nos pedidos-de-pensao-como-foram-esses-100-dias-de-pandemia-na-defensoria-publica**>. Acesso em: 20 set. de 2020.

19 Como observa um Defensor, "é muito comum que a Defensoria Pública de um Estado atue em favor de parte que resida em outra unidade federativa ou que haja declínio de atribuição, exigindo-se que as instituições sejam capazes de migrar seus dados entre si para a manutenção do serviço de assistência jurídica". SILVA, Franklyn R. Alves. A LGPD e o tratamento de dados dos assistidos pela Defensoria Pública. Consultor Jurídico, março de 2020.

base legal adequada para armazenamento dos dados pessoais e utilização para fins de pesquisa, bem como utilização em litígios estratégicos e situações onde os Defensores precisam "argumentar com base em dados".

Essa situação ilustra a centralidade das Defensorias Públicas no sistema de justiça e o conjunto enorme de preocupações com a LGPD com relação às atividades-meio das Defensorias.

Litígios estratégicos e atuação dadocêntrica: atividades-fim das Defensorias Públicas

A jornada continua sob a perspectiva da atividade fim das Defensorias, órgão cujo papel primordial é a defesa de direitos, incluindo direitos fundamentais relativos e relacionados à proteção de dados. Conforme redação da Constituição Federal, após a Emenda Constitucional 80/2004, a Defensoria Pública é instituição permanente, essencial à função jurisdicional do Estado, cabendo-lhe, como expressão e instrumento do regime democrático, "a orientação jurídica, a promoção dos direitos humanos e a defesa, em todos os graus, judicial e extrajudicial, dos direitos individuais e coletivos, de forma integral e gratuita, aos necessitados" (art. 134, CF88).

A LGPD invoca questões ainda mais relevantes àqueles em situação de vulnerabilidade social ou econômica, perfil do público atendido pelas Defensorias. O direito à proteção de dados se consolida enquanto fundamental[20] pelos bens que tutela, dentre eles a dignidade humana, a liberdade e a privacidade[21], os quais são reiteradamente violados e ignorados, tratando-se de segmentos populacionais estigmatizados. Diante do papel central que os dados desempenham na sociedade atual, a matéria da proteção de dados se propõe como o meio que irá legitimar o tratamento de dados, estipulando critérios para conter seus potenciais danos, tais quais a acentuação de práticas discriminatórias.

Esse processo de acentuação de estigmas e discriminações é amplamente

20 SUPREMO TRIBUNAL FEDERAL. Voto da Relatora, MIN. ROSA WEBER. Ações Diretas de Inconstitucionalidade número 6387, 6388, 6389, 6390 e 6393. Julgamento de liminar com pedido de suspensão dos efeitos da Medida Provisória n. 954/2020. DJe. 07.05.2020.

21 RODOTÀ, Stefano. Org. BODIN, Maria Celina. Trad. DONEDA, Danilo e DONEDA, Luciana. A vida na sociedade de vigilância, a privacidade hoje. Rio de Janeiro: Renovar, 2008, p.17-19.

discutido no que toca ao uso de ferramentas de tomadas decisões automatizadas. Tais tecnologias se fundamentam a partir da modelagem de perfis comportamentais e análises estatísticas que se operam replicando padrões sociais identificados pelas informações com que as máquinas são alimentadas. Um exemplo disso são os sistemas de modelagem de crédito, que a partir dos dados pessoais de uma gama de indivíduos cria uma série de perfis de "risco"[22]. Nesse exemplo, aquele que será avaliado para tomar crédito não o é, exclusivamente, pelos seus dados enquanto um bom ou um mau pagador, mas também pela sua identificação dentro de um perfil comportamental predeterminado. Tais perfis podem ser compostos por informações das mais diversas, não se restringindo a dados de pagamento do consumidor. Eles podem incluir hábitos de compra, dados demográficos, faixa etária, entre muitos outros de difícil apreensão, já que os algoritmos de alta complexidade são capazes de criar seus próprios códigos, tornando-se verdadeiras caixas pretas[23]. Assim, da forma como operam, as técnicas de *credit scoring* sem uma devida observância dos ditames da proteção de dados, poderiam induzir e acentuar processos discriminatórios de uma maneira que é ainda pouco transparente[24].

As pressões de mercado por um acesso amplo e facilitado de dados de crédito são um forte sinalizador de que a pauta merece atenção. Recentemente, a Lei do Cadastro Positivo passou por alterações de impacto profundo, na forma como as gestoras de bancos de dados obtém informações de pagamento.[25] A reforma alterou um ponto chave e que era há tempos uma demanda do mercado, ao invés do consumidor ter que, por padrão, dar o aceite sobre o compartilhamento de dados de compra, o compartilhamento tornou-se a regra e a recusa passou a ficar sujeita à manifestação do consumidor[26]. Cabe, ainda ressaltar uma particularidade da Lei Geral brasileira que possui, diferentemente de sua "equivalente" europeia, a GPDR, uma base legal própria que legitima o tratamento de dados com fins de proteção ao crédito, art. 7º, X da LGPD, o que é um indicativo da força que este

22 ZANATTA, Rafael. Pontuação de crédito e direitos dos consumidores: o desafio brasileiro. São Paulo: Idec, 2017.

23 PASQUALE, Frank. The Black Box Society. The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

24 ZANATTA, Rafael; DONEDA, Danilo. O que há de novo no debate sobre "credit score" no Brasil? Jota.info, 2017. Disponivel em: <**https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de dados/o--que-ha-de-novo-no-debate-credit-score-no-brasil-09022017**>. Acesso em: 20 nov.de 2020.

25 O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. Nova York: Crown, 2016, C. 8.

26 BESSA, Leonardo Roscoe. Nova Lei do Cadastro positivo. São Paulo: Revista dos Tribunais, 2019.

mercado possui no contexto nacional.

Os potenciais riscos discriminatórios são, ainda, agravados pela forma como operam muitos dos modelos de negócios de empresas digitais, as quais oferecem serviços em troca da atenção ou dos dados pessoais de seus consumidores[27]. Não se pode ignorar a interpretação de que esta forma de permuta é positiva, ao permitir o acesso a serviços àqueles que não poderiam arcar financeiramente com seus custos. Os dilemas são, entretanto, mais profundos. Importa saber como e para que esses dados estejam sendo utilizados, verificando se há riscos de tais informações servirem para prejudicar o titular. Eventuais abusos no uso dos dados podem representar maiores perdas futuras do que benefícios imediatos.

Fora isso, há ainda situações que obrigam a população que não pode pagar por determinados serviços a abdicar de sua autodeterminação informativa. Em 2017[28], o governo municipal de São Paulo pretendia tornar obrigatório o cadastramento dos usuários das redes de Wi-fi público da cidade, isso porque a própria estrutura de fornecimento da rede pública seria financiada por entes privados, que utilizariam das informações para fins de marketing direcionado. O caso leva a questionamentos sobre a legalidade de vincular o serviço público ao compartilhamento de dados, considerando que este deveria ser garantido de forma gratuita pelo Estado.

Indagações semelhantes foram levantados no caso da Linha 4 do Metrô de São Paulo[29]. A concessionária do trecho instalou câmeras de identificação de expressões e emoções dos usuários do metrô, o que permitia a mensuração de impacto das publicidades transmitidas aos indivíduos. O Instituto Brasileiro de Defesa do Consumidor moveu um processo contra a prática da concessionária, contando com a assistência litisconsorcial da DPE-SP. A tese defendida pelos entes é justamente a da abusividade de sujeitar aqueles que não têm escolha de usar ou não o transporte público a estarem sujeitos a tal situação. Os serviços públicos consistem em atividades de cunho essencial, de modo que não há como garantir a autodeterminação informativa do titular quando a oferta de um serviço desta ordem é posta em detrimento ao compartilhamento de dados.

27 WU, Tim. The attention merchants: the epic scramble to get inside our heads. Nova York: Knopf, 2016.

28 BIONI, Bruno. Expansão do Wi-Fi público à custa de dados pessoais. Disponível em: <https://genjuridico.jusbrasil.com.br/artigos/544067877/expansao-do-wi-fi-publico-as-custas-de_dados-pessoais>. Acesso em: 20 nov.de 2020.

29 Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2018/08/31/concessionaria-do-metro-de_sp-e-processada-por-painel-que-faz-reconhecimento-facil-de-passageiros.ghtml>. Acesso em: 20 nov. de 2020.

Diante do contexto de abusos e riscos a direitos fundamentais, uma Defensoria apta para atuar em defesa dos direitos à proteção de dados da população em situação de vulnerabilidade é, da perspectiva de seu papel institucional, de extrema relevância. Há, porém, ainda outro ponto relacionado à capacitação das Defensorias que tocam o exercício de suas atividades-fim. Espera se que o processo de adequação à Lei Geral de Proteção de Dados traga como consequência um uso mais consciente e organizado das informações controladas pelos órgãos, o que abre uma janela de oportunidades para uma atuação mais estratégica das Defensorias.

O processo de adequação à LGPD força as instituições a se organizarem, a verificarem dados coletados, armazenados, as razões do tratamento e seu fluxo informacional. A consequência direta disto é que se torna mais fácil verificar possibilidades de tornar úteis aquelas informações. Como exemplo prático de uso estratégico de dados, pode-se citar a atuação da DPE-RJ, que, constatando que o número de demandas relativas a vagas em creches mais que dobrou de um ano para outro, entrou com uma ação civil pública contra a prefeitura do Rio de Janeiro requerendo a criação de novas vagas[30]. Parafraseando Evgeny Morozov, que fala da existência de um "capitalismo dadocêntrico"[31], é crucial pensarmos nas possibilidades de uma litigância dadocêntrica, que se apoia em análises agregadas de dados pessoais como estratégia argumentativa e de convencimento de agentes decisórios em casos complexos.

Produzir estatísticas e entender padrões com base em dados abre margem para uma série de atuações estratégicas, como a percepção de perfis mais afetados por uma determinada demanda, casos repetidos que dariam margem à propositura de ações civis coletivas e ações civis públicas, além de servirem, também, enquanto argumentos a serem levados perante o judiciário, em formação de acordos ou para ações de incidência em políticas públicas.

A concepção de uma atuação nesse sentido caminha em consonância com a perspectiva ampla da missão das Defensorias, que deu mais espaço para a atuação do ente e transformou a antiga visão de que o papel do órgão seria fornecer um "advogado" para quem não pode arcar com um por meios próprios[32]. A instituição,

30 Disponível em: <**https://g1.globo.com/rio-de-janeiro/noticia/mais-de-30-mil-criancas-aguardam vagas-em-creches-do-rio.ghtml**>. Acesso em: 20 nov. de 2020.

31 MOROZOV, Evgeny; BRIA, Francesca. Rethinking the smart city. Democratizing Urban Technology. New York, NY: Rosa Luxemburg Foundation, 2018.

32 CONGRESSO NACIONAL. Lei Complementar nº 80, de 12 de janeiro de 1994. Organiza a Defensoria

para além de garantir a defesa de qualidade de seus usuários perante o judiciário, tem a missão de defender seus direitos em sentido lato, incluindo até mesmo questões relativas à educação em direitos. Em um país de desigualdades latentes e problemas sociais graves como o Brasil, cumprir esse papel é uma tarefa hercúlea e que demanda, diante recursos escassos, estratégias de atuação que permitam o maior alcance dentro das possibilidades financeiras disponíveis.

O domínio de informações sobre sua própria atuação é essencial, nesse sentido, razão pela qual um dos pontos centrais a ser ressaltado, no processo de adequação das Defensorias à LGPD, é o de enxergar o desafio como uma janela de oportunidades que permitirá ao ente dimensionar seu próprio trabalho, traçar planos de atuação e dominar informações que podem ser utilizadas diretamente na melhora de seu serviço.

Em síntese, os programas de governança de proteção de dados pessoais construídos pelas Defensorias Públicas nos próximos anos deverão levar em consideração: (i) de que modo a base legal de "exercício regular de direitos em processo judicial" poderá ser utilizada para legitimar tratamentos de dados pessoais dos usuários em litígios, (ii) quais informações devem ser prestadas sobre o uso agregado de informações para fins de pesquisa e de litigância estratégica, (iii) quais as possibilidades de armazenamento e retenção de dados pessoais para fins que não sejam específicos ao atendimento regular dos usuários, e (iv) quais técnicas de anonimização e pseudonimização podem ser mobilizadas para avançar em uma litigância dadocêntrica que não cause riscos significativos às liberdades civis e direitos fundamentais dos usuários, ao mesmo tempo que permitem uma atuação mais qualificada, estratégica e baseada em argumentos empíricos por parte dos Defensores Públicos.

Nesse sentido, programas de governança de dados não podem ser construídos a partir de modelos, templates, tabelas prontas e documentos ao estilo "copia e cola" produzidos pelo setor privado. Há uma necessidade de customização e de construção de programas de adequação à Lei Geral de Proteção de Dados Pessoais que levem em consideração as especificidades das Defensorias e a importância dos dados pessoais para atividades-meio e atividades-fim.

Pública da União, do Distrito Federal e dos Territórios e prescreve normas gerais para sua organização nos Estados, e dá outras providências.

Considerações finais

Os impactos da LGPD sobre entes do poder público merecem uma atenção própria. Não se podem ignorar as razões pelas quais há uma seção específica que disciplina a matéria para estes agentes. Observar tais prerrogativas não deve ser uma tarefa encarada enquanto um fim em si mesmo, pois as determinações da normativa objetivam a tutela de um bem jurídico e social. Nesse sentido, o Estado, que tem a função de garante de uma série serviços consagrados enquanto essenciais, deve servir de exemplo no tocante à proteção de dados pessoais dos cidadãos, considerando que todos estão, em certa medida, obrigados a confiar parte de sua personalidade ao poder público[33].

No tocante às Defensorias, a questão é ainda mais sensível. Um sistema de justiça que se pretenda justo deve garantir que todos os cidadãos tenham condições mínimas para defender seus direitos. Assim, a atribuição legal da Defensoria é de natureza essencialíssima. Em segundo lugar, a população atendida pelas Defensorias é, por atribuição constitucional, uma população em situação de vulnerabilidade, isso implica que estes indivíduos não têm à sua disposição uma miríade de opções à que possam recorrer e tampouco podem exercer plenamente a ideia de "controle sobre os próprios dados" e formas de negociação e declarações de vontade com base em "consentimento livre e informado". É preciso pensar em assimetrias informacionais, desigualdades e barreiras cognitivas que podem ressignificar a leitura do que é efetivamente consentimento, superando a ideia limitada de que esta é a única base legal para tratamento de dados pessoais de acordo com a LGPD.

Pensar no tratamento de dados nesse contexto deve ser uma razão a mais para que exista a máxima diligência e um programa de governança de excelência, não reduzindo aqueles que dependem da atuação do Estado a cidadãos de segunda categoria que devem abdicar de sua autodeterminação informativa para ter acesso a serviços básicos.

O dever de diligência sobressaltado do poder público torna significativo o desafio de sua conformação à LGPD, porém, ainda maior deve ser o olhar de que este processo se trata de uma oportunidade para que, organizando e sistematizando seu tratamento de dados, as funções desempenhadas pelas instituições estatais se deem de modo ainda mais eficiente e com ainda mais qualidade. Longe de oferecer respostas definitivas sobre como construir programas de adequação

dentro das Defensorias, o que problematizamos, neste ensaio, é a complexidade de tal tarefa e a necessidade de uma olhar atento às atividades-meio e atividades-fim, colocando em marcha um esforço coletivo de construção de programas robustos de adequação por parte de Defensores, servidores e profissionais de diversas áreas que fazem parte dessa instituição que é, ao mesmo tempo, agente de transformação e de justiça social no Brasil.

Referências

BESSA, Leonardo Roscoe. Nova Lei do Cadastro positivo. São Paulo: Revista dos Tribunais, 2019.

BIONI, Bruno Ricardo. Expansão do Wi-Fi público às custas de dados pessoais. Disponível em: <https://genjuridico.jusbrasil.com.br/artigos/544067877/expansao-do wi-fi-publico-as-custas-de-dados-pessoais>. Acesso em: 15 set. de 2020.

_____. Proteção de dados pessoais: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Forense, 2020.

EUBANKS, Virginia. Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press, 2018.

FEICHAS, Roger. Principais Regras da LGPD para a Defensoria Pública. JusBrasil, maio de 2020

MADEIRA, Lígia Mori. Institutionalisation, Reform and Independence of the Public Defender's Office in Brazil. Brazilian Political Science Review, v. 8, n. 2, p. 48-69, 2014.

MOROZOV, Evgeny; BRIA, Francesca. Rethinking the smart city. Democratizing Urban Technology. New York, NY: Rosa Luxemburg Foundation, 2018.

O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. Nova York: Crown, 2016.

PASQUALE, Frank. The Black Box Society. The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

RIBEIRO, Marcia Carla Pereira; DE PAULA MACHADO, José Alberto Oliveira. Acesso à Justiça e a Defensoria Pública na América Latina: democratização de direitos como desenvolvimento. Direito e Desenvolvimento, v. 8, n. 1, p. 89-106, 2017.

RODOTÀ, Stefano. Org. BODIN, Maria Celina. Trad. DONEDA, Danilo e DONEDA, Luciana. A vida na sociedade de vigilância, a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SADEK, Maria Tereza. Acesso à justiça: um direito e seus obstáculos. Revista USP, n. 101, p. 55-66, 2014.

SADEK, Maria Tereza. A Defensoria Pública no sistema de justiça brasileiro. São Paulo: APADEP em Notícias, p. 2-2, 2008.

SILVA, Franklyn R. Alves. A LGPD e o tratamento de dados dos assistidos pela Defensoria Pública. Consultor Jurídico, março de 2020.

SILVA, Michelle Valéria Macedo et al. Direitos humanos. Acesso à justiça. Defensoria pública. Pobreza. Exclusão social. Revista da Defensoria Pública da União, n. 06, 2013.

ZANATTA, Rafael; DONEDA, Danilo. O que há de novo no debate sobre "credit score" no Brasil? Jota.info, 2017.

ZANATTA, Rafael. Pontuação de crédito e direitos dos consumidores: o desafio brasileiro. São Paulo: Idec, 2017.

WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades, Revista dos Advogados da AASP, n. 144, nov., 2019, p. 127.

WU, Tim. The attention merchants: the epic scramble to get inside our heads. Nova York: Knopf, 2016.

LGPD E SISTEMA DE JUSTIÇA:
A VOZ E A VEZ DAS DEFENSORIAS PÚBLICAS

LGPD E SISTEMA DE JUSTIÇA: A VOZ E A VEZ DAS DEFENSORIAS PÚBLICAS[1]

BRUNO R. BIONI[2]
FLORISVALDO FIORENTINO JÚNIOR[3]
MARINA S. KITAYAMA[4]
RAFAEL A. F. ZANATTA[5]
RODRIGO BAPTISTA PACHECO[6]

Para o setor público, a LGPD representa um desafio particular

Desde sua entrada em vigor em setembro de 2020, a Lei Geral de Proteção de Dados (LGPD) tem sido uma questão amplamente discutida tanto no setor privado como no público. A Lei, promulgada em 2018, despertou nos agentes

1 Este artigo contempla alguns dos achados originados do Projeto "Defensorias Públicas e Proteção de Dados" da Associação Data Privacy Brasil de Pesquisa, que conta com a parceria das Defensorias Públicas dos estados do Rio de Janeiro e São Paulo e do Colégio Nacional de Defensores Públicos Gerais. Mais informações sobre os pontos aqui apresentados podem ser encontradas no guia "Primeiros Passos para a Adequação das Defensorias à LGPD", Disponível em: http://bit.ly/dprb_guia_defensorias_vf. Originalmente publicado no Jota. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-e-sistema-de-justica-a-voz-e-a-vez-das-defensorias-publicas-09062021>. Publicado em 09/06/2021.

2 Diretor da Associação Data Privacy Brasil de Pesquisa. Doutorando em Direito Comercial e Mestre em Direito Civil na Faculdade de Direito da Universidade de São Paulo. Foi study visitor do Departamento de Proteção de Dados Pessoais do European Data Protection Board/EDPB e do Conselho da Europa, pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa.

3 Florisvaldo Fiorentino Júnior é Defensor Público-Geral do Estado de São Paulo. Ingressou na carreira em 2007, já atuou na Unidade de Bauru, nas áreas criminal e infância e juventude, assumindo também as coordenações regional e da unidade. Foi Terceiro Subdefensor Público-Geral do Estado nos biênios 2016/2018 e 2018/2020.

4 Pesquisadora da Associação Data Privacy Brasil de Pesquisa. Graduanda na Faculdade de Direito da Universidade de São Paulo.

5 Diretor da Associação Data Privacy Brasil de Pesquisa. Doutorando pelo Instituto de Energia e Ambiente da USP. Mestre em Direito pela USP, onde foi coordenador do Núcleo de Direito, Internet e Sociedade. Mestre em Direito e Economia Política pela Universidade de Turim.

6 Rodrigo Pacheco é Defensor Público-Geral do Estado do Rio de Janeiro.

que realizam o tratamento de dados pessoais a necessidade de adequarem suas atividades, o que vai desde aspectos de segurança da informação à estipulação de políticas de governança de dados, além do constante desafio de identificar a base legal correta para diferentes tipos de tratamento de dados, nos termos do artigo 7º e 11º.

Apesar de implicar em mudanças em diferentes setores; no caso do setor público, a LGPD representa um desafio particular. Cabe ressaltar que para esses agentes a Lei estipula condutas e deveres específicos, aos quais dedica um capítulo próprio (capítulo IV), por vezes considerado confuso[7]. O equilíbrio em relação aos agentes públicos é delicado e exige atenção especial, uma vez que o setor é regido por objetivos e princípios próprios do interesse público. Esse ponto traz implicações importantes, pois, na maior parte das vezes, o poder público, diante de obrigações de prestação de contas e de transparência, deverá armazenar determinadas informações mesmo após encerrada a finalidade principal do tratamento de dados.

Mais que isso, no que toca à relação entre cidadão e estado, existe um claro desequilíbrio entre as partes, ou mesmo uma dependência, como ocorre no caso da prestação de serviços essenciais. A conjunção de tais fatores traz uma série de implicações à proteção de dados pessoais, dentre elas, a dificuldade de considerarmos o consentimento como hipótese legitimadora do tratamento de dados realizado pelo Estado[8]. É complexa a identificação da "manifestação livre, informada e inequívoca" de usuários de serviços públicos em situação de marginalização e opressão social e econômica.

Defesa de direitos e litigância dadocêntrica

As Defensorias, por seu turno, além de enfrentarem os desafios específicos do setor público, possuem outras particularidades que tornam ainda mais sensível

7 O artigo 23º indica que sua definição de pessoa jurídica de direito público corresponde àquela do art. 1º da Lei de Acesso à Informação (Lei 12.527/2011), desse modo, entende-se que há o enquadramento das Defensorias como um dos entes referidos no dispositivo, tendo em vista que, apesar de não ser expressamente citada pela LAI, a própria Defensoria compreende sua subordinação às sua previsões.

8 WIMMER, Miriam. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: BIONI, Bruno; SCHERTEL, Laura; DONEDA, Danilo; SARLET, Ingo; RODRIGUES, Otavio. Tratado de Proteção de Dados. Rio de Janeiro: Forense, 2021, p. 276.

sua relação com a matéria. Antes de tudo, as Defensorias são órgãos que colaboram ativamente com a defesa de direitos, de modo que para além de capacitarem-se a fim de promover a adequação da instituição à LGPD, também deverão habilitar-se para lidar com casos de violação à proteção de dados. Ou seja, a instituição está diante de um desafio duplo: o de adequarem-se à nova lei e o de atuarem na tutela dos direitos de proteção de dados da população.

O perfil do público atendido pelos órgãos corresponde também ao perfil daqueles que mais sofrem com as lesões causadas pelo uso abusivo de dados pessoais[9]. A correlação entre determinados perfis socioeconômicos e violações à proteção de dados é notável, seja em virtude de processos de tomada de decisões automatizadas discriminatórias, seja em virtude do assédio de empresas que colocam a privacidade de seus consumidores em detrimento do acesso "gratuito" de serviços. A população assistida, tipicamente marcada por desigualdades e exclusão[10], tende a ser afetada de forma mais severa pela digitalização da sociedade.

É nesse sentido que entende-se que os problemas de proteção de dados pessoais são problemas de ordem coletiva[11], o que torna as Defensorias Públicas um importante agente para a tutela desses direitos, considerando a ampla harmonização da LGPD com o pioneiro sistema de tutela coletiva no Brasil, inaugurado na década de 1980 e fortalecido pelo Código de Defesa do Consumidor. Desse modo, tomando como base também a crescente atuação das Defensorias em litígios coletivos, como no importante caso da adoção de soluções de reconhecimento facial no metrô de São Paulo[12], o ente tende a ser um dos protagonistas na defesa de direitos à proteção de dados.

Nos próximos anos, será crucial que as Defensorias Públicas possuam unidades específicas de proteção de dados pessoais e saibam trabalhar com litígios estratégicos mobilizados a partir do seu próprio conhecimento interno e uso correto de dados pessoais. Por isso entendemos que as Defensorias Públicas atuarão,

9 O'NEIL, Cathy. Algoritmos de Destruição em Massa: Como o Big Data Aumenta a Desigualdade e Ameaça a Democracia. Trad. Rafael Abraham. 1 ed. Santo André, SP: Rua do Sabão, 2020.

10 SILVA, Michelle Valéria Macedo et al. Direitos humanos. Acesso à justiça. Defensoria pública. Pobreza. Exclusão social. Revista da Defensoria Pública da União, n. 06, 2013.

11 ZANATTA, Rafael. Tutela coletiva e coletivização da proteção de dados. in: PALHARES, Felipe (org.). Temas Atuais de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2020, p. 345-374.

12 G1, Justiça dá 30 dias para que Metrô de SP esclareça projeto de câmeras de reconhecimento facial, G1 São Paulo, 12/02/2020. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2020/02/12/justica-da-30-dias-para-que-metro-de-sp-esclareca-projeto-de-cameras-de-reconhecimento-facial.ghtml>.

cada vez mais, por meio de uma "litigância dadocêntrica[13]". A LGPD pode ser um reforço duplo. Ao instrumentalizar o uso correto de dados pessoais para fins de proteção de direitos, amplia a capacidade de litígios estratégicos que mobilizem dados dos próprios usuários dos serviços das Defensorias Públicas.

As transformações das Defensorias Públicas diante da LGPD

Além dos desafios de capacitação para defesa de direitos previstos na LGPD, as Defensorias Públicas também enfrentam o processo de sua própria adequação aos termos da lei. Nesse sentido, uma das dificuldades enfrentadas é a pouca quantidade de material até então produzido sobre proteção de dados no setor público[14]. Isso porque o desenvolvimento de programas de adequação de órgãos públicos da complexidade das Defensorias torna inviável o mero transplante de modelos advindos do setor privado. Há para o setor público um esforço extra de compreensão dos impactos e deveres originados das normativas da proteção de dados.

Soma-se a isso mais dois obstáculos: as limitações de recursos financeiros e humanos dos órgãos. As Defensorias contam com orçamento limitado, o que se torna uma questão ainda mais aguda diante a crise econômica e inflacionária desencadeada pela pandemia. Essa limitação relaciona-se também com um obstáculo em termos de recursos humanos, pois leva muitas Defensorias a não possuírem quadros próprios e a contarem com terceirizados, comissionados e servidores cedidos de outros órgãos. Essa limitação, no entanto, tem sido superada por projetos audaciosos de colaboração e de capacitação dentro das Defensorias Públicas, em uma espécie de transformação silenciosa no interior do sistema de

13 BIONI, Bruno; ZANATTA, Rafael; KITAYAMA, Marina. Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021, p. 41-42.

14 Com exceção, cabe citar os empenhos advindos do Conselho Nacional de Justiça a respeito do tema (como a edição da recomendação no 73) e, também, dos trabalhos de Miriam Wimmer, que reconhecem que "no setor público, o tratamento de dados pessoais não se inicia, em geral, a partir de uma decisão voluntária do titular, mas como decorrência das exigências do próprio pacto social. Ver: WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades. Revista dos Advogados da AASP, n. 144, nov., 2019, p. 127.

justiça brasileiro.

Servidores e Defensores iniciaram cursos de capacitação, criaram Comitês de LGPD e pararam para rever seus processos internos, incluindo a dependência com softwares proprietários no atendimento à população.

Ademais, observa-se, no que toca a adequação dos órgãos, a preocupação de tornar este um processo propulsor de uma atuação estratégica, tanto sobre as atividades de gestão, quanto sobre suas atividades-fim.

Ambos os pontos são perceptíveis diante das ações das Defensorias, como a promoção de eventos sobre o tema, a atuação judicial e extrajudicial no questionamento do uso abusivo de dados pessoais[15] e a nomeação de encarregados pela proteção de dados pessoais (formalização já empreendida por cinco Defensorias Estaduais, vide a das unidades federativas de MG, PR, RJ, RO, SP).

Sobre essas importantes mobilizações, o infográfico abaixo destaca as principais, identificadas no projeto "Defensorias e Proteção de Dados" conduzido pela Associação Data Privacy Brasil de Pesquisa:

A proteção de dados pessoais como pilar de confiança e inovação

Apesar do processo de adequação à LGPD ser uma questão de conformação legal, encará-lo apenas desse ponto de vista não é uma alternativa única. Justamente pela potencialidade de transformá-lo em uma oportunidade de aprimoramento de suas atividades é que as Defensorias Públicas têm se destacado nesse processo.

A adequação evoca um amplo conjunto de medidas de cunho organizacional, o que pode promover também a inovação institucional e a revisão positiva de procedimentos e métodos. Sua execução exige que os agentes empenhem atenção sobre o fluxo informacional de sistemas e os obriga a revisitar as razões pelas quais realizam determinada coleta, processamento e compartilhamento de dados. Assim, tais programas estimulam que os órgãos padronizem seus métodos de trabalho,

15 Defensoria Pública de SP pede liminar contra mudança de termos do WhatsApp. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/04/27/defensoria-publica-de-sp-pede-que-governo-suspenda-atualizacao-do-whatsapp.htm>.

adotem medidas de transparência e conheçam os processos de tratamento de dados, colaborando com uma gestão mais eficiente do trabalho.

Essa capacidade organizacional, de modo indireto, reflete-se também na qualidade do serviço prestado, mas mais que isso, pode ser utilizada diretamente nas atividades-fim das Defensorias. Com ela, abre-se margem para que os órgãos se utilizem de modo estratégico das informações geradas a respeito das demandas percebidas e, com isso, encarar o processo de adequação como um gatilho para inovar e otimizar o acesso à justiça[16]. Como sustenta Maria Tereza Sadek, "as possibilidades de se construir uma sociedade mais inclusiva e republicana estão diretamente relacionadas a atuações baseadas em diagnósticos construídos a partir de dados"[17].

A percepção, por exemplo, da existência de diversas demandas semelhantes pode abrir caminhos para a propositura de ações coletivas, assim como pode servir de argumento para pressionar a implementação de políticas públicas ou mesmo servir como suporte probatório perante o judiciário. Um dos casos que ilustra esse potencial foi a ação da DPE-RJ em relação à oferta de vagas em creches na cidade do Rio de Janeiro. A Defensoria atuava nas execuções individuais de ação civil pública movida pelo MP, que tratava de medidas para a universalização da Educação Infantil na pré-escola e a ampliação da oferta de vagas em creches. A partir dos casos, a Defensoria levantou dados acerca da continuidade da não oferta de vagas. O órgão então trouxe sua análise para o debate do orçamento público junto à Câmara de Vereadores, o qual levou ao remanejamento de verbas destinadas à propaganda do município para educação infantil.

A questão dos dados, portanto, tende a impactar os trabalhos da Defensoria em diferentes frentes. Esse fenômeno irá crescer na medida em que a digitalização avança, criando novos desafios em relação à discriminação e marginalização daqueles em situação de vulnerabilidade. Por outro lado, o desenvolvimento tecnológico e a tomada de decisão baseada em dados podem ser aliados das Defensorias, se incorporados a seus processos e se direcionados ao alcance de sua missão institucional.

Em suma, concluímos que o poder público tem um desafio particular no que toca a adequação à LGPD e, no caso das Defensorias, existem ainda outras especificidades que amplificam os percalços dessa jornada. Ainda assim, os entes

16 BIONI, Bruno Ricardo. Inovar pela lei. GV EXECUTIVO, v. 18, n. 4, p. 30-33, 2019.

17 SADEK, Maria Tereza. Prefácio, in: BIONI, Bruno; ZANATTA, Rafael; KITAYAMA, Marina. Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD. São Paulo: Associaçã o Data Privacy Brasil de Pesquisa, 2021.

têm demonstrado um engajamento positivo em relação à proteção de dados, desenvolvendo ações voltadas ao tema, tanto sobre suas atividades-fim como suas atividades-meio. Mais que isso, observa-se um grande potencial para que o processo de adequação origine uma reforma organizacional positiva aos trabalhos das Defensorias, permitindo-lhes uma atuação estratégica, que coaduna-se tanto com direitos e princípios da proteção de dados, como do próprio serviço público.

Em uma sociedade profundamente desigual, como o Brasil, ampliar a capacidade das Defensorias de inovar e usar corretamente dados pessoais é uma forma de atingir os objetivos constitucionais de justiça social e acesso à justiça. A LGPD não é obstáculo para as Defensorias Públicas. É oportunidade de construir planejamentos estratégicos, inovar e incrementar a confiança da população com o sistema de justiça.

LGPD E DEFENSORIA PÚBLICA: UMA ANÁLISE DA NECESSIDADE DO CONSENTIMENTO

LGPD E DEFENSORIA PÚBLICA: UMA ANÁLISE DA NECESSIDADE DO CONSENTIMENTO[1]

RODRIGO BAPTISTA PACHECO[2]

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD) impôs aos gestores da Defensoria Pública desafios que passam pela criação da cultura organizacional de proteção de dados pessoais; adequação de normativas internas; mudança dos fluxos de trabalho; implementação de ferramentas de segurança dos sistemas que as Instituições operam; e a criação de estruturas administrativas que executem às diretrizes da LGPD.

A transformação tecnológica da Defensoria Pública brasileira sofreu aceleração em 2020, quando as Instituições se viram no desafio de garantir acesso à justiça à população durante a pandemia da covid-19, respeitando os protocolos sanitários do distanciamento social[3].

O uso intensivo de tecnologia de sistemas voltados para atividade-fim – valendo-se da interoperabilidade com sistemas de outros órgãos públicos –, a criação de aplicativos ou a utilização de mensagens instantâneas para atendimento remoto da população, exigem uma governança dos dados da população captados para a prestação do serviço público de assistência jurídica.

Rápido olhar sobre a iniciativas estaduais revela que as Defensorias tratam dados de milhões de brasileiros anualmente, armazenando-os em seus sistemas para subsidiar a atuação judicial e extrajudicial[4]. No estado do Rio de Janeiro, em 5 de abril de 2021, a Defensoria Pública possuía dados de 1.795.745 pessoas no

1 Originalmente publicado no Jota. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-defensoria-publica-uma-analise-da-necessidade-do-consentimento-14042021>. Publicado em 14/04/2021.

2 Rodrigo Baptista Pacheco é Defensor Público-Geral do Estado do Rio de Janeiro.

3 Apenas a título ilustrativo, algumas Defensorias Pública estaduais lançaram assistentes virtuais para fazer frente à necessidade de prestar o serviço público com segurança sanitária, como a DEFI de São Paulo; a LUNA de Tocantins; DONA DEDÉ do Ceará.

4 Voltado para a atividade-fim, além do Verde, adotado pela Defensoria Pública do Rio de Janeiro e em implementação na do Distrito Federal, há o Solar, desenvolvido pela Defensoria Pública do Tocantins e utilizado por outras Defensorias estaduais.

seu Sistema Verde, ocupando 6,8 terabytes do *datacenter*.

Ocorre que as particularidades do tema levaram o legislador a reservar um capítulo específico para o Poder Público na LGPD, destacando-se o art. 23 segundo o qual o tratamento de dados pessoais na gestão pública "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (...)".

Justifica-se a disciplina do tratamento de dados pela Administração Pública diversa da regra geral com o fato de, na maior parte das vezes, a relação do cidadão com o Poder Público é compulsória e pautada pelo desequilíbrio de forças[5].

Ademais, a definição de consentimento na LGPD, exigindo a manifestação livre, informada e inequívoca, torna uma tarefa quase utópica alcançá-lo em razão das desigualdades sociais existentes no Brasil e que repercutem na ausência de letramento da população sobre o tratamento de dados. A insuficiência do paradigma do consentimento para garantir um regime protetivo efetivo no tratamento de dados também se dá em razão das limitações cognitivas dos titulares diante da complexidade e da forma como as informações são disponibilizadas, agravada pela utilização de conceitos técnico-jurídico incompreensíveis para a maior parte da população[6].

Também são apontadas como aspectos de fragilização do consentimento a quantidade e a velocidade de informações trafegadas, em níveis que inviabilizam a tomada de decisão plenamente consciente, além dos dados gerados pela própria pessoa – "pegadas digitais" – independentes da sua concordância[7].

Trazendo essas ideias para a Defensoria Pública, a etapa de obtenção do consentimento inequívoco e informado para cada cidadão atendido[8] implicaria uma demora sem sentido no fluxo de demandas urgentes. Diariamente, são veiculadas

5 WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In MENDES, Schertes Mendes; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otavio Luiz (Coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

6 MENDES, Laura Schertel; DA FONSECA, Gabriel Campos. Proteção de dados para além do consentimento: tendências de materialização. Op. cit.

7 RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018. Op. cit.

8 Em 2020, a Central de Relacionamento com o Cidadão da Defensoria Pública do Estado do Rio de Janeiro recebeu 2,5 milhões de telefonemas, 140.000 e-mails, cabendo destacar ainda as mensagens via whatsapp – impossíveis de medir – recebida diariamente por cada equipe da Defensoria.

centenas de petições, requerimentos e medidas urgentes que não podem prescindir da celeridade e, por envolverem o tratamento de dados sensíveis, são lastreadas na relação de confiança do cidadão em relação à Defensoria Pública.

Assim, seria possível afirmar que o consentimento do usuário é dispensável na atividade da Defensoria quando do atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Contudo, especialmente em relação à Defensoria, a questão parece mais complexa e merecedora de reflexão. A chamada terceira onda renovatória da Defensoria Pública, concretizada pela Lei Complementar 132/2009 e pela Emenda Constitucional 80/2014, trouxe como objetivos institucionais a primazia da dignidade da pessoa humana e a redução das desigualdades sociais, incluindo-se aí não apenas as de cunho econômico, mas também as demais vulnerabilidades

Como corolário desse objetivo, o artigo 4º, III, da Lei Complementar 132/2009 inovou ao acrescentar como função da Defensoria Pública a difusão e a conscientização dos direitos humanos, da cidadania e do ordenamento jurídico.

A promoção de educação em direitos pode se concretizar numa dimensão coletiva por meio de projetos institucionais, como cursos voltados para população em plataforma digitais ou a produção de cartilhas, mas também no plano individual por intermédio de cada defensor público em seu local de trabalho ao contribuir para a construção da cidadania e emancipação social.

Se parte da doutrina elenca a privacidade ou a proteção dos dados pessoais como um direito fundamental[9], é possível conectar esse direito ao dever de promoção da educação pela Defensoria.

Havendo concordância de que o consentimento do usuário cria barreiras para a rotina de atuação da Defensoria, por outro é possível concluir que defensores e suas equipes têm o dever, diante da vulnerabilidade da população atendida, de informar e promover a cultura de proteção de dados pessoais.

Informar e promover a cultura da proteção de dados pessoais é diferente da obtenção de consentimento livre e inequívoco, daí porque se discorda do entendimento, externado por Franklyn Roger Alves Silva, de que o consentimento deverá ser obtido de todos os usuários da Defensoria Pública[10].

9 SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: Tratado de proteção de dados pessoais. Op. cit.

10 ALVES, SILVA, Franklyn Roger. A LGPD e o tratamento de dados dos assistidos pela Defensoria Pública. <https://www.conjur.com.br/2020-mar-31/tribuna-defensoria-lgpd-tratamento-dados-assistidos-defensoria>. Acesso em 29/03/2021.

Isso deve se dar no atendimento a cada pessoa, podendo se valer de estratégias como, por exemplo, a inserção de texto nas "declarações de hipossuficiência econômica" para dar ciência plena ao cidadão de que seus dados pessoais serão objetos de tratamento.

No cenário pandêmico, quando o atendimento remoto se disseminou via aplicativo de *Whatsapp*, inclusive com tráfego de documentos, é fundamental que defensores e servidores façam a advertência de que os dados pessoais serão tratados.

No plano da gestão da Defensoria Pública, todas as plataformas de atendimento remoto (telefone, e-mail ou aplicativo) deverão conter mensagens claras e de fácil apreensão por parte do usuário, informando-lhe que, para prestação do serviço público, a Instituição precisará manejar seus dados pessoais, garantindo-lhe segurança e proteção contra vazamentos.

Evidente que outras hipóteses surgirão no curso das atividades da Defensoria, ainda em processo de adaptação, como toda a sociedade brasileira, à cultura da proteção dos dados pessoais. Contudo, dispensando o consentimento, incumbe-lhe, pelo dever de promover e difundir os direitos fundamentais e os direitos humanos, dar plena e clara ciência a cada cidadão atendido de que os seus dados pessoais serão tratados durante a prestação do serviço público, assegurando-lhe a adoção de ferramentas de segurança que impeçam o compartilhamento indevido.

A PRERROGATIVA DE REQUISIÇÃO DAS **DEFENSORIAS PÚBLICAS** E A JUSTIÇA DE DADOS

A PRERROGATIVA DE REQUISIÇÃO DAS DEFENSORIAS PÚBLICAS E A JUSTIÇA DE DADOS[1]

BEATRIZ CUNHA[2]
BRUNO R. BIONI[3]
HANA MESQUITA AMARAL FIGUEIRA[4]
JOHANNA MONAGREDA[5]
MARINA LOWENKRON[6]
RAFAEL A. F. ZANATTA[7]

Recentemente, a Procuradoria-Geral da República (PGR) ajuizou 22 Ações Diretas de Inconstitucionalidade contra dispositivos das leis orgânicas estaduais e da Lei Orgânica Nacional da Defensoria Pública (LC nº 80/94), que previam a prerrogativa da requisição.

1 Originalmente publicado no Jota. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/prerrogativa-requisicao-defensorias-publicas-justica-de-dados-04122021>. Publicado em 04/12/2021.

2 Defensora Pública, encarregada de Proteção de Dados na Defensoria Pública do Estado do Rio de Janeiro.

3 Diretor da Associação Data Privacy Brasil de Pesquisa. Doutorando em Direito Comercial e Mestre em Direito Civil na Faculdade de Direito da Universidade de São Paulo. Foi study visitor do Departamento de Proteção de Dados Pessoais do European Data Protection Board/EDPB e do Conselho da Europa, pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa.

4 Graduada em Direito pela PUC-Rio. Advogada com atuação em proteção de dados e privacidade. Pesquisadora do Data Privacy Brasil. Pesquisadora do grupo Legalite da PUC-Rio.

5 Doutora e Mestre em Ciência Política pela Universidade Federal de Minas Gerais (UFMG). Licenciada em Ciência Política e Administrativa pela Universidad Central de Venezuela (UCV). Pesquisadora do Núcleo de Estudos e Pesquisas sobre a Mulher NEPEM/UFMG. Coordenadora de projetos na ONG Data Privacy Brasil.

6 Defensora Pública, encarregada de Proteção de Dados na Defensoria Pública do Estado do Rio de Janeiro.

7 Diretor da Associação Data Privacy Brasil de Pesquisa. É mestre pela Faculdade de Direito da USP e doutorando pelo Instituto de Energia e Ambiente da USP. Mestre em direito e economia pela Universidade de Turim. Alumni do Privacy Law and Policy Course da Universidade de Amsterdam. Research Fellow da The New School (EUA). Membro da Rede Latino-Americana de Vigilância, Tecnologia e Sociedade (Lavits). Membro do Instituto Brasileiro de Responsabilidade Civil (Iberc).

O início do julgamento da ADI nº 6852, que questionava a LC nº 80/94, foi marcado por forte movimentação da comunidade jurídica, da mídia e das redes sociais, seja em perfis jurídicos ou não, de celebridades ou de pessoas comuns, em apoio à causa que levou à #DefensoriaSim aos tópicos mais comentados do Twitter.

O impacto da campanha nas redes e o seu apoio por atores de diversos setores demonstrou que a importância do julgamento não decorre de mero corporativismo, mas coloca em xeque instrumento essencial para a democracia no país. Afinal, a prerrogativa de requisição tem papel essencial na promoção do acesso à ordem jurídica justa, tentando equilibrar as balanças da Justiça em um país que lamentavelmente figura no ranking das nações mais desiguais do mundo. Pelo indicador Gini, usado pelo Banco Mundial para medir desigualdade e distribuição de renda, o Brasil em 2019 era o 8º pior país no mundo em desigualdade, atrás apenas de alguns países da África.

Considerando que injustiça social e violações de direitos andam de mãos dadas, o constituinte de 1988 se preocupou em prever uma instituição com autonomia e instrumentos e lhe determinar a missão de promoção dos direitos humanos e defesa dos direitos individuais e coletivos dos vulneráveis: a Defensoria Pública. Para se desincumbir da missão constitucional, ferramentas de trabalho são necessárias.

A requisição, ora questionada, é apenas isso: uma ferramenta de trabalho para o equilíbrio de forças, que permite aos Defensores auxiliarem o vulnerável na obtenção de dados necessários para avaliar se sofre ameaça ou lesão a direito e tomar as medidas necessárias para a cessação ou reparação do risco ou dano diagnosticado.

Mas, ao mesmo tempo em que é "apenas" um instrumento de trabalho das Defensoras e Defensores Públicos, a requisição é uma conquista histórica do acesso material à justiça, na compreensão desse direito como efetivo acesso à ordem jurídica justa. Atualmente, segundo dados da Pesquisa Nacional da Defensoria Pública de 2021, estima-se que o país possua ao menos 186.299.853 habitantes considerados como público potencial da Defensoria Pública por força de vulnerabilidade econômica, isto é, 88% da população total do país. Ainda, a mesma pesquisa estima que, desses usuários em potencial, 51.733.631 habitantes não possuem acesso aos serviços jurídico-assistenciais oferecidos pela Defensoria Pública, em violação ao art. 134 da Constituição Federal e à diretriz do art. 98 do ADCT. Em outras palavras, se a Defensoria, no atual estado da arte, sequer tem pernas para cumprir a missão constitucionalmente imposta, a quem interessa lhe

cortar os braços?

De nada adianta prever uma instituição formalmente constituída para tutela dos direitos humanos dos indivíduos e grupos vulneráveis e privá-la de meios para desempenhar o seu papel.

Como se sabe, os Defensores Públicos são responsáveis por concretizar direitos em uma sociedade extremamente desigual[8] e atuam nas tutelas coletiva e individual na defesa de direitos e garantias fundamentais, o que naturalmente inclui aqueles relacionados à proteção de dados[9].

Reconhecimento facial e fotográfico[10], discriminação algorítmica[11] e a garantia do exercício dos direitos dos titulares de dados – temas nos quais as Defensorias Públicas brasileiras vêm notadamente atuando – são exemplos claros dessa interface entre proteção de dados e justiça social.

Longe de ser um "superpoder" que exorbita as atribuições da Defensoria Pública, a prerrogativa de requisição é uma ferramenta imprescindível para a contenção e redução de injustiças informacionais no Brasil. Afinal, conforme destacam Luciana Gross Cunha e Maria Tereza Sadek: "(...) **a prerrogativa de requisição de informações e de documentos aos órgãos públicos é, sem dúvida nenhuma, um instrumento fundamental para que a Defensoria Pública possa exercer suas atividades em conformidade com a afirmação do Estado Democrático de Direito e com reverência à primazia da dignidade da pessoa humana**".

É mais uma camada, ao lado dos direitos do titular cristalizados nos arts. 17 a 22 da LGPD, que é capaz de reduzir a assimetria de informação de como os cidadãos são catalogados, fichados, enfim, julgados e avaliados por um banco de dados. Considerando que muitas vezes o titular se depara com verdadeiros **"labirintos"** para exercer seus direitos, isto é, arquiteturas que reforçam a sua hipossuficiência. Tal poder atribuído às Defensorias é vital para a efetiva materialização de direitos básicos como de acesso, retificação, deleção e oposição.

8 BIONI, Bruno; ZANATTA, Rafael; KITAYAMA, Marina. Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. p. 6.

9 BIONI, Bruno; MESQUITA, Hana; ZANATTA, Rafael. Relatório de Discussões da Oficina Prática de Adequação à LGPD – Defensorias Públicas e Proteção de Dados. Revisão Maraísa Rosa Cezarino. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021.p. 25.

10 Relatório da Defensoria Pública do Estado do Rio de Janeiro sobre reconhecimento fotográfico em sede policial. Disponível em: <**https://www.defensoria.rj.def.br/uploads/arquivos/54f8edabb6d0456698a-068a65053420c.pdf**>. Acessado em 23 de novembro de 2021.

11 Para saber mais sobre a atuação das Defensorias Públicas em matéria de discriminação algorítmica, confira o Webinar Proteção de Dados Pessoais e o papel das Defensorias Públicas realizado em parceria pela Defensorias do Estado de São Paulo, do Rio de Janeiro e Associação Data Privacy Brasil de Pesquisa.

Os casos concretos abaixo evidenciam isso.

As pessoas socioeconomicamente fragilizadas que recorrem à instituição sequer têm condição de diligenciar para conseguir os documentos necessários para ajuizar suas demandas. É nesse cenário que se insere a prerrogativa de requisição, que se tornou ainda mais decisiva em razão da crise sanitária da Covid-19. Durante a pandemia, diversas famílias brasileiras foram beneficiadas pela prerrogativa para reclamar contra o indeferimento do auxílio emergencial.

Foi a prerrogativa de requisição, ainda, que permitiu a obtenção de prontuários médicos indispensáveis para instruir ações pleiteando vagas em unidade hospitalar, exames e medicamentos. É que, sem a possibilidade de requisitar tais informações, a Defensoria Pública vê-se impossibilitada de comprovar a situação de saúde do/a usuário/a, e, ainda, a circunstância de urgência ou emergência. Trata-se, pois, de condição imprescindível para a obtenção de qualquer medida liminar e, caso não atendida, pode implicar morte ou dano irreversível à integridade do paciente.

De outro lado, a requisição também foi e é ferramenta indispensável para a defesa criminal. Afinal, ela permite que Defensores Públicos tenham acesso a certidões de nascimento para comprovar que a pessoa privada de liberdade é indispensável aos cuidados de criança ou pessoa com deficiência. Sem essa prerrogativa, perder-se-ia um instrumento fundamental para a substituição da prisão por prisão domiciliar, afastando-se dos objetivos do Conselho Nacional de Justiça (CNJ) ao editar a Recomendação nº 62/2020 e a Resolução nº 369/2021.

Em outro caso, a prerrogativa instrumentalizou pedido de retirada da foto de um homem negro de um álbum de suspeitos em uma determinada delegacia de polícia. Para além da autodeterminação informativa, o simples fato de a foto permanecer naquele álbum fazia com que diversas vítimas fossem levadas a reconhecer aquele indivíduo como o autor do crime contra elas praticado, incentivando falsas memórias em evidente prejuízo à presunção de inocência.

Ademais, Defensoras e Defensores Públicos puderam continuar monitorando as condições carcerárias e socioeducativas à distância. Em tendo sido decretada a emergência sanitária e em tendo sido fechadas as portas de tais unidades para o público externo, a requisição foi o que permitiu que a Defensoria Pública obtivesse informações sobre internos pertencentes aos grupos de risco ou com suspeita de Covid-19. Semanalmente, os gestores eram instados a enviar à instituição tais dados, a fim de que fossem feitos os respectivos requerimentos de liberdade e/ou atendimento de saúde.

Com efeito, a partir da análise desses casos, pode-se extrair algumas conclusões. A primeira delas é que a prerrogativa de requisição é instrumento para dar efetividade a uma série de direitos fundamentais, dentre os quais também se insere o direito à proteção de dados pessoais. Desse modo, ela permite que se obtenham informações sobre a confirmação do tratamento; o acesso aos dados pessoais eventualmente tratados; a retificação desses mesmos dados; e, até mesmo, a eliminação quando ausente uma base legal que os justifique ou quando caracterizado o excesso.

Os casos acima evidenciam que nem sempre a instituição poderá se valer pura e simplesmente dos arts. 18 a 22 da Lei Geral de Proteção de Dados (LGPD). Afinal, há situações em que não há tempo hábil para se aguardar o prazo da LGPD ou da Lei de Acesso à Informação (LAI) para se obter a providência necessária para salvaguardar o direito do(a) usuário(a). Foi esse o **caso em que, após negativa de atendimento à requisição, propôs-se ação judicial para obter relatório médico e o paciente morreu antes que pudesse pleitear a sua vaga em unidade de terapia intensiva**. Do mesmo modo, é irrazoável, por exemplo, que se aguarde por 15, 20 ou 30 dias quando a resposta puder ter o condão de colocar uma pessoa em liberdade, assegurá-la o recebimento de um auxílio que se pretende "emergencial" ou livrá-la de uma grave violação de direitos humanos.

Daí nasce a segunda conclusão: quando em pauta a defesa do direito à proteção de dados pessoais, a prerrogativa de requisição é ainda mais essencial nos casos em que houver urgência ou emergência, caracterizada pelo risco de perecimento do direito e/ou dano irreparável ou de difícil reparação. Por meio dela, permite-se que a assistência jurídica seja efetiva e que o direito em xeque seja levado a sério, saindo verdadeiramente do papel com a celeridade necessária para permitir a sua fruição.

Logo, é evidente que a restrição da prerrogativa de requisição impacta a tutela coletiva e individual na defesa dos direitos fundamentais, incluindo também a proteção de dados pessoais. A vulnerabilidade socioeconômica do usuário das Defensorias Públicas acentua seu grau de exposição aos efeitos negativos do processo de datificação da sociedade de modo que a prerrogativa de requisição das Defensorias é imprescindível para dar efetividade aos direitos consagrados em nosso ordenamento jurídico. Assim, para que um tratamento de dados pessoais efetivamente justo e democrático ocorra, é indispensável que as Defensorias Públicas estejam adequadamente munidas das ferramentas necessárias para combater as assimetrias da complexa realidade brasileira.

A GOVERNANÇA DE DADOS COMO POLÍTICA PÚBLICA: PERSPECTIVAS DA COOPERAÇÃO ENTRE DEFENSORIAS PÚBLICAS

A GOVERNANÇA DE DADOS COMO POLÍTICA PÚBLICA: PERSPECTIVAS DA COOPERAÇÃO ENTRE DEFENSORIAS PÚBLICAS[1]

BRUNO R. BIONI
RAFAEL A. F. ZANATTA
MARINA KITAYAMA

RESUMO

A implementação de programas de governança de dados pelo sistema de justiça é importante política pública de garantia de direitos fundamentais e de aprimoramento organizacional das instituições. O processo implica a adoção de uma série de medidas de adequação à Lei Geral de Proteção de Dados (Lei. 13.709/2018), de modo que sua execução é de extrema complexidade, principalmente em um cenário em que pouco material foi produzido acerca das particularidades da proteção de dados em relação ao setor público. No caso das Defensorias, por uma série de razões, esse desafio é ainda maior. Mesmo diante disso, o ente tem se apresentado como agente de transformação no que toca a implementação de programas de governança de dados. Atuando em conjunto com organizações da sociedade civil, a Defensoria Pública demonstra possibilidades que a cooperação pode ter para alavancar esse tipo de política e com ela ir de encontro a seus objetivos institucionais.

PALAVRAS-CHAVE

Defensoria Pública, Governança de Dados, Política pública

1 Originalmente publicado no Cadernos da Defensoria Pública do Estado de São Paulo v.6. n.31 dez/2021

ABSTRACT

The implementation of data governance programs by the legal system is an important public policy to guarantee fundamental rights and to improve institutional organization. The process implies the adoption of a series of measures to adapt the agent to the General Data Protection Law (Law 13.709/2018), so that its execution is of extreme complexity, especially in a scenario in which little material has been produced about the particularities of data protection in relation to the public sector. In the case of the Public Defenders' Offices, for a number of reasons, this challenge is even greater. Even so, the entity has presented itself as an agent of transformation when it comes to the implementation of data governance programs. Acting in conjunction with civil society associations, the Defender's Offices have been demonstrating the possibilities that cooperation can have to leverage this type of polity and to meet the entity's institutional objectives.

KEYWORDS

Public Defenders' Office, *Data Governance*, *Public policy*

Introdução

Desde os trabalhos pioneiros de Maria Tereza Sadek, Rogério Arantes e pesquisadores do Centro Brasileiro de Estudos e Pesquisas Judiciais, o Judiciário tornou-se objeto de análise para políticas públicas, atraindo atenção das ciências sociais para além do direito[2]. Com a criação do Conselho Nacional de Justiça, tornou-se evidente a existência de políticas judiciárias e políticas públicas formuladas especificamente para o sistema de justiça. Nesse campo de estudo das instituições do sistema de justiça, encontra-se uma rica literatura interdisciplinar, por vezes chamada de "sociologia política do direito"[3].

Partindo dessa tradição de estudos, o presente artigo discute como, diante da complexidade da implementação de políticas públicas no sistema de justiça, torna-se desafiadora e positiva a cooperação entre entes do setor público e da sociedade civil. Em específico, essa análise se pauta sobre a mobilização conjunta das Defensorias Públicas e movimentos da sociedade civil para o desenvolvimento de seu projeto de adequação à Lei Geral de Proteção de Dados Pessoais.

Em linhas gerais, entende-se como "projeto de adequação" o processo de cumprimento com a Lei 13.709/2018, que exige uma intensa atividade organizacional para compreensão (i) dos fluxos de dados pessoais dentro da organização, (ii) das finalidades legítimas para o uso de dados, (iii) dos fundamentos legais que habilitam o tratamento de dados (chamado de "base legal" nos termos da Lei 13.709/2018) e, ao mesmo tempo, *modificação das práticas administrativas e organizacionais*, em especial com relação à (i) criação de canais de atendimento para cumprimento dos direitos dos titulares com relação aos dados, (ii) nomeação de um encarregado pela proteção de dados pessoais, como exigido pela legislação.

Muitas das análises empíricas aqui apresentadas são originadas do projeto desenvolvido pela Associação Data Privacy Brasil de Pesquisa[4], que conta com a

2 SADEK, Maria Tereza. Judiciário: mudanças e reformas. Estudos avançados, v. 18, n. 51, p. 79-101, 2004. SADEK, Maria Tereza. Acesso à justiça: visão da sociedade. Revista Justitia, São Paulo, v. 65, n. 198, p. 271-279, 2008.

3 GERALDO, Pedro Barros; FONTAINHA, Fernando; VERONESE, Alexandre. Sociologia empírica do direito: Uma introdução. Revista Ética e Filosofia Política, v. 2, n. 12, 2010. LOPES, José Reinaldo de Lima; FILHO, Roberto Freitas. Law and Society in Brazil at the crossroads: a review. Annual Review of Law and Social Science, v. 10, p. 91-103, 2014. FONTAINHA, Fernando; DE OLIVEIRA, Fabiana Luci; VERONESE, Alexandre. Por uma sociologia política do direito no Brasil. Revista Brasileira de Sociologia, v. 5, n. 11, p. 29-47, 2017.

4 Ver: https://www.dataprivacybr.org/projeto/expandindo-o-papel-dos-defensores-publicos-na-protecao-de-dados-pessoais-no-brasil/.

parceria das Defensorias Públicas Estaduais do Rio de Janeiro[5] e de São Paulo[6] e do Colégio Nacional de Defensores Públicos Gerais[7]. Com as informações coletadas, pretendemos demonstrar como esse tipo de engajamento tem o potencial de ampliar o caráter transformador de uma política pública, tal qual a implementação de programas de governança de dados.

Para tanto, o texto foi dividido em cinco partes. Em um primeiro momento, o artigo explora como a ideia de implementação de políticas públicas "dadocêntricas" tem sido alavancada pelo sistema de justiça como um todo. Na segunda parte, demonstramos por que os programas de governança de dados enquadram-se no conceito de política pública e por que sua execução apresenta um alto grau de complexidade. Na terceira parte, argumentamos como a complexidade dos programas de governança de dados pode ser enfrentada por meio da cooperação entre entes públicos e sociedade civil, tomando como base a matriz teórica da Nova Governança. Em seguida, descrevemos a mobilização das Defensorias Públicas junto a organizações sociais ligadas ao tema da proteção de dados, apresentando os desafios particulares do ente e as razões que corroboram a necessidade de cooperação. Por fim, concluímos que a atuação conjunta entre Defensorias e uma entidade civil tem se mostrado virtuosa da perspectiva de superação de limitações cognitivas para execução de políticas públicas complexas e experimentais[8] e apontamos de que forma a cooperação incide positivamente sobre os objetivos institucionais da Defensoria Pública.

5 Ver: http://www.defensoria.rj.def.br/uploads/arquivos/Doe/2020.09.28.pdf.

6 Ver: https://www.imprensaoficial.com.br/DO/BuscaDO2001Documento_11_4.aspx?link=%2f2020%2fexecutivo%2520secao%2520i%2fsetembro%2f05%2fpag_0061_3b88308dff6d7040a058c93f0f9d31bf.pdf&pagina=61&data=05/09/2020&caderno=Executivo%20I&paginaordenacao=100061.

7 DEFENSORIA PÚBLICA DO DISTRITO FEDERAL. Defensoria Pública-Geral. Acordo De Cooperação Nº 2/2021. Processo: 00401-00003839/2021-29 Doc. SEI/GDF 57821789. Brasília, março 2021.

8 Ver, em especial, o capítulo 12 ("Traditional policy styles and contemporary design trends") do livro Designing Public Policies do Prof. Michael P. Howlett, diretor de pesquisa no Departamento de Ciência Política da Universidade Simon Fraser no Canadá. "It has been argued in many circles that in response to the increased complexity of society and the international environment, governments in many countries in Western Europe, in particular, have turned away from the use of a relatively limited number of traditional, more or less command-and-control oriented, 'substantive' policy tools such as public enterprises, regulatory agencies, subsidies and exhortation and begun to increasingly use their organizational resources to support a different set of 'procedural' tools such as government reorganizations, reviews and inquiries, governmentNGO partnerships and stakeholder consultation. These all act to guide or steer policy processes in the direction the government wishes through the manipulation of policy actors and their interrelationships and constitute a 'new governance' system". HOWLETT, Michael. Designing public policies: Principles and Instruments. London: Routledge, 2019.

Políticas Públicas no sistema de Justiça Brasileiro

No ano de 2014, o Ministério da Justiça apresentou durante a audiência pública organizada pelo CNJ um relatório produzido pelo próprio Ministério que indicava os três principais problemas que afligem o sistema de justiça brasileiro: o excesso de processos, a morosidade e a falta de acesso à justiça[9]. Em 2015, o Brasil atingiu a marca de 100 milhões de processos em tramitação cerca de um processo ativo para cada dois habitantes, quadro que melhorou em comparação aos dados mais recentes[10]. No último relatório Justiça em Números, o sistema de justiça brasileiro parece ter obtido ganhos em termos de eficiência, apesar da litigiosidade continuar crescendo (identificado o aumento da entrada de processos entre os anos de 2018 e 2019), a quantidade de casos solucionados foi 17% maior do que a de entrada de novos processos e o ano de 2019 fechou com cerca de 23 milhões de casos a menos se em comparação a 2015[11]. Aponta-se como uma das causas do desafogamento a modernização do sistema, que hoje conta com boa parte dos processos digitalizados[12].

Fora as perspectivas de um Judiciário menos moroso e com menor carga acumulada, projetos de inovação tecnológica no sistema de justiça também geram expectativas positivas quanto à ampliação do acesso à justiça. O CNJ tem promovido a agenda de incluir o sistema legal do país na era digital, com o objetivo de promover a inovação para desenvolver estratégias, estudos, metodologias e ações para ampliação da prestação jurisdicional e facilitação do acesso à justiça no Brasil[13]. A agenda tem como foco o desenvolvimento de políticas judiciárias relacionadas a eixos de trabalho prioritários para o sistema no contexto atual e o

9 Migalhas. MJ aponta principais problemas do Judiciário brasileiro. Disponível em: <https://www.migalhas.com.br/quentes/195678/mj-aponta-principais-problemas-do-judiciario-brasileiro>.

10 Consultor Jurídico. Brasil atinge a marca de 100 milhões de processos em tramitação na Justiça. Disponível em: <https://www.conjur.com.br/2015-set-15/brasil-atinge-marca-100-milhoes-processos-tramitacao>.

11 Conselho Nacional de Justiça. Justiça em Números 2020. Disponível em: <https://www.cnj.jus.br/wpcontent/uploads/2020/08/WEB_V2_SUMARIO_EXECUTIVO_CNJ_JN2020.pdf>.

12 Conselho Nacional de Justiça. PB: Judiciário conclui digitalização de mais de 44 mi de páginas de processos. Disponível em: <https://www.cnj.jus.br/pb-judiciario-conclui-digitalizacao-de-mais-de-44-milhoes-de-paginas-de-processos/>.

13 Conselho Nacional de Justiça. Projetos de inovação promoverão efetividade e ampliação do acesso à justiça no Brasil. Disponível em: <https://www.cnj.jus.br/inovacao-promoverao-efetividade-e-ampliacao-do-acesso-a-justica-no-brasil/>.

fortalecimento da gestão da informação para formulação de políticas judiciárias baseadas em evidências e gestão por resultados.

Apesar da pauta ganhar maior notoriedade no momento presente, a ideia de desenvolvimento de políticas judiciárias como um dos aspectos centrais da reforma do sistema de justiça já é debatida há mais de uma década[14]. Quando assumiu o cargo de presidente do CNJ, o Ministro do Supremo Tribunal Federal, Gilmar Mendes, trouxe em seu discurso de posse a necessidade de elaboração de políticas públicas abrangentes que resultem na modernização do sistema legal brasileiro[15], colocando essa modernização como meio para, por exemplo, a eliminação das disparidades notadas entre juízos e tribunais dos estados federativos[16]. No mesmo discurso, o Ministro ressaltou o processo de informatização total dos órgãos jurisdicionais como uma das políticas mais importantes nesse sentido, o qual aponta ser um facilitador em termos financeiros e operacionais para garantir eficiência, publicidade, entre outros princípios caros à sociedade democrática.

No nível mais geral das políticas judiciárias, nota-se a crescente centralidade das políticas de informatização e uma visão mais estratégica orientada à gestão da informação. Nesse sentido, a formulação de programas de governança de dados enquadra-se em uma reflexão estratégica sobre o papel da informação, incluindo dados pessoais, nas práticas administrativas e na potencialização de atividades dentro de uma organização inserida no sistema de justiça.

14 Já se argumentou que, a partir das especificidades da Justiça brasileira, o CNJ assume um papel central de concepção e elaboração de políticas para incrementar a atuação jurisdicional e torná-la mais célere, efetiva e responsiva às necessidades sociais. DA SILVA, Jeovan Assis; DE ABREU, Pedro; FLORÊNCIO, Lima. Políticas judiciárias no Brasil: o Judiciário como autor de políticas públicas. Revista do Serviço Público, v. 62, n. 2, p. 119-136, 2011.

15 Conselho Nacional de Justiça. Gilmar Mendes assume presidência do CNJ. Disponível em: <https://www.cnj.jus.br/gilmar-mendes-assume-presidia-do-cnj/>.

16 João Murta argumenta que, enquanto Ellen Gracie Northfleet deu forte ênfase à informatização e padronização das informações em sua gestão no Conselho Nacional de Justiça, Gilmar Mendes privilegiou a formulação de políticas de gestão e estabeleceu metas de produtividade, incluindo o uso instrumental da informatização. MURTA, João. Descontinuidade na administração judiciária. Belo Horizonte: Editora Dialética, 2021.

Programas de governança de dados no sistema de justiça: uma política pública de alta complexidade

Partindo do contexto atual, em que as políticas públicas têm se evidenciado dentro da agenda de reforma e aprimoramento do sistema de justiça, merece destaque uma política de matriz informacional de extrema relevância: a implementação de programas de governança de dados. O programa em questão refere-se à adoção pelos agentes que realizam o tratamento de dados pessoais de medidas que estabeleçam condições de organização, regime de funcionamento, procedimentos, incluindo reclamações e petições de titulares, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento, ações educativas, mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados[17].

Portanto, quando pensamos na implementação de políticas de governança de dados, estamos nos referindo a todo um conjunto de medidas, o que implica que sua execução ocasione um amplo processo de inovação institucional e de revisão de procedimentos e métodos. Isso porque, menos do que propriamente um programa de inclusão de ferramentas digitais, a governança de dados provoca um movimento organizacional. Sua construção exige que os agentes despendam atenção sobre todo o fluxo informacional de seus sistemas e os obriga a revisitar as razões pelas quais realizam determinada coleta, tratamento e compartilhamento de dados, incentivando que se eliminem os processos excessivos e disfuncionais.

A esse respeito, as poucas pesquisas empíricas produzidas sobre o tema indicam que os três maiores gargalos da incorporação da proteção de dados pessoais em organizações, tanto em termos estruturais como comportamentais, são: i) o isolamento entre equipes e a falta de comunicação, uma vez que persiste a ideia equivocada de que o programa de governança de dados é tarefa única e exclusiva dos departamentos jurídicos e de segurança da informação; ii) o baixo investimento em capacitação, que mesmo após investimentos iniciais pode se manter uma questão quando não há periodicidade no processo, nesse caso, deve-se ter em mente a rotatividade das pessoas que cumularam expertise para a manutenção e ampliação do programas; iii) ausência de uma cultura voltada à proteção de dados na organização, isto é, sua internalização como parte da missão e prioridade nas

17 CONGRESSO NACIONAL. Lei Geral de Proteção de Dados. Lei nº 13.709/2018, art. 50. Brasília, 2018.

atividades cotidianas[18]. Em resumo, os três gargalos convergem para um desafio central: a criação de um processo de aprendizagem organizacional capaz de promover a reestruturação da arquitetura informacional e da forma como todos os envolvidos da instituição lidam com os dados pessoais.

Sob a ótica de uma política informacional e organizacional, a governança de dados apresenta tanto efeitos internos quanto externos. Primeiramente, ela permite que o agente possa rever e avaliar se a maneira como tem operado até então é a mais eficiente, abrindo portas para a estipulação de novas estratégias de uso de dados. Em segundo lugar, a política fornece uma visão mais clara ao controlador sobre as informações que constam em seu próprio banco, o que pode trazer indicativos úteis para questões de planejamento, a partir, por exemplo, da identificação de demandas e estatísticas de produtividade, que poderiam pautar metas anuais, distribuições de tarefas e alocação de servidores de um modo fundamentado em informações concretas e não apenas em impressões pessoais. Em poucas palavras, é uma jornada que deve ser encarada enquanto uma janela de oportunidade e não como um custo decorrente da aderência à legislação sobre o tema[19].

Duas mentalidades de processo de conformidade à LGPD[20]	
Obrigação legal	**Oportunidade**
Manutenção e revisão dos processos existentes	Melhoramento dos processos existentes, automatização e criação de novos usos para fins de política pública
Análise estanque centrada no diagnóstico de riscos	Análise dinâmica centrada em que a instituição pode se aprimorar
Gestão baseada em mitigação de risco	Gestão baseada na inovação
Reputação com base no medo de sanções	Reputação com base em dar mais transparência ao uso dos dados
Desincentivo à inovação no uso dos dados, riscos reputacionais, ampliação da burocracia	Formas inovadoras de utilização dos dados, educação em direitos através de exemplos sobre o devido tratamento de dados, automatização de processos e redução da burocracia.

18 WALDMAN, Ari Ezra. Designing without privacy. Hous. L. Rev., v. 55, p. 659, 2017.

19 BIONI, Bruno Ricardo. Inovar pela lei. GV EXECUTIVO, v. 18, n. 4, p. 30-33, 2019.

20 Tabela adaptada de: BIONI, Bruno Ricardo. Inovar pela lei. GV EXECUTIVO, v. 18, n. 4, p. 30-33, 2019.

Assim como outras políticas públicas, a implementação de programas de governança de dados no sistema de justiça promove ganhos diretos e indiretos em relação à missão institucional desse sistema. Tomando as Defensorias Públicas como exemplo, esses programas estimulam que os entes padronizem seus métodos trabalho, adotem medidas de transparência e conheçam os processos de tratamento de dados, colaborando com uma gestão mais eficiente do trabalho, o que de modo indireto reflete-se na qualidade do serviço público prestado. De modo direto, dois aspectos podem ser ressaltados, o primeiro deles é que a adoção do programa promove uma maior conformidade às previsões da LGPD e, portanto, também ao direito fundamental à proteção de dados[21]. O segundo aspecto é que o nível de organização informacional que se desenvolve a partir da implementação de um programa de governança, abre margem para que as Defensorias se utilizem de modo estratégico das informações geradas. A percepção, por exemplo, da existência de diversas demandas semelhantes pode abrir caminhos para a propositura de ações coletivas, assim como pode servir de argumento para pressionar a implementação de políticas públicas ou mesmo servir como suporte probatório perante o judiciário.

Evidentemente, a implementação de programas de governança de dados tem uma particularidade em relação a outros tipos de políticas no sistema de justiça, no caso, esse tipo de programa está relacionado à própria adequação das instituições à LGPD. Aprovada em agosto de 2018 e vigente desde setembro de 2020, a Lei Geral de Proteção de Dados Pessoais, como seu próprio nome sugere, tem um escopo de aplicação amplo, regulamentando e incidindo sobre todo tipo de tratamento de dados, seja este no setor público ou privado. O capítulo IV da LGPD dispõe sobre a aplicação da Lei em relação ao poder público, estabelecendo, conforme o art. 23º, que o tratamento para esses agentes "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público". Assim, os entes integrantes do setor público de forma geral, incluindo aqui a própria Defensoria, deverão adequar suas atividades para estar em consonância com as disposições da LGPD. O artigo 23º indica que sua definição de pessoa jurídica de direito público corresponde àquela do art. 1º da

21 SUPREMO TRIBUNAL FEDERAL. Voto da Relatora, MIN. ROSA WEBER. Ações Diretas de Inconstitucionalidade número 6387, 6388, 6389, 6390 e 6393. Julgamento de liminar com pedido de suspensão dos efeitos da Medida Provisória n. 954/2020. DJe. 07.05.2020.

Lei de Acesso à Informação (Lei 12.527/2011)[22], desse modo, entende-se que há o enquadramento das Defensorias como um dos entes referidos no dispositivo, tendo em vista que, apesar de não ser expressamente citada pela LAI, a própria Defensoria compreende sua subordinação às suas previsões.

Apesar de ser componente do processo de adequação à Lei Geral de Proteção de Dados, encarar a governança de dados apenas do ponto de vista legal não é uma alternativa única. Justamente pela potencialidade de transformá-lo em uma verdadeira política pública é que as Defensorias Públicas têm se destacado nesse processo. O que se observou durante este estudo é existência de uma grande preocupação dos órgãos em garantir o respeito aos direitos dos titulares cujos dados são tratados na instituição, com especial atenção aos dados de seus usuários, e de, além disso, tornar sua organização informacional útil para a atuação estratégica, tanto em termos de atividades de gestão, como em termos de suas atividades-fim. Isso é notável em razão da quantidade de eventos sobre LGPD organizados por Defensorias Públicas, o anúncio de estruturação de "encarregados pela proteção de dados pessoais"[23] dentro das Defensorias e a participação ativa de Defensorias em ações civis públicas que questionam uso abusivo de dados pessoais na prestação de serviços públicos[24].

A atuação das Defensorias nesse sentido ainda ganha destaque em razão de sua própria missão e atribuição legal, encarregado pela defesa de direitos daqueles que se encontram em situação de vulnerabilidade[25]. As Defensorias são guardiãs de uma quantidade vultosa de dados pessoais, muitos dos quais sensíveis. A Defensoria Público do Estado do Rio de Janeiro, por exemplo, maneja dados pessoais de mais de um milhão de cidadãos. O perfil do público atendido corres-

22 Há uma confluência entre LAI e LGPD, de modo a se construir uma narrativa que alie transparência e proteção. A LGPD faz referência explícita à LAI para operacionalizar o exercício de direitos nela previstos perante o poder público. WIMMER, Miriam. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: BIONI, Bruno; SCHERTEL, Laura; DONEDA, Danilo; SARLET, Ingo; RODRIGUES, Otavio. Tratado de Proteção de Dados. Rio de Janeiro: Forense, 2021, p. 276.

23 Defensoria Pública do Estado de São Paulo. Ato Normativo DPG nº 183, de 21 de setembro de 2020. Disponível em: <https://www.defensoria.sp.def.br/dpesp/Conteudos/Materia/MateriaMostra.aspx?idItem=91034&idModulo=9788>.

24 Portal G1. Defensoria Pública cobra na Justiça informações do Metrô de SP sobre câmeras de reconhecimento facial. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2020/02/11/defensoriapublica-cobra-na-justica-informacoes-do-metro-de-sp-sobre-cameras-de-reconhecimento-facial.ghtml>.

25 RIBEIRO, Marcia Carla Pereira; DE PAULA MACHADO, José Alberto Oliveira. Acesso à Justiça e a Defensoria Pública na América Latina: democratização de direitos como desenvolvimento. Direito e Desenvolvimento, v. 8, n. 1, p. 89-106, 2017.

ponde também ao perfil daqueles que mais sofrem das lesões causadas pelo uso abusivo de dados pessoais, seja em virtude de processos de tomada de decisões automatizadas discriminatórias, seja em virtude do assédio de empresas que colocam a privacidade de seus consumidores em detrimento do acesso "gratuito" de serviços[26]. A população assistida, tipicamente marcada por desigualdades e exclusão, tende a ser afetada de forma mais severa pela digitalização da sociedade[27]. Como argumentado por Virginia Eubanks, populações socialmente vulneráveis são alvo de mais vigilância e controle, alimentando um "*feedback looping*" de automação e injustiças[28]. Ao implementar seus programas de governança de dados, as Defensorias quebram com a lógica socioeconômica da privacidade enquanto um "bem de luxo"[29]. É um quadro exige uma reflexão renovada para as Defensorias sobre as condições de igualdade e uma ordem jurídica justa[30].

Nova Governança e cooperação da sociedade civil em políticas públicas

A partir dos pontos elencados anteriormente, chegamos a três constatações. A primeira é a de que se formou uma agenda dentro do sistema de justiça de incorporar políticas públicas para fins de melhoria da eficiência. A segunda é a de que a implementação de programas de governança de dados é mais que um meio para cumprir as disposições da LGPD, podendo ser enquadrada dentro do conceito de política pública. A terceira é a de que as Defensorias têm se colocado como entes do sistema de justiça com grande potencial para alavancar esses programas sob o viés das políticas públicas. Partindo deste último ponto, passaremos

26 O'NEIL, Cathy. Algoritmos de Destruição em Massa: Como o Big Data Aumenta a Desigualdade e Ameaça à Democracia. Trad. Rafael Abraham. 1 ed. Santo André, SP: Rua do Sabão, 2020.

27 SILVA, Michelle Valéria Macedo et al. Direitos humanos. Acesso à justiça. Defensoria pública. Pobreza. Exclusão social. Revista da Defensoria Pública da União, n. 06, 2013.

28 EUBANKS, Virginia. Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press, 2018.

29 A expressão é emprestada do artigo: PAPACHARISSI, Zizi. Privacy as a luxury commodity. First Monday, 2010.

30 SADEK, Maria Tereza. A Defensoria Pública no sistema de justiça brasileiro. São Paulo: APADEP em Notícias, p. 2-2, 2008. SADEK, Maria Tereza. Acesso à justiça: um direito e seus obstáculos. Revista USP, n. 101, p. 55-66, 2014.

a explorar de que forma o engajamento das Defensorias Públicas com organizações da sociedade civil se mostra como positivo para que se torne possível o alcance de seu objetivo.

Como descrito no capítulo anterior, a implementação de um programa de governança de dados envolve um conjunto de medidas e apresenta-se como política de alta complexidade, por essa razão, a cooperação conjunta entre entes do setor público que enfrentam este processo e organizações da sociedade civil se mostra como uma alternativa para sua efetivação. Os desafios da implementação de políticas públicas e o papel da sociedade dentro dessa perspectiva é uma questão amplamente discutida pelas teorias da Nova Governança (*new governance*). Um dos novos paradigmas da administração pública, a Nova Governança, evoca modelos mais participativos de gestão, baseados em redes, co-produção, flexibilidade no uso de instrumentos de gestão[31]. O ideal por detrás desse novo paradigma é o da introdução de uma dimensão social na gestão pública, considerando que os valores sociais não podem ser exclusivamente tratados a partir da ótica da eficiência econômica dos mercados. O alcance de tais valores sociais se daria a partir do fortalecimento dos relacionamentos institucionais com a sociedade e com a formação de redes interorganizacionais, operacionalizadas com o envolvimento mais amplo e proativo das partes interessadas da sociedade, o que exige um sistema mais colaborativo[32].

As razões que levam a um novo paradigma da governança pública emergem da caracterização do contexto social organizacional do século XXI, o qual traduz um ambiente multidimensional e dinâmico em que a coprodução se torna intrínseca aos processos e práticas de gestão pública[33]. A necessidade desse tipo de abordagem mais participativa da sociedade é mais evidente nos casos de governança de sistemas complexos de prestação de serviços ao cidadão. A complexidade do ambiente de atuação das organizações públicas da atualidade, como aquela experienciada pelas Defensorias, demanda soluções igualmente complexas, para as quais as velhas práticas não são suficientes. Essa nova realidade aponta para uma revisão de tais práticas de gestão e governança públicas, trazendo à tona a

31 FORD, Cristie. New Governance in the Teeth of Human Frailty: lessons from financial regulation. Wisconsin Law Review, n. 441, 2010, p. 445.

32 PESTOFF, Victor e BRANDSEN, Taco. Public governance and the third sector: opportunities for coproduction and innovation? In: Osborne, Stephen P. "The new public governance? Routledge: 2010, p. 223- 236

33 TRUBEK, David M.; TRUBEK, Louise G. New governance & (and) legal regulation: Complementarity, rivalry, and transformation. Colum. J. Eur. L., v. 13, p. 539, 2006.

importância da modernização como elemento essencial à criação de valor público.

Como argumentado por estudiosos como David Trubek e John Braithwaite[34], é certo que a Nova Governança encontra desafios particulares em democracias instáveis e sociedades que não possuem uma estrutura robusta de organizações da sociedade civil, dificultando práticas mais experimentais e responsivas, mas isso não impede que, nessas sociedades, o poder público busque a cooperação com outros agentes para superação de limitações cognitivas na compreensão dos problemas de políticas públicas e na coordenação estatal de ações que estruturam políticas complexas.

É nesse sentido de enfrentamento de um grande desafio relativo à implementação de uma ambiciosa e necessária política pública, como um programa de governança de dados, que o engajamento das Defensorias Públicas junto a entidades da sociedade civil tem se mostrado de forma positiva. Identificamos durante a realização do projeto em parceria com as Defensorias Públicas dos Estados do Rio de Janeiro e São Paulo enormes avanços e grandes perspectivas no que toca a implementação de um programa de governança de dados, isso não só restrito às Defensorias Estaduais oficialmente conveniadas, mas também em todas as regiões do país, justamente pelo grau de capilaridade que esse tipo de atuação conjunta permite.

Governança de dados, um desafio particular às Defensorias Públicas

O projeto que fornece parte do material empírico que sustenta o presente artigo atua em duas frentes, uma de capacitação das Defensorias para manejar o tema da proteção de dados e, outra, de acompanhamento da implementação de programas de governança de dados. Um dos seus objetivos é que as Defensorias estejam aptas para lidar com casos que digam respeito à defesa do direito fundamental à proteção de dados. Para além disso, outro objetivo central é o de alinhar a perspectiva de adequação à LGPD com a promoção de políticas públi-

34 BRAITHWAITE, John. Responsive regulation and developing economies. World Development, v. 34, n. 5, p. 884-898, 2006. TRUBEK, David M.; COUTINHO, Diogo R.; SCHAPIRO, Mario G. Toward a New Law and Development: new state activism in Brazil and the challenge for legal institutions. World Bank Legal Rev., v. 4, p. 281, 2013.

cas, ou seja, incentivar que o ente não somente atue em conformidade com a lei, mas que também possa com isso ampliar sua capacidade de cumprir sua missão institucional.

É nesse sentido que a colaboração público-privada se mostra importante. Os objetivos não são o de ensinar um modelo de governança pronto às Defensorias ou forçar a incorporação de modelos forjados no Setor Privado. Pelo contrário, a ideia é que haja uma junção de conhecimentos para a construção de uma metodologia que seja adequada às Defensorias de um modo geral, para que cada uma, em suas particularidades, possa criar seu próprio programa de governança de dados. Outro ponto positivo, é que a cooperação se retroalimenta e se difunde, pois, a aproximação de instituições da sociedade civil da realidade das Defensorias, permite que essas instituições produzam mais materiais e conhecimentos que sirvam às necessidades do setor público, o que cria capilaridade a projetos que a priori ficam restritos à poucos agentes. No caso da parceria da Associação Data Privacy e das DPEs RJ e SP, houve uma abertura de portas para difusão em outras Defensorias[35].

Impossibilidade de transpante de matrizes do setor privado

Um dos primeiros pontos positivos do engajamento entre as Defensorias e a sociedade civil foi o enfrentamento da ausência de um exemplo de governança de dados dentro das instituições que compõem o sistema de justiça[36]. Apesar de muitos conteúdos serem produzidos para tratar da proteção de dados na esfera privada, até o presente momento, pouco material foi produzido no que diz respeito

35 Participaram do Curso extensivo de Proteção de Dados integrantes de catorze diferentes Defensorias de todas as cinco regiões do Brasil e o Grupo Focal de construção do Guia de Adequação à LGPD conta com a participação de integrantes de cinco Defensorias. Ainda, no que se refere à parceria junto ao Colégio Nacional de Defensores Públicos Gerais, foram distribuídas 120 vagas para realização do curso EAD da Data Privacy Brasil de Ensino, vagas estas que contemplaram integrantes de 21 Defensorias Públicas distintas, envolvendo as unidades federativas de: AC, AL, AM, BA, DF, ES, GO, MA, MT, MS, MG, PB, PI, RJ, RN, RS, RO, SC, SP, SE e TO.

36 Cabe aqui a ressalva acerca dos esforços e conquistas advindos das ações do CNJ. Ver: CONSELHO NACIONAL DE JUSTIÇA. Portaria N° 62 de 23/02/2021. Altera a Portaria nº 212/2020, que institui o Grupo de Trabalho destinado à elaboração de estudos e de propostas voltadas à adequação dos tribunais à Lei Geral de Proteção de Dados e dá outras providências. CONSELHO NACIONAL DE JUSTIÇA. Recomendação N° 73 de 20/08/2020. DJe/CNJ nº 272/2020, em 21/08/2020, p. 9-11.

à proteção de dados e as especificidades do poder público[37], com exceção dos trabalhos de Miriam Wimmer, que reconhecem que "no setor público, o tratamento de dados pessoais não se inicia, em geral, a partir de uma decisão voluntária do titular, mas como decorrência das exigências do próprio pacto social"[38]. Considerando não ser adequado o simples transplante das teorias, doutrinas e entendimentos próprios do setor privado para dentro da organização estatal, há para os entes públicos um esforço extra de compreensão dos impactos e deveres originados pelas normativas da proteção de dados.

Mesmo sem diferenciar as dificuldades entre o setor público e privado, a matéria, enquanto uma novidade no contexto brasileiro, traz um cenário de incertezas gerais experimentado por todos aqueles a quem a lei se aplica. No momento presente, existe uma série de especulações sobre como a ANPD se posicionará a respeito de determinadas matérias e até dúvidas acerca de quais outros órgãos terão competência para decidir impasses, litígios e inobservâncias à lei. A Autoridade publicou em janeiro de 2021, sua agenda regulatória para o próximo biênio, o documento prevê iniciativas normativas sobre temas relevantes como os direitos dos titulares, regras de notificação e comunicação à ANPD, o encarregado, entre outros, questões estas que todo agente de tratamento deve estar atento[39].

Apesar de se tratar de um cenário generalizado de insegurança jurídica, reafirmamos que os desafios são ainda maiores em relação às instituições públicas. Os efeitos da globalização já haviam forçado alguns entes privados a se adaptarem a normativas de proteção de dados no âmbito internacional, tais como a GDPR[40] e instruções da OCDE[41]. Apesar de empresas de atuação local não terem passado

37 Dentre os materiais disponíveis no momento, podemos citar os guias produzidos pelo Governo Federal. GOVERNO FEDERAL, Comitê Central de Governança de Dados. Guia De Boas Práticas, Lei Geral De Proteção de Dados (LGPD). Agosto de 2020. Disponível em: <https://www.gov.br/governodigital/ptbr/governanca-de-dados/GuiaLGPD.pdf>. Ver também: <https://www.gov.br/governodigital/ptbr/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd>.

38 WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades. Revista dos Advogados da AASP, n. 144, nov., 2019, p. 127.

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

40 O General Data Protection Regulation, Regulamento 2016/679 da União Europeia, é a normativa do direito europeu sobre privacidade e proteção de dados pessoais promulgada em 2018. Ver: https://gdprinfo.eu

41 Sigla para Organização para a Cooperação e Desenvolvimento Econômico, ente intergovernamental, fundado em 1961 com o propósito de estimular o progresso econômico e o comércio mundial. Ver: https://www.oecd.org

por esse processo em um primeiro momento, fato é que muito conhecimento se formou sobre as dinâmicas da proteção de dados dentro das perspectivas dos agentes privados. Isso traz duas consequências: o mercado possui mais material para guiar suas práticas e os aplicadores da lei possuem mais material para guiar e fiscalizar as práticas do mercado. No que diz respeito às instituições públicas, o cenário é muito mais incerto.

Diante da escassez de ferramentas teóricas e movimentos de liderança no campo da proteção de dados para o setor público, a cooperação com movimentos da sociedade civil inteirados na matéria se mostra como uma saída que viabiliza a consecução de um projeto de implementação de um programa de governança de dados. Assim, o que se busca alcançar não é transplante do privado para o público, mas a construção de conjunta de conhecimentos e trocas de experiências para que se possa garantir que os entes públicos consigam, por si mesmos, identificar quais os seus pontos mais sensíveis e para que a sociedade civil possa ajudar nessa descoberta e colaborar com soluções. Em um paralelo com o debate do direito comparado sobre "transplantes jurídicos"[42], defendemos a impossibilidade dos transplantes de metodologias de conformidade com a LGPD do setor privado para o público, como se "culturas jurídicas" distintas pudessem utilizar os mesmos instrumentos jurídicos, criados a partir de contextos radicalmente diferentes.

Nesse sentido, as perspectivas trazidas a respeito de uma nova governança pública se distanciam das ideias do paradigma administrativo irmão, a nova gestão pública[43], a qual promove a ideia de absorção de métodos de gestão do setor privado pelo setor público. Trata-se da inclusão daqueles interessados no tema dentro da execução das políticas com o objetivo de construção conjunta a partir da troca de conhecimentos e experiências.

Como exemplo de colaboração e construção conjunta, dentro do trabalho em desenvolvimento entre a Associação Data Privacy e as Defensorias Estaduais, podemos indicar a forma como foi estruturado o curso extensivo de proteção de dados para integrantes das Defensorias. Os cursos de proteção de dados em geral voltam-se exclusivamente para o setor privado, por isso, os exemplos, os estudos de casos e a literatura costumam estar sempre direcionados à realidade

42 LEGRAND, Pierre. The impossibility of 'legal transplants'. Maastricht Journal of European and Comparative Law, v. 4, n. 2, p. 111-124, 1997. EWALD, William. Comparative jurisprudence (II): the logic of legal transplants. The American Journal of Comparative Law, v. 43, n. 4, p. 489-510, 1995.

43 WIESEL, Fredrika; MODELL, Sven. From new public management to new public governance? Hybridization and implications for public sector consumerism. Financial Accountability & Management, v. 30, n. 2, p. 175-205, 2014.

corporativa. Identificando que seria importante capacitar os defensores a partir da aplicação da proteção de dados em sua realidade, houve uma extensa modulação metodológica para construção de um curso que trouxesse exemplos e atividades práticas coerentes com o dia a dia das Defensorias. Foram realizadas inúmeras reuniões com coordenadores e Defensores Públicos Gerais das DPEs, houve um processo de revisão bibliográfica sobre o funcionamento e a história das Defensorias e, além disso, foi conduzida uma série de entrevistas semiestruturadas com integrantes de diferentes setores dos órgãos. Com esse processo, identificamos um ganho duplo, por um lado os defensores foram convidados durante o curso a refletir sobre questões que realmente dizem respeito aos seus trabalhos cotidianos, o que traz um ganho de aprendizagem muito maior, e, por outro, isso forneceu novos insumos para que os pesquisadores da Associação compreendessem a realidade das Defensorias e os maiores desafios no que toca a proteção de dados na instituição.

Diferentemente de metodologia majoritariamente adotada no setor privado em que o principal instrumento para mapear os fluxos de dados se dá através de entrevistas com áreas estratégicas e preenchimentos de formulários semiestruturados, percebeu-se que o curso de capacitação, desde que formatado em uma metodologia ativa de aprendizado, é tão senão mais potente que tais ferramentas. Ao longo das atividades práticas e resolução de casos, os defensores e servidores não apenas relatavam, mas, também, já propunham soluções e conexões com outras áreas e outros processos também afetados, ainda que não como o objeto principal da atividade. Uma posição ativa e menos reativa que tornou, inclusive, mais ágeis as discussões travadas nos Comitês de Governança, formado em sua grande maioria por participantes do curso, que já tinham vislumbrado os principais gargalos e vulnerabilidades do fluxo de dados das Defensorias nas atividades de simulação.

Diferenças estruturais entre Defensorias

Uma segunda especificidade que toca às Defensorias é a forma particular de organização interna de cada ente e de cada órgão. Apesar de utilizarmos o termo Defensorias de uma forma ampla para nos referirmos às Defensorias da União, do Distrito Federal e das diversas Defensorias Estaduais, a estruturação e

a organização de cada um desses entes se dá de uma forma bastante particular. Defensorias Públicas como a do Rio de Janeiro, atuam há mais de 50 anos[44], enquanto outras como a de São Paulo há pouco mais de 15[45], em estados como o Paraná o número de Defensores por habitante chega a quase 100 mil, enquanto em Roraima, o número é de cerca de 13 mil[46].

Fora isso, há de se considerar também a autonomia funcional e administrativa das Defensorias. A autonomia nos dois aspectos serve para garantir às Defensorias Públicas o exercício de suas funções de modo livre de ingerências de qualquer outro órgão do Estado[47], a previsão as protege de pressões políticas e desvios de sua missão institucional. Garantia distinta, mas correlata é a independência funcional dos Defensores Públicos, prevista no art. 3º da Lei Complementar nº 80/94, que conhece aos Defensores a liberdade para atuar conforme seu melhor julgamento e convicção profissional. A autonomia e a independência colaboram com o cumprimento da missão institucional das Defensorias, e ocasionam, também, particularidades organizacionais entre elas e outros órgãos.

A consequência disso é que não podemos falar simplesmente na criação de um único modelo de governança de dados que servirá adequadamente para todas as Defensorias. O desafio que surge, portanto, é muito maior, pois envolve a construção de metodologias que permitam que cada um desses órgãos compreenda adequadamente como desenvolver seus próprios programas. Nesse sentido que os materiais que têm sido produzidos conjuntamente entre as Defensorias e a Associação de Pesquisa possuem como foco não a formulação de um passo a passo do que deve ser feito, mas os relatos dos desafios e soluções observados durante o acompanhamento do trabalho dos comitês de proteção de dados e, também, metodologias possíveis a serem adotadas para que as Defensorias, compreendendo sua realidade, possa construir um programa de governança de dados.

44 Ver: https://defensoria.rj.def.br/Institucional/historia

45 ASSEMBLÉIA LEGISLATIVA DO ESTADO DE SÃO PAULO. Lei Complementar Estadual nº 988, de 9 de janeiro de 2006. Organiza a Defensoria Pública do Estado, institui o regime jurídico da carreira de Defensor Público do Estado. Disponível em: <https://www.al.sp.gov.br/repositorio/legislacao/lei.complementar/2006/lei.complementar-988-09.01.2006.html>.

46 MIGALHAS. Acesso à Justiça. Paraná é o Estado com menos defensores públicos por habitante no Brasil. Disponível em: <https://www.migalhas.com.br/quentes/318863/parana-e-o-estado-com-menos-defensores-publicos-por-habitante-no-brasil>.

47 DA SILVA, José Afonso. Comentário contextual à Constituição. 2a ed. São Paulo, Malheiros, 2006. p. 615

Capacitação e papel educacional

As possibilidades em termos de conscientização e de capilaridade de difusão de conhecimentos são outro ponto positivo que pode ser alavancado pela atuação conjunta das Defensorias e entidades da sociedade civil. A cooperação ajuda, por exemplo, que a rede de contatos de pessoas engajadas no tema seja ampliada, o que faz surgir oportunidades para criação de eventos e para a formação de grupos específicos de construção de materiais, abrindo espaços para o compartilhamento de experiências. Criam-se também, oportunidades para capacitação dos profissionais. Neste projeto de parceria, desenvolvemos um eixo educacional, composto por um curso extensivo, um curso EAD e a perspectiva de realização de seminários de aprendizagem horizontal. Esse processo de capacitação dos integrantes permite que eles colaborem com a construção de materiais didáticos que servirão de insumo para outras Defensorias pelo país. No primeiro semestre de 2021, lançamos um guia de primeiros passos para a adequação das Defensorias à LGPD, elaborado junto a um grupo focal de alunos de diferentes Defensorias que realizaram o curso extensivo. As perspectivas são de que no futuro sejam ainda produzidos uma matriz de governança de dados adaptada à realidade das Defensorias e um roadmap condensando as experiências de todo o projeto de parceria.

O engajamento também traz resultados da perspectiva externa aos órgãos. As Defensorias têm promovido discussões abertas ao público, webinars e palestras que se designam não somente à Defensores, mas a outros membros do setor público. Como exemplo de alguns eventos que foram promovidos como fruto desta parceria mencionamos os seminários: "Defensoria Pública: novos desafios"[48], "Reflexões sobre a Lei Geral de Proteção de Dados e a atuação das Defensorias Públicas"[49], "Proteção de Dados Pessoais e o papel das Defensorias Públicas"[50] e "LGPD e acesso à justiça, da teoria à prática"[51].

Fora isso, as Defensorias também têm se preocupado com seu papel de promover a educação em direitos para a população. Nas reuniões de acompanhamento dos comitês de proteção de dados, algo ressaltado diversas vezes foi a im-

48 Ver: https://www.anadef.org.br/noticias/ultimas-noticias/item/webinar-anadef-enadpu-defensoria-publica-novos-desafios.html

49 Evento organizado pela Escola Nacional da Defensoria Pública da União, realizado em 28 de agosto de 2020.

50 Ver: https://www.youtube.com/watch?v=Cgc7QALFHZs&feature=youtu.be

51 Evento organizado pela Defensoria Pública do Estado do Ceará, realizado em 4 de dezembro de 2020.

portância da adequação da Defensoria como forma de se dar exemplo, mostrando aos usuários da instituição que a proteção de seus dados deve ser considerada por todo e qualquer outro agente de tratamento. Quando discutia a respeito da criação de uma página específica para o seu órgão encarregado, a Defensoria Pública de São Paulo frisou esse aspecto, valorando a ideia de transparência e facilidade para que o usuário faça valer seu direito à proteção de dados.

Em síntese, o debate sobre a proteção de dados pessoais nas Defensorias Públicas deve levar em consideração (i) a impossibilidade dos transplantes de metodologias do setor privado para o setor público, (ii) as diferenças estruturais entre Defensorias, rompendo com a ideia de algo monolítico e (iii) as oportunidades de experimentação e capacitação, promovendo aprendizados horizontais entre Defensorias. As políticas públicas no sistema de justiça podem aproveitar o potencial de aprendizado horizontal e experimentação, sem necessariamente um nódulo central de coordenação, controle e irradiação normativa[52].

52 HUITEMA, Dave et al. Policy experimentation: core concepts, political dynamics, governance and impacts. Policy Sciences, v. 51, n. 2, p. 143-159, 2018.

Conclusão

A partir do projeto analisado, concluímos que a atuação conjunta entre Defensorias e sociedade civil tem colaborado para o enfrentamento daqueles previamente identificados como os três grandes gargalos da incorporação da proteção de dados em organizações. No que toca o isolamento entre equipes e falta de comunicação, essa atuação promoveu o engajamento multissetorial dentro da instituição, incorporando integrantes de diferentes áreas de atuação nos cursos de capacitação promovidos e também nos grupos e comitês de formulação de documentos de apoio e eventos. Em relação aos investimentos em capacitação, a cooperação não só permitiu que integrantes das Defensorias tivessem acesso a cursos e materiais como também, desencadeou processos em que os próprios órgãos promovem seminários e trocam entre si experiências em uma rede de apoio inter-regional. Por fim, a ausência de um clima institucional voltado à proteção de dados foi enfrentada com o constante diálogo entre o setor de gestão das Defensorias e a Associação, que juntos construíram uma perspectiva de projeto que fosse adequada a realidade do ente e que promovesse a ideia de que a adequação da LGPD não é apenas uma questão de conformação legal, mas um trabalho com o potencial colaborar com o alcance da missão institucional das Defensorias.

A atuação conjunta entre as Defensorias e uma organização da sociedade civil para a incorporação de uma política pública de alta complexidade como um programa de governança de dados tem se mostrado de forma benéfica ao ampliar o alcance da política e ampliar sua capacidade de transformação, indo de encontro com a missão institucional das Defensorias. Do ponto de vista do potencial que um programa de governança possui sobre a eficiência administrativa, há os impactos internos de melhoria organizacional da gestão interna e, também, os impactos externos em termos da qualidade e alcance do serviço prestado. No mesmo sentido, a governança de dados possibilita que a administração tenha mais facilidade para automatizar sistemas e para tomar decisões baseadas em dados. Isso traz ganhos em termos de eficiência, o que de modo indireto implica também na qualidade do serviço. De forma direta, a capacidade da Defensoria de perceber com fidedignidade o trabalho realizado pelo ente como um todo abre espaços para que ela utilize tais informações para atuar estrategicamente sob demandas, como por meio de ações civis públicas e coletivas ou mesmo se utilizando dos dados gerados pelos seus sistemas para apontar a existência de um determinado

problema ao executivo, pressionando a execução de determinada política pública.

Essa perspectiva de ganhos de gestão é um dos pontos que norteou a estruturação do projeto de parceria entre a Associação de Pesquisa e as Defensorias Estaduais. Com base em experiências prévias e conhecimentos da Associação acerca de outros casos de sucesso em que instituições obtiveram melhorias organizacionais a partir da implementação de programas de governança de dados, foi possível construir conjuntamente com as Defensorias um plano de trabalho que incorporasse a perspectiva da eficiência administrativa. A existência de cursos com atividades práticas permite que sejam exploradas diferentes formas de utilização das informações como meios de garantir uma administração guiada por dados. Do mesmo modo, o trabalho contínuo de acompanhamento das reuniões junto aos comitês de proteção de dados, permite que pesquisadores compreendam as particularidades dos desafios de uma defensoria e possam colaborar com a construção conjunta de soluções e com sua divulgação.

Ainda no que diz respeito ao alcance dos objetivos das Defensorias, é necessário lembrar que a governança de dados está diretamente relacionada à tutela dos direitos à privacidade e à proteção de dados dos usuários desse serviço público. As Defensorias realizam milhões de atendimentos anualmente e possuem sob sua guarda e confiança informações das mais diversas de seus usuários, público que pela própria atribuição das Defensorias encontra-se em algum tipo de situação de vulnerabilidade, seja econômica ou social. Isso traz duas implicações, que os titulares que compõem a base de dados das Defensorias correspondem em boa medida ao público que mais sofre violações de seus direitos à privacidade e proteção de dados e, também, que para essa população a Defensoria é a única alternativa a qual podem recorrer a fim de buscar a defesa de seus direitos. Em razão do volume e do potencial discriminatório das informações que compõem o banco de dados das Defensorias, o cuidado com o manejo e a segurança das informações deve ser redobrado. Para além do risco ou do dano em si, há ainda a perspectiva de uma relação de confiança. O usuário da Defensoria não pode ficar sujeito a uma menor proteção de suas informações pessoais, primeiro por ser este um direito, segundo, porque na maioria das vezes buscar outro serviço não é uma opção.

Por tudo isso, conclui-se existir um grande potencial para que as Defensorias transformem seu processo de conformação à LGPD em uma verdadeira política pública. Essa política se desenrola ao garantir o tratamento de dados adequado dos usuários, mas vai além, criando espaços para que a reestruturação organizacional

alavanque outros processos que vão de encontro com a missão institucional dos entes e com os princípios da administração pública. Considerando que esta é uma abordagem ainda pouco explorada e cuja execução não é simples, a cooperação junto a organizações da sociedade civil é bem-vinda, hipótese esta até então corroborada pelos resultados obtidos no projeto.

Bibliografia

BIONI, Bruno Ricardo. Inovar pela lei. *GV EXECUTIVO*, v. 18, n. 4, p. 30-33, 2019.

BRAITHWAITE, John. Responsive regulation and developing economies. *World Development*, v. 34, n. 5, p. 884-898, 2006.

Conselho Nacional de Justiça. Gilmar Mendes assume presidência do CNJ. Disponível em: <https://www.cnj.jus.br/gilmar-mendes-assume-presidia-do-cnj/>.

Conselho Nacional de Justiça. Justiça em Números 2020. Disponível em: <https://www.cnj.jus.br/wpcontent/uploads/2020/08/WEB_V2_SUMARIO_EXECUTIVO_CNJ_JN2020.pdf>.

Conselho Nacional de Justiça. PB: Judiciário conclui digitalização de mais de 44 mi de páginas de processos. Disponível em: <https://www.cnj.jus.br/pb-judiciario-concluidigitalizacao-de-mais-de-44-milhoes-de-paginas-de-processos/>.

Conselho Nacional de Justiça. Projetos de inovação promoverão efetividade e ampliação do acesso à justiça no Brasil. Disponível em: <https://www.cnj.jus.br/inovacao--promoveraoefetividade-e-ampliacao-do-acesso-a-justica-no-brasil/>.

Consultor Jurídico. Brasil atinge a marca de 100 milhões de processos em tramitação na Justiça. Disponível em: <https://www.conjur.com.br/2015-set-15/brasil-atinge-marca-100-milhoes-processos-tramitacao>.

DA SILVA, Jeovan Assis; DE ABREU, Pedro; FLORÊNCIO, Lima. Políticas judiciárias no Brasil: o Judiciário como autor de políticas públicas. *Revista do Serviço Público*, v. 62, n. 2, p. 119-136, 2011.

DA SILVA, José Afonso. *Comentário contextual à Constituição*. 2ª ed. São Paulo, Malheiros, 2006.

EUBANKS, Virginia. Automating inequality: How high-tech tools profile, police, and punish the poor. *St. Martin's Press*, 2018.

FONTAINHA, Fernando; DE OLIVEIRA, Fabiana Luci; VERONESE, Alexandre. Por uma sociologia política do direito no Brasil. *Revista Brasileira de Sociologia*, v. 5, n. 11, p. 29-47, 2017.

FORD, Cristie. New Governance in the Teeth of Human Frailty: lessons from financial regulation. *Wisconsin Law Review*, n. 441, 2010.

GERALDO, Pedro Barros; FONTAINHA, Fernando; VERONESE, Alexandre. Sociologia empírica do direito: Uma introdução. *Revista Ética e Filosofia Política*, v. 2, n. 12, 2010.

HOWLETT, Michael. *Designing public policies: Principles and Instruments*. London: Routledge, 2019.

HUITEMA, Dave et al. Policy experimentation: core concepts, political dynamics, governance and impacts. *Policy Sciences*, v. 51, n. 2, p. 143-159, 2018.

LEGRAND, Pierre. The impossibility of 'legal transplants'. Maastricht Journal of European and Comparative Law, v. 4, n. 2, p. 111-124, 1997. EWALD, William. Comparative jurisprudence (II): the logic of legal transplants. *The American Journal of Comparative Law*, v. 43, n. 4, p. 489-510, 1995.

LOPES, José Reinaldo de Lima; FILHO, Roberto Freitas. Law and Society in Brazil at the crossroads: a review. *Annual Review of Law and Social Science*, v. 10, p. 91-103, 2014.

MIGALHAS. Acesso à Justiça. Paraná é o Estado com menos defensores públicos por habitante no Brasil. Disponível em: <**https://www.migalhas.com.br/quentes/318863/parana-eo-estado-com-menos-defensores-publicos-por-habitante-no-brasil**>.

Migalhas. MJ aponta principais problemas do Judiciário brasileiro. Disponível em: <**https://www.migalhas.com.br/quentes/195678/mj-aponta-principais-problemas-do-judiciario-brasileiro**>.

MURTA, João. *Descontinuidade na administração judiciária*. Belo Horizonte: Editora Dialética, 2021.

O'NEIL, Cathy. Algoritmos de Destruição em Massa: Como o Big Data Aumenta a Desigualdade e Ameaça à Democracia. Trad. Rafael Abraham. 1 ed. Santo André, SP: Rua do Sabão, 2020.

PAPACHARISSI, Zizi. Privacy as a luxury commodity. First Monday, 2010.

PESTOFF, Victor e BRANDSEN, Taco. Public governance and the third sector: opportunities for co-production and innovation? In: Osborne, Stephen P. "The new public governance? Routledge: 2010.

Portal G1. Defensoria Pública cobra na Justiça informações do Metrô de SP sobre câmeras de reconhecimento facial. Disponível em: <**https://g1.globo.com/sp/saopaulo/noticia/2020/02/11/defensoria-publica-cobra-na-justica-informacoes-do-metro-de-sp-sobre-cameras-de-reconhecimento-facial.ghtml**>.

RIBEIRO, Marcia Carla Pereira; DE PAULA MACHADO, José Alberto Oliveira. Acesso à Justiça e a Defensoria Pública na América Latina: democratização de direitos como desenvolvimento. Direito e Desenvolvimento, v. 8, n. 1, p. 89-106, 2017.

SADEK, Maria Tereza. A Defensoria Pública no sistema de justiça brasileiro. São Paulo: APADEP em Notícias, p. 2-2, 2008.

SADEK, Maria Tereza. Acesso à justiça: um direito e seus obstáculos. *Revista USP*, n. 101, p. 55-66, 2014.

SADEK, Maria Tereza. Acesso à justiça: visão da sociedade. *Revista Justitia*, São Paulo, v. 65, n. 198, p. 271-279, 2008.

SADEK, Maria Tereza. Judiciário: mudanças e reformas. Estudos avançados, v. 18, n. 51, p. 79-101, 2004.

SILVA, Michelle Valéria Macedo *et al*. Direitos humanos. Acesso à justiça. Defensoria pública. Pobreza. Exclusão social. Revista da Defensoria Pública da União, n. 06, 2013.

TRUBEK, David M.; COUTINHO, Diogo R.; SCHAPIRO, Mario G. Toward a New Law and Development: new state activism in Brazil and the challenge for legal institutions. World Bank Legal Rev., v. 4, p. 281, 2013.

TRUBEK, David M.; TRUBEK, Louise G. New governance & (and) legal regulation: Complementarity, rivalry, and transformation. Colum. J. Eur. L., v. 13, p. 539, 2006.

WALDMAN, Ari Ezra. Designing without privacy. Hous. L. Rev., v. 55, p. 659, 2017

WIESEL, Fredrika; MODELL, Sven. From new public management to new public governance? Hybridization and implications for public sector consumerism. *Financial Accountability & Management*, v. 30, n. 2, p. 175-205, 2014.

WIMMER, Miriam. O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: BIONI, Bruno; SCHERTEL, Laura; DONEDA, Danilo; SARLET, Ingo; RODRIGUES, Otavio. *Tratado de Proteção de Dados*. Rio de Janeiro: Forense, 2021, p. 276.

WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades. *Revista dos Advogados da AASP*, n. 144, nov., 2019, p. 127.

GUIA DE **PRIMEIROS PASSOS** PARA A ADEQUAÇÃO DAS **DEFENSORIAS PÚBLICAS** À LGPD

GUIA DE PRIMEIROS PASSOS PARA A ADEQUAÇÃO DAS DEFENSORIAS PÚBLICAS À LGPD[1]

BRUNO R. BIONI
RAFAEL A. F. ZANATTA
MARINA KITAYAMA

Agradecimentos

Este Guia é fruto de um amplo trabalho de cooperação, sem as muitas mãos e cabeças que colaboraram com a Associação Data Privacy Brasil de Pesquisa este documento não poderia ter sido elaborado. Agradecemos, portanto, a todos aqueles que contribuíram com a formação de ideias, coleta de materiais, escrita e críticas ao presente Guia de Primeiros Passos. Deixamos aqui nosso especial agradecimento:

À Fundação Ford, nas pessoas da Graciela Selaimen e Alberto Cerda, pela confiança depositada no trabalho da Associação Data Privacy Brasil de Pesquisa e pelo financiamento do projeto "Defensorias e Proteção de Dados", do qual se origina este documento.

Aos Defensores Públicos Gerais dos Estados do Rio de Janeiro e São Paulo, Rodrigo Baptista Pacheco e Florisvaldo Fiorentino Junior, que promoveram a parceria entre os entes e a Associação Data Privacy Brasil, representando o espírito público que move as Defensorias e demonstrando o constante interesse da instituição em aprimorar-se enquanto referência na promoção do acesso à justiça em diferentes frentes.

Aos Comitês de Proteção de Dados Pessoais das Defensorias dos Estados do Rio de Janeiro e São Paulo, que acolheram os pesquisadores da Associação durante suas discussões sobre a adequação do ente à LGPD e que forneceram

1 Esse material foi produzido no âmbito do projeto "Defensorias Públicas e Proteção de Dados" e aborda uma série de aspectos técnicos e jurídicos relacionados à adequação das Defensorias Públicas à LGPD. Originalmente foi disponibilizado no site <https://www.dataprivacybr.org/projeto/expandindo-o-papel-dos-defensores-publicos-na-protecao-de-dados-pessoais-no-brasil/>.

grande parte dos insumos e materiais empíricos do presente projeto.

Ao Grupo Focal deste Guia, composto por integrantes de diferentes Defensorias do Brasil, que trouxe perspectivas e críticas construtivas para o aprimoramento do material. Nominalmente, agradecemos a: Bruna Simões, Defensora Pública do Estado de São Paulo; Daniela Cecin Lima, Analista Processual na Corregedoria-Geral da Defensoria Pública do Estado do Rio Grande do Sul; Eduardo Fontes, Defensor Público do Estado de São Paulo; Marina Lowenkron, Defensora Pública do Estado do Rio de Janeiro; Nelson Keller, Defensor Público do Estado do Rio de Janeiro; Rogério Souza Couto, Defensor Público do Estado do Rio Grande do Sul; Sarah Gomes Sakamoto, Analista de informática na Defensoria Pública do Estado do Paraná e; Thales de Almeida, Coordenador de Modernização e Informática na Defensoria Pública do Estado da Bahia.

À Professora Maria Tereza Sadek, por prefaciar o presente Guia, pela participação nas discussões junto ao Grupo Focal e pelos ensinamentos que nortearam muitas das percepções sobre acesso à justiça deste documento.

Prefácio

MARIA TEREZA AINA SADEK[2]

"O avanço tecnológico traz oportunidades e desafios.
Se não aproveitarmos as oportunidades logo,
ficaremos apenas com os desafios" - Ronaldo Lemos

Nos últimos anos, a utilização de dados deixou de ser uma opção. Sem dados, qualquer diagnóstico não passa de mero "achismo" ou de uma suposição que se acredita retratar a realidade. Boas intenções não garantem resultados. Dados são absolutamente imprescindíveis para a elaboração de análises que direcionem políticas públicas com chances de alcançar os objetivos propostos.

Assim, produzir, colher e sistematizar dados compõem o ponto de partida de todo e qualquer projeto ou de planos de gestão, quer em organizações públicas ou privadas. Tais tarefas tornam-se imperativas em contextos em que os recursos são escassos – tanto humanos como materiais.

As instituições do sistema de Justiça não estão imunes a essas exigências. Ao contrário, cabe a elas, como instituições com atribuições de trabalhar em favor da cidadania, moldar-se a essas imposições. Quanto maior for esse compromisso, melhores e mais efetivos serão os resultados. Em outras palavras, as possibilidades de se construir uma sociedade mais inclusiva e republicana estão diretamente relacionadas a atuações baseadas em diagnósticos construídos a partir de dados.

No caso das Defensorias Públicas, esses pressupostos são ainda mais vitais. O número de defensores é muito inferior ao de integrantes do Poder Judiciário e do Ministério Público. Defensores não estão em todas as varas e em todos os municípios. A relação entre o número de defensores e de indivíduos em situação de vulnerabilidade fica muito aquém do desejado, tanto assim, que muitas Defensorias contam com o trabalho de advogados. Além disso, faltam recursos materiais. Consequentemente, procurar minimizar essas deficiências deve ser o principal objetivo na elaboração de planos de ação e na eleição de prioridades. Torna-se, pois, absolutamente indispensável conectar, relacionar dados institucionais e dados da realidade econômica e social.

Defensores são responsáveis por concretizar direitos em uma sociedade muito desigual. O contingente de excluídos dos bens públicos é significativo. Dados

do Ministério da Cidadania contabilizaram, em 2020, 40 milhões de indivíduos vivendo em condições de miséria. Esta situação sofreu impactos devastadores com a pandemia, que acelerou e agravou problemas já existentes. Foram expostas mazelas, como o número de invisíveis, isto é, de não cidadãos, de indivíduos sem identidade civil, sem condições de receber qualquer auxílio governamental.

Políticas de prevenção à disseminação do vírus recomendaram o isolamento. Advertência cientificamente correta, mas difícil de ser concretizada em uma sociedade marcada por altos graus de desigualdade. De fato, como se isolar em habitações que abrigam várias pessoas, sem espaço, sem privacidade, sem infraestrutura básica? Depauperados pela crise, como não se expor para buscar renda, como sobreviver? Em condição ainda mais crítica estão aqueles que sequer possuem um teto. Nessa situação, reclamar direitos, procurar a solução de conflitos, ainda que conste do rol de demandas desse contingente populacional, tornou-se mais difícil. Ao já extenso rol de disparidades econômicas e sociais, foi acrescida a desigualdade digital.

Tal confluência de problemas levou as Defensorias Públicas a se reinventarem. Medidas sanitárias passaram a impedir o atendimento presencial. Ferramentas tecnológicas foram acionadas, aprimoradas, adaptadas à nova realidade. O recebimento de solicitações e o respectivo processamento por meio digital implicou alterações de grande magnitude nos integrantes da instituição. Dentre essas mudanças, uma das mais importantes foi a necessidade de passar a compartilhar a cultura de dados, de tecnologia e suas implicações.

A despeito desses entraves, informações obtidas em Defensorias apontam números expressivos de atendimento tanto pelo telefone (0800), como pelo *WhatsApp*, como por outros meios digitais. Formulários eletrônicos foram encaminhados e respostas, providenciadas.

Assim, ao acúmulo de dados relativos aos usuários, às demandas, às soluções judiciais e extrajudiciais, em tempos ditos "normais", somaram-se as informações durante a pandemia. Esse extraordinário banco de dados é um patrimônio. Um patrimônio que deve ser protegido tal como determina a Lei Geral de Proteção de Dados, aprovada em 2018 e em vigor a partir de setembro de 2020.

O caminho para se adequar às determinações da Lei não é sem obstáculos. Saliente-se que nas instituições do sistema de Justiça são distintas as dificuldades. No Poder Judiciário, por exemplo, mesmo antes da crise sanitária prevaleciam as metas de digitalização de dados, de processos eletrônicos e de videoconferência. Esta situação é muito diferente daquela a que foi obrigada a enfrentar a Defen-

soria Pública. Bastaria lembrar que defensores lidam com indivíduos em situação de vulnerabilidade, que o contato pessoal faz a diferença.

As necessárias adaptações, tanto por parte dos vulneráveis como por parte dos defensores, como apontado, não paralisaram os atendimentos. Dessa forma, a Defensoria Pública somou aos dados já existentes os obtidos durante a pandemia. Trata-se de um acervo que armazena uma grande quantidade de informações relativas aos usuários. Ora, a proteção desses dados é uma questão da maior relevância. Pois, ao mesmo tempo em que dados pessoais podem contribuir para a obtenção de informações geradoras de benefícios para o conhecimento do perfil dos usuários e, consequentemente, para a elaboração de políticas institucionais, também podem constituir ameaças à privacidade.

A Lei Geral de Proteção de Dados, aprovada em 2018, e em vigor desde setembro de 2020, reforça a necessidade de investir em segurança digital. Como bem aponta o Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD, "as Defensorias possuem um desafio duplo no que toca à vigência da LGPD, tanto o de se adequar às previsões normativas do texto, quanto o de se capacitar para defender os interesses de seus usuários no que toca às violações de seus direitos à proteção de dados pessoais."

O aproveitamento dessa oportunidade tem condições de redundar em aperfeiçoamento de gestão, em atuações mais efetivas e em significativa contribuição no processo de universalização da inclusão social.

Preâmbulo

COMO LER ESSE GUIA?

Este Guia pretende abordar uma série de aspectos relacionados à adequação das Defensorias Públicas à Lei Geral de Proteção de Dados (LGPD). O documento percorre considerações de naturezas e profundidades diversas: desde as perspectivas e desafios que motivam a elaboração de um Guia até descrições históricas e estruturantes da matéria da proteção de dados e da LGPD, passando por questões práticas de execução de um projeto de adequação. Tendo em vista que determinados elementos podem ser de maior ou menor relevância para cada perfil de leitor, explicitamos neste preâmbulo um quadro geral de cada uma das quatro partes que compõem o Guia.

Na parte I, contextualizamos e descrevemos os aspectos metodológicos deste documento. Nesse sentido, o guia explora os desafios e perspectivas relacionadas ao processo de adequação das Defensorias à LGPD, tomando como base os materiais empíricos e bibliográficos coletados durante mais de um ano do projeto "Defensorias e Proteção de Dados" conduzido pela Associação Data Privacy Brasil de Pesquisa. Portanto, nessa primeira parte, fornecemos um panorama geral do problema de pesquisa, das razões que nos levam a acreditar que este é um tema de especial relevância às Defensorias e dos procedimentos adotados para a condução do projeto.

Na parte II, o guia trata dos aspectos centrais da LGPD. Para tanto, abordamos a história da tutela jurídica da proteção de dados no Brasil e do trâmite legislativo da LGPD, entendendo que esta perspectiva é de grande relevância para a leitura e interpretação da Lei. Também, nesta parte, tratamos da estrutura esquemática do texto legal, indicando algumas características de seus capítulos e situando o leitor sobre cada um deles.

Na parte III, o objetivo do guia é desmistificar o processo de adequação à LGPD, entendendo-o não somente como uma obrigação legal, mas também como um projeto compatível, em diversas frentes, com a missão institucional das Defensorias. Assim, a parte III perpassa diferentes processos relativos aos trabalhos diários do ente, a fim de apontar quais os possíveis impactos da LGPD e quais as vantagens relacionadas à implementação de um programa de governança de dados.

Na parte IV, nosso objetivo é tratar de alguns aspectos preliminares sobre como implementar, na prática, um projeto de adequação à LGPD. Assim, nesse

momento, o Guia aponta possíveis eixos de segmentação do processo e etapas que poderão compor a estratégia de execução de um projeto como este.

Antes de iniciar a leitura, é importante observar que o objetivo do Guia não é, e nem poderia ser, propor um "passo a passo" absoluto das medidas que uma Defensoria Pública deve adotar para se adequar à LGPD. Na realidade, todo o trabalho de pesquisa que embasa este documento parte da premissa de que não seria possível entregar um modelo pronto, que servisse apropriadamente à realidade complexa e múltipla de diferentes Defensorias brasileiras. Por essa razão, este Guia é um convite para reflexões acerca do uso dos dados, trazendo ideias e metodologias para que as próprias Defensorias compreendam o que é compatível com a sua realidade, recursos, necessidades e objetivos.

Parte 1
CONTEXTUALIZAÇÃO DO PROJETO, DESAFIOS E PERSPECTIVAS DE UM PROCESSO DE ADEQUAÇÃO À LGPD

Introdução e metodologia: contextualizando o projeto

O presente guia foi elaborado a partir das experiências do projeto desenvolvido pela Associação Data Privacy Brasil de Pesquisa e pelas Defensorias Públicas dos Estados do Rio de Janeiro e de São Paulo entre 2020 e 2021. Os convênios foram formalizados em setembro de 2020, mas as conjecturas em torno do projeto tiveram início quase um ano antes, e tanto as experiências da fase pré-convênio como as posteriores colaboraram para os resultados do guia, o qual pretende servir de inspiração para outras Defensorias iniciarem ou revisitarem seus programas de governança de dados, buscando adequar suas atividades à Lei 13.709/2018, a LGPD.

A idealização desta parceria surgiu a partir de algumas constatações sobre a importância de se pensar na adequação do sistema de Justiça à LGPD e na relevância das Defensorias como parte deste. Afinal, se Defensorias Públicas realizam o atendimento de milhões de cidadãos por ano, não haveria tratamento de dados pessoais de milhões de pessoas que buscam esse serviço público garantido pela Constituição? Além disso, considerando seu papel de promoção do acesso à justiça, as Defensorias também são importantes agentes da perspectiva de defesa de direitos da população frente ao uso abusivo de dados pessoais. Desse modo, a LGPD traz impactos tanto da perspectiva de seus trabalhos internos, como externos.

Aprovada em agosto de 2018 e vigente desde setembro de 2020, a Lei Geral de Proteção de Dados, como seu próprio nome sugere, tem um escopo de aplicação amplo e incide sobre todo tipo de tratamento de dados, seja no setor público ou privado (ressalvadas as hipóteses do art. 4º). O capítulo IV da LGPD dispõe sobre a aplicação da Lei em relação ao poder público, estabelecendo, conforme o art. 23º, que o tratamento para esses agentes "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público".

O artigo ainda indica que sua definição de pessoa jurídica de direito público corresponde àquela do art. 1º da Lei 12.527/2011 (Lei de Acesso à Informação, LAI daqui em diante). Desse modo, entende-se que há o enquadramento das Defensorias como um dos entes a que se refere o art. 23º da LGPD, tendo em vista que, apesar de não ser expressamente citada no dispositivo da LAI, a própria Defensoria compreende sua subordinação às suas previsões. Assim, as Defensorias, enquanto agentes de tratamento, estão submetidas aos ditames da LGPD e sujeitas às fiscalizações e determinações da Autoridade Nacional de Proteção de Dados (ANPD, daqui em diante) e de outros entes competentes[3].

Tal constatação traz implicações profundas para as Defensorias Públicas, considerando sua complexa organização funcional e administrativa, assim como a quantidade e a natureza dos dados pessoais tratados cotidianamente.

Em um país marcado por profundas desigualdades, a atribuição das Defensorias de defesa de direitos daqueles em situação de vulnerabilidade torna inevitável que o órgão detenha um alto volume de dados pessoais. A começar pelo fato de que, diante da escassez de recursos, as Defensorias precisam de critérios que determinem quem receberá atendimento. Assim, a grande maioria daqueles que buscam seus serviços tem de passar pelo procedimento de triagem socioeconômica, o que implica a coleta de quantidades substanciais de dados de renda do indivíduo e de integrantes de seu núcleo familiar.

Ainda, a relevância da adequação não é adstrita apenas ao volume e sensibilidade de dados tratados cotidianamente para a efetivação da assistência jurídica. A missão da Defensoria inclui também sua atuação na defesa de direitos coletivos e difusos, inclusive da população em situação de vulnerabilidade econômica e social, que é, normalmente, a mais constrangida a fornecer seus dados, seja para se tornar elegível e beneficiária de políticas e serviços públicos, seja como condição de acesso a serviços e produtos de consumo. Nesse sentido, mais do que se tornar uma instituição exemplar em termos de governança de dados, é de suma importância que os defensores e defensoras estejam capacitados para atuar em casos de abusos, do setor privado ou público, em relação ao tratamento de dados pessoais da população.

Como ficará claro ao longo deste Guia, a proteção de dados pessoais está profundamente ligada a assimetrias, desigualdades, cidadania e poder. Com a digi-

3 Sobre o assunto, ver FEICHAS, Roger, Da adequação da Defensoria Pública à Lei Geral de Proteção de Dados, in: FALEIROS JUNIOR, José Luiz; ROZATTI LONGHI, João Victor; GUGLIARA, Rodrigo. Proteção de dados pessoais na sociedade da informação: entre dados e danos. Indaiatuba: Editora Foco, 2021.

talização da sociedade em um cenário pós pandemia agravado pela crise sanitária (que é também social e econômica), aumentará a demanda de atuação das Defensorias, com uma pressão cada vez maior para que esses dados sejam protegidos adequadamente. Nesse sentido, há uma complementaridade entre defender os direitos relacionados aos dados no Judiciário e saber trabalhar corretamente com esses dados internamente, seja na jornada do atendimento, nas pesquisas ou nas atividades regulares da Defensoria.

Constatada a iminente necessidade de adequação das Defensorias à LGPD e sua relevância enquanto instituição voltada à proteção de direitos fundamentais, surgiram as primeiras imagens de um projeto que abordasse tais questões. Para além disso, o projeto surgiu de uma percepção do interesse das próprias Defensorias e de um cenário de escassez de materiais específicos para o setor público. A Data Privacy Brasil Ensino, atuando enquanto escola de formação em proteção de dados, capacitou mais de 3 mil alunos, muitos deles defensores que traziam para as aulas questões relativas à instituição[4]. Alguns dos professores da escola, mobilizados pelas Defensorias, foram convidados a participar de seminários e palestras sobre o tema, iniciativas estas tomadas pelos próprios entes, não existindo um planejamento ou coordenação unificada do sistema de Justiça com o intuito de promover conhecimentos sobre as particularidades do setor público em relação à adequação à LGPD.

Todos estes elementos compuseram a força motriz para a criação de um projeto que promovesse a discussão do tema junto às Defensorias. A Fundação Ford, entidade que financia projetos de direitos humanos há décadas no Brasil, reconheceu a importância da proteção de dados pessoais para as atividades meio e fim das Defensorias e financiou a proposta da Associação Data Privacy Brasil de Pesquisa. O objetivo é subsidiar a dupla jornada a ser enfrentada pelas Defensorias: a de adequação interna e a de capacitação de seus membros para a defesa de direitos fundamentais relacionados à proteção de dados.

Assim as perguntas que orientam o projeto são: como otimizar a atuação das Defensorias Públicas na defesa de direitos fundamentais, especialmente a privacidade e a proteção de dados pessoais, e como o ente pode se adequar à LGPD e tornar-se um exemplo para o setor público, especialmente para o sistema de Justiça?

4 A escola passou a ofertar bolsas gratuitas para Defensores Públicos e para membros de organizações da sociedade civil que atuam com direitos difusos e coletivos.

O convênio firmado com as Defensorias Públicas do Rio de Janeiro e São Paulo foi idealizado a fim de enfrentar tais questões. Para tanto, fundamenta-se em dois pilares: um educacional e outro de acompanhamento da implementação de programas de governança de dados das Defensorias, o qual pretende trazer, como resultado, documentos como este, que sirvam como diretriz para outras Defensorias do país.

Nesta primeira parte do Guia, explicamos como a pesquisa em curso foi concebida, quais os principais desafios identificados e qual a finalidade deste material.

a. Fase inicial: aproximação e modelagem de pesquisa-colaboração

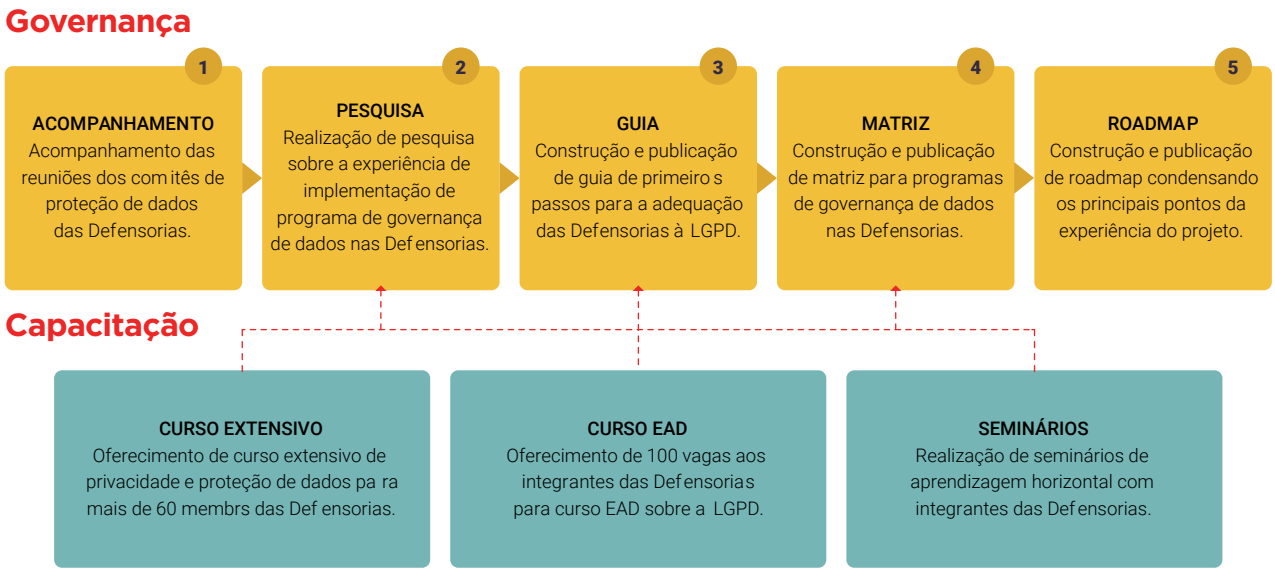
Para atender aos dois pilares estruturantes do projeto, foi essencial traçar um plano de trabalho compatível com a realidade das Defensorias, razão pela qual sua construção ocorreu de modo colaborativo. Tendo em vista a complexidade do projeto, não seria possível estabelecer parcerias formais com todas as Defensorias Públicas do país, de modo que a Associação optou por firmar convênios com os dois maiores entes (em termos de número de defensores e de atendimentos realizados) sendo estas as Defensorias dos estados do Rio de Janeiro e de São Paulo. Apesar dessa escolha, a proposta do projeto é ter um alcance amplo, que gere exemplos institucionais e materiais de engajamento a serem difundidos pelo país.

Sobre o primeiro pilar, o programa de capacitação tem como finalidade fornecer capacitação, por meio de aulas, além de outros insumos e materiais para que os membros das Defensorias possam conduzir seus próprios programas de governança de dados e, também, para que estejam aptos a atuar na defesa de direitos relacionados à proteção de dados pessoais. Nesse sentido, entendeu-se como essencial a adequação do curso à realidade da instituição, razão pela qual a estruturação das aulas se deu a partir de uma pesquisa qualitativa, realizada a partir de 14 (catorze) entrevistas com membros de diferentes áreas das Defensorias. A compreensão de suas particularidades e dinâmicas internas permitiu que o curso trouxesse estudos de casos modulados à realidade das Defensorias (anexo I).

A introdução de casos personalizados, além de promover uma capacitação mais compatível com o perfil dos alunos, também se revelou uma chave central para o segundo pilar do projeto, servindo como indicador das principais fragilidades e dificuldades a serem enfrentadas em um processo de adequação.

Este segundo pilar, por sua vez, também possui dois componentes: o de acompanhamento da implementação do programa de governança de dados e o de realização de pesquisa sobre a experiência das Defensorias durante o processo de adequação. O método adotado foi o da pesquisa etnográfica, a partir do acompanhamento das reuniões de grupos de trabalho das Defensorias conveniadas. Apesar da restrição aos entes formalmente envolvidos no projeto, este componente pretende concretizar as experiências dos participantes e consolidar materiais e guias que poderão ser difundidos para os demais órgãos do Brasil.

No desenho do projeto, a Associação Data Privacy Brasil de Pesquisa não realiza uma consultoria às Defensorias. Na realidade, a Associação engaja-se em um processo de formação, capacitação e pesquisa qualitativa de campo, com acompanhamento das reuniões e processos decisórios conduzidos pelas próprias Defensorias.



b. Estratégias de engajamento e mobilização

Dentre os desafios enfrentados para a consecução deste projeto, o primeiro deles foi o de engajamento. Era necessário demonstrar aos membros das Defensorias, afora os que compõem sua administração, que a pauta é relevante. O trabalho exige uma mudança de hábitos e de cultura considerável, o processo de adequação não cessa no tempo, e surgem deveres e procedimentos que só fazem sentido se forem perpetuados por aqueles envolvidos nas atividades diárias

das Defensorias. Assim, trata-se de um desafio coletivo, de modo que promover o engajamento dos membros é essencial.

Para concretizar este primeiro passo, antes do início efetivo dos trabalhos, foram realizadas diversas reuniões com membros da administração das Defensorias do Rio de Janeiro, de São Paulo e da União, além de encontros com Defensores dos estados de Minas Gerais e Paraná[5]. A série de diálogos e trocas, além de aproximar a Associação dos membros das Defensorias, deu origem ao seminário de lançamento do projeto[6], que contou com a presença dos Defensores Públicos Gerais dos estados conveniados, Rodrigo Pacheco e Florisvaldo Junior, defensores de diferentes áreas e incluiu palestra da Professora Maria Tereza Sadek, referência acadêmica no tema do acesso à justiça e prefaciadora do Guia. Além disso, logo de início foi travada uma série de diálogos entre a Associação e membros das Defensorias. As entrevistas (anexo I) realizadas para a elaboração do curso de capacitação também auxiliaram nesse processo de engajamento com os integrantes dos órgãos.

Formalmente iniciado no começo de setembro de 2020, já é possível verificar frutos do trabalho que vem sendo desenvolvido. No que diz respeito à mobilização, as Defensorias já começaram a se organizar em grupos de trabalho e a pensar em seus próprios projetos de adequação. A Defensoria de São Paulo, por exemplo, promulgou o Ato Normativo no 183[7], designando um órgão encarregado colegiado responsável por toda a matéria de proteção de Dados referente às atividades do ente, enquanto a Defensoria do Rio de Janeiro promulgou a Resolução nº 1090[8], que institui sua política de governança de dados.

5 Apesar do projeto vincular-se à parceria formal com as Defensorias Públicas dos Estados do Rio de Janeiro e São Paulo a Associação Data Privacy está em constante diálogo com entes de outros estados que, pelas limitações de recursos financeiros e humanos do projeto, não puderam ser oficialmente incluídas em todas as etapas de pesquisa.

6 Disponível em: https://youtu.be/Cgc7QALFHZs.

7 DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO. Ato Normativo DPG nº 183, de 21 de setembro de 2020. Disponível em: <https://www.defensoria.sp.def.br/dpesp/Conteudos/Materia/MateriaMostra.aspx?idItem=91034&idModulo=9788>.

8 DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO. Resolução DPGERJ nº 1090 de 09 de abril de 2021.

c. Desafios imediatos

A perspectiva positiva sobre o andamento do projeto é, sem dúvida, uma vitória, mas os desafios a serem enfrentados ainda são muitos, principalmente considerando o cenário de incertezas sobre a matéria no âmbito nacional. Primeiramente, ainda é um obstáculo a ausência de exemplos concretos dentro das instituições que compõem o sistema de Justiça (apesar dos esforços do Conselho Nacional de Justiça em reforçar a importância da LGPD e de projetos de adequação no Judiciário). A consequência direta disso é a falta de materiais e instruções claras do que deve ou não ser realizado. Apesar de muitos conteúdos serem produzidos para tratar da proteção de dados na esfera privada, há pouco material que aborda a série de peculiaridades da atuação pública. Transplantar as teorias, doutrinas e entendimentos para dentro da organização estatal demanda um esforço extra em relação aos processos de adequação vivenciados por entes privados.

Considerando que a matéria é uma novidade no contexto brasileiro, há ainda o cenário de incertezas gerais experimentado por todos aqueles a quem a lei se aplica. No momento presente, existe uma série de especulações sobre como a ANPD se posicionará a respeito de determinadas matérias e também dúvidas sobre possíveis conflitos e sobreposições de competências para regular, fiscalizar e aplicar a lei. A Autoridade publicou, em janeiro de 2021, sua agenda regulatória para o próximo biênio[9]. O documento prevê iniciativas normativas sobre temas relevantes como os direitos dos titulares, regras de notificação e comunicação de incidentes de segurança à ANPD e aos titulares, a figura do encarregado, entre outros, questões estas relevantes para todo agente de tratamento de dados pessoais.

Apesar de se tratar de um cenário de insegurança jurídica geral, ele afeta ainda mais as instituições públicas. Os efeitos da globalização já haviam forçado alguns entes privados a se adaptarem a normativas de proteção de dados no âmbito internacional, tais como a GDPR[10] e instruções da OCDE[11]. Apesar de empresas

9 Autoridade Nacional de Proteção de Dados. Portaria nº 11, de 27 de janeiro de 2021. Torna pública a agenda regulatória para o biênio 2021-2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>.

10 O General Data Protection Regulation, Regulamento 2016/679 da União Europeia, é a normativa do direito europeu sobre privacidade e proteção de dados pessoais promulgada em 2018. Ver: https://gdpr-info.eu

11 Sigla para Organização para a Cooperação e Desenvolvimento Econômico, ente intergovernamental, fundado em 1961 com o propósito de estimular o progresso econômico e o comércio mundial. Ver: https://www.oecd.org

de atuação local não terem passado por esse processo em um primeiro momento, o fato é que muito conhecimento se formou sobre as dinâmicas da proteção de dados a partir das perspectivas dos agentes privados. Assim, tanto o mercado tem mais material para guiar suas práticas, como os aplicadores da lei têm mais material para guiar e fiscalizar as práticas do mercado. No que diz respeito às instituições públicas, o cenário é consideravelmente mais incerto.

d. Pandemia da COVID-19

A crise sanitária ocasionada pela pandemia de COVID-19 não poderia deixar de ser referenciada neste documento. O colapso na saúde está diretamente relacionado ao aumento expressivo de problemas sociais e econômicos, o que impacta também o trabalho das Defensorias. As circunstâncias levaram a instituição a atuar em novas demandas (como por vagas em leitos de UTI[12]) e também acentuaram o aparecimento de questões diretamente relacionadas à redução de renda da população (como casos de pensão alimentícia[13]). A necessidade de medidas de isolamento social impactou principalmente a renda e a saúde (física e mental) dos mais pobres, o que, além de ser um fator de crescimento de demandas, também é fator de aumento da população que se enquadra nos critérios de vulnerabilidade social para atendimento nas Defensorias.

Fora os impactos na carga de trabalho da instituição, a pandemia ainda forçou mudanças repentinas sobre o modelo de atendimento e trabalho interno da Defensoria Pública. O atendimento direto aos usuários sempre fora majoritariamente presencial, assim como os trabalhos dos defensores e demais integrantes dos órgãos, os quais se desenvolviam dentro das próprias unidades. Frente à necessidade de manter o máximo de isolamento social, as Defensorias tiveram que explorar novas formas de receber demandas e novas formas de dar seguimento aos seus trabalhos diários remotamente. Com isso, a utilização de serviços em nuvem e ferramentas de comunicação privadas tornaram-se necessárias à manutenção das atividades das Defensorias, de modo que práticas como o compartilhamento

12 Ver: https://www.defensoria.to.def.br/list_tag/UTI e http://www.defensoriapublica.go.gov.br/depego/index.phpoption=com_content&view=article&id=2305:dpe-go-cobra-informacoes-sobre-vagas-de-uti-e-enfermaria-para-tratamento-da-covid-19-em-goias&catid=8&Itemid=180.

13 Ver: http://www.defensoria.rs.def.br/mais-de-200-mil-atendimentos-e-aumento-nos-pedidos-de-pensao-como-foram-esses-100-dias-de-pandemia-na-defensoria-publica

de documentos entre usuários e defensores via aplicativos transformaram-se em rotina de trabalho.

Houve, portanto, a imposição de uma intensa e repentina aceleração do processo de digitalização no dia a dia das Defensorias, um desafio sem precedentes. Nesse contexto, uma das questões mais latentes foi a de como criar mecanismos de atendimento e recebimento de demandas de populações que sofrem com a exclusão digital. Em resposta, uma das saídas encontradas foi a colaboração com instituições e coletivos que se disponibilizaram a intermediar o contato entre a Defensoria e comunidades[14]. Outra foi a garantia de meios para que aqueles com conexão à Internet pudessem contatar as Defensorias remotamente, como a disponibilização de números de *Whatsapp* institucionais ou *chatbots*. Vale lembrar que, no Brasil, a maioria das pessoas de Classe C e D acessam a Internet somente por meio de redes móveis e com planos com baixas franquias de dados (os planos "*zero rating*", com Whatsapp que pode ser usado mesmo sem pacote de dados).

As medidas foram tomadas em caráter de urgência, dada a necessidade de continuar a prestação de serviços essenciais. Nesse sentido, é esperado que nem sempre a preocupação com a privacidade e a proteção dos dados dos usuários e integrantes da instituição tenha ficado em primeiro plano na sua implementação. Ainda assim, as Defensorias se mostram preocupadas em relação a essa problemática e buscam soluções para garantir tais direitos dentro do novo modelo de trabalho remoto, entendendo que as atividades de tratamento de dados pessoais que desempenham envolvem aspectos sensíveis da vida das pessoas.

Em muitos casos, não será possível evitar por completo o uso das ferramentas mais populares do mercado, mesmo quando não sejam consideradas as mais adequadas. Entretanto, isso não significa que não existam medidas a serem tomadas para mitigar possíveis riscos relacionados ao uso dessas ferramentas. Nesse sentido, mais do que nunca, devemos nos preocupar com o armazenamento excessivo de informações em servidores na nuvem, com o compartilhamento de informações e de senhas e, ainda, manter em vista que, sempre que possível, deve-se dar preferência a canais e instrumentos de comunicação institucionais.

14 Informação obtida nas entrevistas semiestruturadas realizadas durante o projeto.

WhatsApp como ferramenta de trabalho

O *Whatsapp* é o aplicativo de mensageria mais popular no Brasil. A ferramenta é "gratuita"[15] e ainda conta com a vantagem de ser oferecida com oferta de banda ilimitada em alguns pacotes de Internet. Por sua ampla difusão e acessibilidade, é compreensível que o aplicativo tenha se tornado um meio de comunicação comum entre a Defensoria e seus usuários. As circunstâncias, sem dúvidas, dificultam a sugestão de abandono da plataforma e sua substituição por um canal institucional. Assim, as ponderações a seguir se dão não com o objetivo de rechaçar o uso do aplicativo como ferramenta de trabalho, mas de promover esse uso de forma mais responsável:

Compartilhamento de dados

- O aplicativo faz parte do grupo *Facebook*, de modo que os metadados de seu uso são compartilhados com a gigante de tecnologia. Isso não significa que o conteúdo das conversas é compartilhado, mas sim dados como "hora que usuário ficou online", "contatos que o usuário teve conversas ou realizou ligações", "tempo de uso", "IP do aparelho celular", "número do telefone", etc.

- Chamamos a atenção de que metadados não são informações insignificantes e podem revelar aspectos íntimos e sensíveis da vida dos indivíduos. Por exemplo, o contínuo contato do usuário com a Defensoria Pública revela um *proxy* da situação de vulnerabilidade daquele indivíduo. Isso não implica que haverá uso abusivo dos dados, entretanto, é importante termos em mente o fluxo informacional intrínseco a uma "mera" conversa.

Aplicação de golpes

- Outro ponto de destaque é a recente onda de golpes promovidos por meio da plataforma. Principalmente após os eventos de grandes vazamentos de dados, o Brasil vive um aumento de clonagens do aplicativo, em que os invasores buscam se passar pelo indivíduo clonado, geralmente a fim de solicitar transferências bancárias.

- Importante mantermos cuidado quanto às informações trocadas com o usuário e quanto à segurança do próprio *WhatsApp* utilizado pela Defensoria. A relação entre usuário e defensor é marcada pela confiança, de modo que qualquer tipo de golpe aplicado em nome da instituição ou a partir de informações de uma conversa com o ente tem o potencial devastador de resultar em aproveitamento indevido da situação de vulnerabilidade de um indivíduo. Uma medida cabível a ser tomada nesse sentido é garantir que sempre que um documento seja encaminhado, o responsável cuide do seu armazenamento em local seguro e o exclua do aplicativo.

e. Percepções e perspectivas

Os impactos da LGPD sobre entes do poder público merecem uma atenção própria. Não se pode ignorar as razões pelas quais há uma seção específica da LGPD que disciplina a matéria para estes agentes. Observar tais prerrogativas não deve ser uma tarefa encarada como um fim em si mesmo, pois as determinações da norma objetivam a tutela de um bem jurídico e social. Nesse sentido, o Estado, que tem a função de garantidor de uma série de serviços considerados essenciais, deve servir de exemplo quanto à proteção de dados pessoais dos cidadãos, considerando que todos estão, em certa medida, obrigados a confiar parte de sua

personalidade ao poder público.

No tocante às Defensorias, a questão é ainda mais sensível. Um sistema de Justiça que se pretenda justo deve garantir que todos os cidadãos tenham condições mínimas para defender seus direitos. Assim, a atribuição legal da Defensoria é de natureza essencialíssima. Além disso, a população atendida pelas Defensorias é, por atribuição constitucional, uma população em situação de vulnerabilidade, o que implica que estes indivíduos não têm à sua disposição um grande número de opções a que possam recorrer, o que deve ser uma razão a mais para a máxima diligência e construção de um programa de governança de excelência, de forma a não reduzir aqueles que dependem da atuação do Estado a cidadãos de segunda categoria. Nesse sentido, é que, principalmente em relação ao poder público, o desafio de conformação à LGPD é considerável. Porém, mais do que um dever legal, esse processo também pode ser encarado como uma janela de oportunidade para que, por meio da organização e sistematização de seu fluxo informacional, as funções desempenhadas pelas instituições estatais passem a ocorrer de modo ainda mais eficiente e com ainda mais qualidade.

Em síntese, pela experiência construída ao longo de 2020, podemos afirmar que um primeiro passo para a construção de um programa de adequação à Lei Geral de Proteção de Dados Pessoais dentro das Defensorias Públicas depende (i) do efetivo interesse da instituição em aprofundar o assunto (vontade política de seus dirigentes), (ii) de um grau mínimo de nivelamento sobre o que é a LGPD e no que consistem suas normas e (iii) da intenção de constituição de um grupo interdisciplinar para levar a cabo a tarefa de construção de um programa inicial de adaptação à lei. Estes pontos serão abordados com maior profundidade na parte III deste documento.

Parte 2

LEI GERAL DE PROTEÇÃO DE DADOS: ORIGEM E ESTRUTURA

Por que há uma Lei Geral de Proteção de Dados no Brasil?

Leis de dados pessoais existem há mais de cinquenta anos, apesar de serem novidade no Brasil. Elas possuem como função básica assegurar um conjunto de direitos às pessoas com relação ao modo como o tratamento de seus dados pessoais é realizado. São legislações inspiradas nas ideias de dignidade da pessoa humana, liberdade e respeito à privacidade. Além disso, são normas que buscam inverter a lógica tradicional do "segredo" ou da "liberdade negativa". A preocupação maior das leis de proteção de dados é assegurar uma liberdade positiva para que o cidadão possa ter autonomia e controle sobre como seus dados circulam (para quem, por que e para qual fim)[16].

Essa tutela de valores como liberdade, dignidade e autonomia dos titulares é um dos pilares de sustentação das leis de proteção de dados, que também se fundamentam em valores como desenvolvimento econômico e inovação, cumprindo uma dupla função. O intuito da proteção de dados é o de balancear esses dois interesses legítimos, uma vez que o tratamento de dados é de fato necessário não só para o desenvolvimento das atividades de muitas empresas, como para a própria prestação de uma série de serviços públicos. Tomando o próprio trabalho das Defensorias como exemplo, o tratamento de dados de seus usuários é requisito, em muito sentidos, para a prestação do atendimento, sendo necessário para realizar o processo de triagem socioeconômica, para cadastrar indivíduos a fim de contatá-los e até mesmo para coletar documentações exigidas pelo Judiciário. Contrapondo os dois pilares da matéria, a imprescindibilidade do tratamento de dados não exime o controlador de respeitar suas finalidades, ser transparente, garantir a segurança e a qualidade das informações armazenadas. No caso das Defensorias, mais que uma adequabilidade às previsões legais, essa postura é também relevante para consolidação de uma relação de confiança entre o ente e

16 DONEDA. Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

seus usuários.

No Brasil, diversas normas buscaram regular o fluxo de dados e assegurar alguns direitos básicos para as pessoas. Foi o caso do Habeas Data na Constituição Federal, do art. 43 do Código de Defesa do Consumidor[17], do capítulo sobre Direitos da Personalidade no Código Civil, da Lei do Cadastro Positivo de 2011 e do capítulo sobre direitos básicos dos usuários da Internet no Marco Civil da Internet. No entanto, faltava um regramento mais geral que pudesse detalhar funções dos agentes de tratamento de dados, princípios gerais para tratamento, obrigações prévias ao uso econômico dos dados, direitos básicos dos titulares e critérios de responsabilização em caso de condutas abusivas e lesões de direito[18].

As discussões em torno da elaboração de uma Lei Geral de Proteção de Dados Pessoais se iniciaram em dezembro de 2010, a partir do primeiro texto de Anteprojeto submetido a consulta pública pelo Ministério da Justiça. A questão desenvolveu-se em dois Projetos de Lei que tramitaram paralelamente na Câmara e no Senado, o PL 4060/2012 e o PLS 330/2013, mas que permaneceram em aberto por alguns anos. Apenas em 2015, com a realização de uma nova consulta pública, a qual contou com mais de 2.500 contribuições dos mais diversos atores nacionais e internacionais, que o debate retornou com fôlego, após aprovação do Marco Civil da Internet[19]. Porém, somente após mais dois anos de amadurecimento do texto, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados pessoais foi sancionada. Este, contudo, não era o fim da jornada. Depois de atrasos e ameaças ao início da vigência, o texto passou a valer apenas a partir de setembro de 2020[20].

Os anos que transcorreram desde o início do processo refletem um novo paradigma, aquele em que a sociedade e a economia são cada vez mais dependentes de dados pessoais. Hoje, tanto setor público quanto privado pautam enorme parte de suas atividades cotidianas em dados, seja para traçar estratégias de atu-

17 MENDES. Laura S. Transparência e Privacidade: Violação e Proteção da Informação Pessoal na Sociedade de Consumo.Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>.

18 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Forense, 2020

19 RIELLI, Mariana. O processo de construção e aprovação da Lei Geral de Dados Pessoais: bases legais para tratamento de dados em um debate multissetorial. Revista do Advogado, a. XXXIX, n. 144.

20 Após uma série de disputas sobre um novo adiamento da vigência da LGPD, o Congresso Nacional decidiu, em agosto de 2020, que a lei passaria a viger em partes ainda no mesmo ano. Assim, trechos referentes à materialidade da norma começaram a vigorar em setembro de 2020, entretanto, os artigos de aplicações sancionatórias ao seu descumprimento, bem como também a fiscalização por parte da Autoridade Nacional de Proteção de Dados, passariam a valer apenas em 2021.

ação interna, seja para autenticar usuários de um sistema ou para compreender e responder às demandas sociais e de mercado. Estamos diante de um estágio organizacional com muitos benefícios em termos de eficiência e qualidade dos serviços prestados (públicos e privados), situação que não deverá se reverter a um momento anterior. Portanto, coexistindo a necessidade de tutela sobre os dados e o papel central que estes desempenham dentro da organização socioeconômica atual, surge a busca por um arcabouço normativo que dê segurança ao sistema e que equilibre os dois lados dessa balança: que dê legitimidade ao tratamento de dados, permitindo sua realização e que crie balizas a este tratamento, garantindo a autodeterminação informativa dos indivíduos.

Desse modo, percebe-se que a LGPD não surge para barrar ou evitar atividades de tratamento de dados pessoais. Pelo contrário: seu intuito é o de garantir sua continuidade e legitimidade, a partir de uma série de princípios e regras. A Lei Geral brasileira teve ainda o grande mérito de ter sido construída de forma coletiva, com a participação de inúmeros atores, o que fortalece seu caráter democrático e sua dupla finalidade.

Atualmente, são centenas de países que contam com normas gerais de proteção de dados pessoais. Na América Latina, países como Argentina, Chile, Colômbia e Uruguai contam com leis semelhantes há anos. O Brasil adotou tardiamente a sua própria LGPD, com a vantagem de poder assimilar reformas legislativas importantes no mundo, como a General Data Protection Regulation (GDPR) na União Europeia e reformas recentes no contexto sul-americano.

O que há na Lei Geral de Proteção de Dados?

A LGPD possui uma anatomia própria. A Lei possui dez capítulos que se desdobram em 65 artigos. Longe de exaurir completamente sua explicação, detalha-se a seguir sua "estrutura óssea" principal.

O primeiro capítulo dedica-se às disposições preliminares. Aqui afirma-se que a Lei tem como objetivo "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". São apresentados os fundamentos da legislação, os critérios da aplicação territorial e material da Lei, as hipóteses de não aplicação da norma (e.g. atividade exclusiva jornalística

ou tratamento de dados para fins exclusivamente particulares e não econômicos), as definições e os princípios. Essa parte é extremamente importante, em especial a apresentação dos conceitos jurídicos do art. 5º (aqui há, dentre outras definições, a diferença entre controlador e operador, a diferença entre dados pessoais e dados pessoais sensíveis, a distinção entre anonimização e pseudoanonimização, a noção de encarregado) e dos princípios de tratamento no art. 6º, que consistem no verdadeiro coração da Lei. Aqui encontram-se os parâmetros de finalidade, adequação, segurança, qualidade, livre acesso, prevenção, não discriminação e outros, cuja leitura é fundamental para uma compreensão mínima da LGPD.

A segunda parte da Lei dedica-se ao tratamento de dados pessoais. Aqui, a norma se ocupa de quatro tópicos. Primeiro, os requisitos para o tratamento de dados. Nesse ponto, a LGPD apresenta as "bases legais para tratamento de dados" (as pré-condições jurídicas que precisam ser cumpridas para que o controlador possa tratar os dados de forma lícita), as características específicas do consentimento, as regras básicas sobre o Aviso de Privacidade e as características do legítimo interesse. O segundo tópico é o tratamento de dados sensíveis. Aqui, há um cuidado especial com as condições em que dados de saúde, de raça ou de orientação política, dentre outros, devem ser tratados. A Lei impõe limites à exploração econômica de dados de saúde e estipula condições para que a anonimização ocorra, prevendo a possibilidade de reconsiderar tais dados como dados pessoais. O terceiro tópico é o tratamento de dados de crianças e adolescentes, que possui regras próprias, com possibilidade de controle parental e atendimento ao melhor interesse da criança. Por fim, a Lei estipula parâmetros para o término do tratamento de dados, incluindo as condições em que o controlador pode reter os dados.

A terceira parte da Lei volta-se aos direitos do titular. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. A Lei aprofunda os direitos básicos (e.g. confirmação, acesso, correção, oposição, anonimização, portabilidade, revogação do consentimento, entre outros previstos no art. 18), prevê regras para o direito de revisão de decisão automatizada e estipula que a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente.

A quarta parte dedica-se ao tratamento de dados pelo poder público. Aqui, são estipuladas regras específicas sobre contratação de entes privados e compartilhamento de dados, aplicação para empresas públicas, critérios de interoperabi-

lidade, parâmetros de uso compartilhado de dados e poderes específicos para a Autoridade Nacional de Proteção de Dados, que tem o dever de fiscalizar também o poder público.

A quinta parte da Lei volta-se à transferência internacional de dados. A Lei estipula as hipóteses em que a transferência pode ocorrer de forma lícita, os critérios para que seja reconhecido o nível de proteção de dados de país estrangeiro, e poderes da Autoridade Nacional de Proteção de Dados na definição do conteúdo de cláusulas-padrão contratuais, verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta.

O sexto capítulo dedica-se aos agentes de tratamento de dados, com ênfase nas noções de controlador e operador, e regras específicas sobre o encarregado, que deve ser a figura de referência para os titulares dos dados, bem como o ponto de contato para comunicações com a Autoridade Nacional de Proteção de Dados. A Lei também apresenta o regime de responsabilidade civil dos agentes, as excludentes de responsabilidade e regras específicas sobre expectativas em torno da segurança da informação.

O sétimo capítulo se volta à segurança e boas práticas. Nele, a Lei determina o dever dos agentes de tratamento de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, assim como a adotar regras de boas práticas e de governança que garantam a adequabilidade do tratamento. O capítulo fornece diretivas gerais acerca dos procedimentos a serem adotados e deixa a cargo da Autoridade Nacional de Proteção de Dados estabelecer padrões mínimos a serem cumpridos pelos agentes.

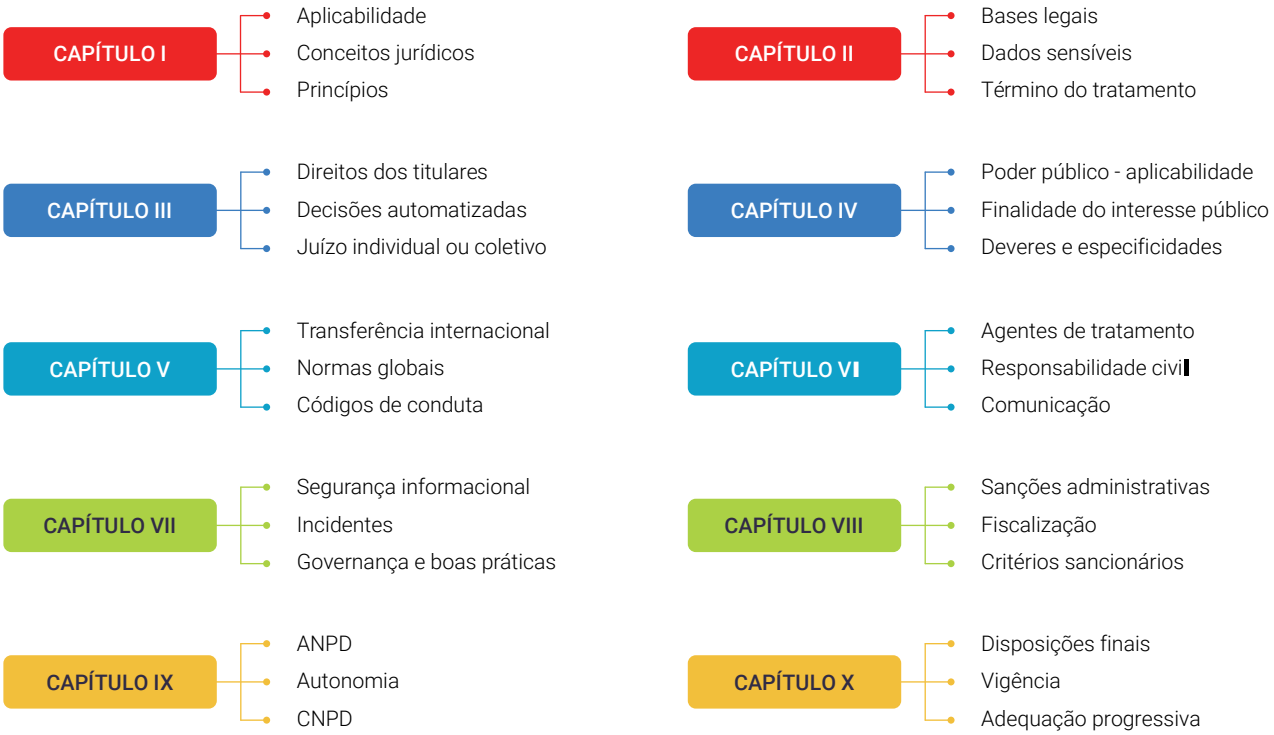
O capítulo oito, sobre fiscalização, abarca disposições sobre as sanções administrativas aplicáveis pela Autoridade no caso de descumprimento da Lei. Além de prever os diferentes tipos de penalidades, que variam entre advertências, multas até o valor de 50 milhões de reais e a proibição das atividades de tratamento, também dispõe a respeito dos padrões de balizamento para a aplicação das sanções. A atenção a tais critérios demonstra que a LGPD leva em consideração o comportamento dos agentes de tratamento ao longo do tratamento e que a demonstração de um dever de cuidado contínuo é fator considerado na dosimetria das sanções.

No capítulo nove, sobre Autoridade e Conselho, se determina a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão da Administração

Pública federal, integrante da Presidência da República, e do Conselho Nacional da Privacidade e da Proteção de Dados Pessoais (CNPD). À ANPD garante-se autonomia técnica e decisória, sendo o ente responsável não só pela fiscalização e aplicação da lei, como também pela expedição de normativas e promoção de atividades que incentivem a cultura da proteção de dados pessoais. Ainda que, a priori, seja parte da Administração Direta, espera-se que a Autoridade venha a ganhar o status autárquico que lhe garantiria a completude de sua autonomia e independência. Em relação ao CNPD, ente composto por representante de diferentes setores (governamentais, laborais, empresariais e da sociedade civil), cabe a propositura de diretrizes estratégicas a serem tomadas pela Autoridade, a elaboração de relatórios de avaliação da execução da Política Nacional de Proteção de Dados Pessoais e da Privacidade e, também, a realização de estudos e audiências públicas sobre o tema da proteção de dados.

O Capítulo dez, sobre disposições finais e transitórias, apresenta questão importante referente ao início fatiado da vigência da Lei. Como antes comentado, existiram alguns percalços até a determinação do início da vigência da Lei, assim, conforme sucessivas alterações em seu art. 68, passaram a valer a ampla maioria de seus artigos em setembro de 2020. Contudo, as disposições referentes às sanções passarão a viger apenas em agosto de 2021.

LGPD em capítulos



O cumprimento da Lei Geral de Proteção de Dados é tarefa complexa, pois envolve mudanças organizacionais, logísticas e de fluxos internos. Ao mesmo tempo, trata-se de uma oportunidade de mudanças e inovação para as Defensorias Públicas. Dito isso, destacamos a seguir as vantagens de se iniciar um programa de conformidade à LGPD.

Agenda Regulatória da Autoridade Nacional de Proteção de Dados

Atenção à ANPD nos próximos anos! A LGPD indica em diferentes momentos que a regulamentação de determinados aspectos da legislação ficará a cargo da Autoridade Nacional de Proteção de Dados. Em janeiro de 2021, a Autoridade publicou sua agenda regulatória

para o próximo biênio, documento importante para guiar nossos olhares aos tópicos de maior interesse às Defensorias. A ANPD é — e será — um importante ponto de apoio para aqueles que estão conduzindo programas de adequação à LGPD. É crucial acompanhar seu trabalho e, em especial, as consultas públicas e tomadas de subsídios lançadas.

Agenda Regulatória da ANPD para o próximo biênio

2021 — FASE 1
Publicação do primeiro Regimento interno da ANPD

2021 — FASE 1
Planajemanento Estratégico da ANPD

2021 — FASE 1
Proteção de dados e da privacidade para pequenas e médias empresas, startups e pessoas físicas que tratam dados pessoais com fins econômicos.

2021 — FASE 1
Estabelecimento de normativos para aplicação do art. 52 e seguintes da LGPD

2021 — FASE 1
Comunicação de incidentes e espécificação do prazo de notificação

2021 — FASE 1
Relatório de impacto à Proteção de Dados Pessoais

2022 1º sem — FASE 2
Encarregado de proteção de dados pessoais

2022 1º sem — FASE 2
Transferência internaiconal de dados pessoais

2022 2º sem — FASE 3
Direitos dos titulares de dados pessoais

2022 2º sem — FASE 3
Hipóteses legais de tratamento de dados pessoais

Parte 3
DESMISTIFICANDO O PROCESSO DE ADEQUAÇÃO À LGPD

Vantagens de um programa de conformidade

a. Inovação

Se, ao contrário de criar barreiras ao uso dos dados, a Lei objetiva dar-lhe legitimidade, o que de fato a LGPD impõe é um dever de justificação do tratamento, além do comprometimento dos agentes de tratamento em garantir os direitos dos titulares e atender aos princípios da proteção de dados. Ainda que os deveres dos agentes de tratamento e as garantias do titular representem, em certa medida, um ônus, o trabalho de atendê-los pode ser encarado como algo além de um desafio burocrático, mas como uma janela de oportunidades da perspectiva administrativa e organizacional daquele que realiza o tratamento de dados.

Do ponto de vista administrativo, a adequação "força" um processo de inovação institucional, de revisão de procedimentos e métodos, o que traz benefícios em diferentes aspectos. Não se trata somente da inclusão de ferramentas digitais, mas da organização do órgão, o que envolve atividades internas e externas e exige que os agentes analisem o que se realiza com os dados e possam avaliar se a maneira como tem operado até então é a mais eficiente, abrindo portas para a estipulação de novas estratégias de uso de dados. Essa visão mais clara do agente sobre as informações que constam em seu próprio banco pode, além de tudo, trazer indicativos úteis para questões de planejamento, a partir, por exemplo, da identificação de demandas e estatísticas de produtividade, que poderiam pautar metas anuais e a distribuições de tarefas de um modo fundamentado em informações concretas, e não apenas em impressões pessoais.

Além da eficiência operacional, a adequação permite insights a partir do diálogo entre áreas e profissionais com diferentes visões disciplinares. É possível, então, enxergar novas formas de usos de dados e inovar.

O processo de mapeamento de dados, que geralmente é uma das primeiras etapas no processo de conformidade à LGPD, é uma oportunidade para a compreensão da riqueza dos dados que uma Defensoria possui sob sua custódia, permitindo uma reflexão sobre automações, utilização das informações de forma lícita e inovação na prestação dos serviços.

b. Planejamento estratégico e eficiência

Essa reestruturação está relacionada aos princípios da Administração Pública e do serviço público, como o da eficiência e da qualidade. Logo de pronto, um projeto de adequação à LGPD demanda que a instituição elimine informações excessivas de seu sistema (art. 6o, II e III), o que abre espaço para aquilo que é de fato relevante. Além disso, o cumprimento da Lei demanda a atualização das informações, atendendo ao princípio da qualidade dos dados (art. 6o, V), o que "limpa" o sistema de conteúdos que podem prejudicar o desempenho das atividades de uma Defensoria.

Para além das questões mais diretas de organização dos sistemas, o processo abre também oportunidades de melhor capacidade de gestão. Como antes levantado, ter uma visão clara e fidedigna do trabalho desempenhado permite uma administração mais consciente, capaz de relacionar fins almejados aos meios necessários para alcançá-los.

Em termos de planejamento estratégico, a visão ampla que pode ser proporcionada por dados quantitativos e qualitativos de diferentes aspectos do trabalho realizado pelas Defensorias é de grande valia, principalmente em relação à compreensão de prioridades. Nesse sentido, instituídas a missão, a visão e os valores do ente, os dados são valiosos em especial para os objetivos e para o mapeamento estratégico, etapas que relacionam diretrizes ao mote da instituição. O que se espera é que esse banco de dados organizado seja capaz de fornecer informações sobre as principais forças e fraquezas dos trabalhos então desenvolvidos e do que a própria Defensoria compreende como mais valioso.

Dentro desta perspectiva, um sistema integrado e padronizado de trabalho, além de facilitar a implementação de uma política de governança de dados, pode ser bastante útil, ao servir como fonte de informações para que a Defensoria compreenda melhor sua própria atuação. Chamamos aqui de sistema integrado um ambiente digital que reúna e promova a interoperabilidade das atividades de diferentes instâncias da Defensoria, podendo contemplar um maior ou menor número de processos, em mais ou menos setores. Um exemplo básico seria um sistema que armazena os dados de atendimento, concentrando as informações de cadastramento dos usuários, andamentos processuais, eventuais acordos, peças, tipos de demanda, solução do caso, etc. Se armazenadas de modo padronizado e contínuo, esse tipo de informação poderia dar origem a análises valiosas sobre quantidade de sobrecarga de órgãos, demandas mais recorrentes, correlações

entre tipos de demanda e perfil de atendidos, demora para a resolução de casos e avaliação das soluções mais eficientes. Este seria um sistema pensado apenas para um único micro processo, considerado para o atendimento de balcão, mas que poderia incluir também espaços com layout próprio para núcleos especializados e que poderia ser interoperável com sistemas de gestão de pessoal, entre outros.

Ainda, as possibilidades de uso dessas informações não se esgotam em um nível de planejamento estratégico, mas são ferramentas importantes também para iniciativas a serem tomadas em nível tático, isto é, relacionadas a objetivos específicos no curto prazo. Assim como uma visão do todo ajuda a administração a perceber as principais prioridades da Defensoria, o mesmo vale para os coordenadores, que podem também criar um planejamento de atuação mais bem embasado na realidade prática. Mais que isso, permite um melhor alinhamento entre os dois níveis, pois compartilham de uma mesma fonte capaz de oferecer imagens sobre o todo e sobre as partes.

c. Reputação e alinhamento junto ao sistema de Justiça

As Defensorias devem considerar questões de cunho reputacional, pois estar em conformidade com a Lei, mais do que obrigação legal, é sinal de uma política de governança consistente. O próprio Conselho Nacional de Justiça (CNJ) publicou a Recomendação n. 73/2020, com orientações para a adequação dos órgãos do Poder Judiciário à Lei Geral de Proteção de Dados. O documento traz uma série de orientações sobre os procedimentos a serem executados pelos entes do sistema de Justiça para o cumprimento da LGPD. Dentre as indicações, há ênfase na criação de grupos de trabalho para a formulação de estudos de medidas necessárias à implementação da LGPD, estruturação de planos de ação, além da publicização de registros relativos ao tratamento de dados pessoais dos usuários, contendo informações sobre a finalidade do tratamento, base legal, categorias de dados, prazo de conservação, medidas de segurança adotadas e a política de segurança da informação.

Assim, a implementação de um programa de governança de dados que adeque as Defensorias não se trata de mera questão de conformidade à Lei, mas de conformidade da instituição ao que se espera dela e de seus pares no sistema de Justiça. Evidentemente, diferente do que ocorre no setor privado, um abalo reputacional não interferirá nos rendimentos desses entes ou afetará seu valor de

mercado, mas, pior que isso, interferirá ou na credibilidade do ente e do sistema público, ou na credibilidade do diploma legal.

d. Relação de confiança

Vinculadas à reputação, encontram-se também questões relativas à ética e à relação de confiança estabelecida entre as Defensorias e seus usuários. A instituição é a guardiã de uma série de informações sensíveis, fato que se deduz da própria natureza de seu trabalho, que abarca a defesa de direitos e o atendimento de demandas jurídicas e sociais daqueles em situação de vulnerabilidade. Não se trata somente de uma questão qualitativa dos dados, mas também quantitativa, considerando o número massivo de atendimentos realizados pelos órgãos diariamente. Colocando em perspectiva, somente no estado de São Paulo, realizam-se cerca de 1,5 milhões de atendimento por ano, considerando ainda que no processo de atendimento, muitas vezes é necessário coletar não só dados referentes àqueles que efetivamente procuram os serviços da Defensoria, mas também de seus familiares ou terceiros envolvidos em uma demanda.

Existe assim, para além de tudo, um compromisso e um dever ético com os usuários do sistema da Defensoria. Aqueles que são atendidos encontram-se em alguma situação de vulnerabilidade e, na maioria das vezes, não teriam a escolha de procurar um serviço alternativo. O Brasil tem o grande mérito de fornecer em seu sistema de Justiça o amparo gratuito de assistência jurídica de alta qualidade. Ainda assim, é necessário que tal serviço seja prestado com respeito aos direitos dos usuários, inclusive os direitos relativos à proteção de dados, os quais não podem ser tratados como artigos de luxo e privilégios daqueles que possuem condições econômicas mais privilegiadas.

Devemos ter em mente que o serviço prestado pelas Defensorias Públicas, assim como qualquer outro serviço público, envolve um dever de cautela especial sobre os dados de seus usuários. Durante a execução das entrevistas do projeto, a fala de um dos membros das Defensorias foi muito marcante nesse sentido. O servidor destacou sua percepção de como os cidadãos chegavam até o órgão ansiosos e aflitos para resolverem seus problemas perante a Justiça, o que criava uma relação de incontestabilidade ao que lhe fosse requisitado ou ao trabalho realizado

pela instituição[21]. Os usuários confiam seus dados, que representam também parte de sua personalidade, sem questionar a respeito: seja porque confiam no ente, seja porque ainda não percebem a importância e o valor daquela informação. Independente do motivo, essa dinâmica , ao contrário de afastar a responsabilidade das Defensorias, apenas a reforça, sendo esta instituição defensora e garante da justiça e dos interesses e direitos de seus usuários.

Sistemas integrados

Muitas Defensorias utilizam sistemas integrados de acesso, armazenamento documental e cadastramento de casos. Essas ferramentas são de grande importância em termos organizacionais e de padronização do trabalho, e além disso, podem ser ainda utilizadas como fontes poderosas na geração de inteligência para a instituição.

Apesar de na maioria das vezes o acesso ao sistema ser restrito àqueles que possuem um login, alguns pontos merecem destaque para garantir a segurança e o tratamento adequado das informações:

Restrições de acesso: uma das formas de mitigar riscos de uso indevido das informações constantes no sistema das Defensorias é restringir o acesso a determinados conteúdos e funcionalidades com base na atribuição ou cargo exercido pelo detentor do login.

Não compartilhamento de senhas: evitar o compartilhamento de senhas é medida importante para garantir a segurança e uso devido das informações, principalmente tendo em vista a rotatividade de determinados agentes dentro da instituição.

Casos em sigilo: é interessante que exista a possibilidade de tornar sigilosas as informações relativas a determinados casos. A avaliação

21 Conselho Nacional do Ministério Público. Relatório da Pesquisa de Satisfação e Imagem do CNMP e do Ministério Público. Jul. 2017. Disponível em: <https://www.cnmp.mp.br/portal/images/Apresenta%C3%A7%C3%A3o_da_pesquisa_CNMP_V7.pdf>.

de circunstâncias em que é cabível o sigilo pode ficar sob o controle interno da Corregedoria a pedido do defensor responsável.

Padronização: para que o sistema possa servir como ferramenta de geração de inteligência é importante que exista um compromisso amplo de registro dos atendimentos e também uma uniformidade no preenchimento dos cadastros. Ressalta-se que as informações ali constantes têm enorme potencial de guiar a atuação do ente, mas, para isso, é necessário que os dados sejam confiáveis e fidedignos e representem a realidade dos atendimentos.

e. Papel educacional

Uma visão ampla do papel das Defensorias como instituição que vai além da defesa judicial de pessoas em situação de vulnerabilidade reforça sua atuação na educação em direitos, o que dialoga também com a tutela da proteção de dados. A Defensoria Pública de São Paulo foi a primeira neste projeto a iniciar seu programa de adequação à LGPD; um dos aspectos destacados pelo órgão em uma de suas primeiras reuniões acerca de políticas de transparência de dados foi justamente a da promoção educacional. Um dos pontos destacados pelos participantes foi o potencial que a transparência da Defensoria sobre o tratamento de dados e direitos dos titulares poderia ter sobre a educação dos usuários acerca de seus direitos, incidindo não somente em sua relação com a própria Defensoria, mas com outras instituições que nem sempre possuem o mesmo compromisso.

Isso traria impactos positivos principalmente tendo em vista que o público de atendidos pelas Defensorias é aquele que também é a maior vítima do uso abusivo de dados pessoais. Na medida em que se atende predominantemente àqueles em situação de vulnerabilidade econômica, há a sobreposição com o público que mais sofre os assédios de empresas que ofertam serviços "*freemium*", em que o acesso ao produto ou serviço é condicionado à concessão de dados pessoais. Esse modelo de negócios coleta, muitas vezes, quantidades desproporcionais e desnecessárias de dados, a fim de realizar inferências comportamentais preditivas, que poderão ser usadas em prejuízo do titular, sem que esse tenha

qualquer conhecimento do ocorrido. Os exemplos mais clássicos desse tipo de uso são as técnicas de análise de risco de crédito, as quais, com base no uso de ferramentais estatísticos, alimentados por dados dos mais variados, servem para determinar valores de juros, e acabam por muitas vezes identificar e replicar os padrões discriminatórios de uma sociedade.

Duas mentalidades de processo de conformidade à LGPD[22]	
Obrigação legal	**Oportunidade**
Manutenção e revisão dos processos existentes	Melhoramento dos processos existentes, automatização e criação de novos usos para fins de política pública
Análise estanque centrada no diagnóstico de riscos	Análise dinâmica centrada em que a instituição pode se aprimorar
Gestão baseada em mitigação de risco	Gestão baseada na inovação
Reputação com base no medo de sanções	Reputação com base em dar mais transparência ao uso dos dados
Desincentivo à inovação no uso dos dados, riscos reputacionais, ampliação da burocracia	Formas inovadoras de utilização dos dados, educação em direitos através de exemplos sobre o devido tratamento de dados, automatização de processos e redução da burocracia

Compreendendo o papel dos dados nas Defensorias

Compreendendo que as Defensorias terão que pensar na proteção de dados tanto no que tange a suas atividades meio - administrativas e diárias de manutenção de seu sistema de atendimento e trabalho - quanto da perspectiva da sua atividade fim - a assistência na resolução de litígios, promoção de políticas públicas e da justiça em um sentido amplo -, destacamos em seguida alguns pontos de reflexão sobre cada um desses aspectos.

22 Tabela adaptada de: BIONI, Bruno Ricardo. Inovar pela lei. GV EXECUTIVO, v. 18, n. 4, p. 30-33, 2019.

a. Atividade-meio

Gestão de recursos (SI & TI)

As áreas de Segurança da Informação e Tecnologia da Informação são chaves importantes de um projeto de adequação. Antes de tudo, é necessário que exista a percepção de que as áreas de TI e SI possuem um potencial estratégico que transborda sua tarefa de garantir o funcionamento da estrutura informática de uma Defensoria. Pensar nos dados abre margem para que as atividades desses profissionais sejam utilizadas da melhor forma possível para impactar de forma mais direta o trabalho dos órgãos. A participação desses profissionais poderia ser mais ativa em relação aos dados se pensarmos em formas inteligentes de integração dos sistemas e na criação de padrões de consolidação de informações, o que evitaria retrabalho e permitiria a concentração de conhecimentos.

A questão da padronização e da organização foi inúmeras vezes destacada durante as entrevistas realizadas neste projeto. Um dos exemplos ilustrativos desse ponto foi o de situações em que o usuário se dirige até a Defensoria e relata seu caso, mas é direcionado para receber o atendimento em um outro dia. Ocorre que as informações referentes a sua primeira passagem pelo órgão não são armazenadas em um local específico, de modo que, ao retornar, é exigido ao usuário que este apresente informações que já havia fornecido em momento anterior. Em uma situação como essa, o trabalho de coleta de informações sobre o caso poderia se tornar mais eficiente com a padronização do armazenamento das atividades dos órgãos em um determinado sistema, pois evitaria a realização de trabalhos repetidos. A estruturação organizacional que cumprisse tal função poderia ser realizada com a ajuda das equipes de informática.

Outro ponto de destaque que pode contar com a participação mais ativa do setor de tecnologia e informações é a acessibilidade e a autenticação nos sistemas da Defensoria. Uma das preocupações que se repetiu durante as entrevistas foi a possibilidade da Defensoria atender partes distintas de um mesmo processo, o que em determinadas circunstâncias gera receio dos defensores de inserir certas informações em sistemas integrados e abertos a outros membros da instituição. O receio, nesse caso, é de que as informações confiadas pelo usuário dos serviços da Defensorias possam ser utilizadas em seu desfavor pelo próprio ente (no caso, por outro defensor), por exemplo, em uma situação que os dados de residência de um atendimento sejam utilizados para realizar a citação do próprio usuário em

outro processo, ou dados de vínculo empregatício sejam utilizados para indicar a possível penhora de verbas.

A questão envolve dilemas éticos que precisam ser enfrentados, mas há também ferramentas técnicas que podem ser aplicadas a fim de dirimir as inseguranças relatadas. As próprias Defensorias é que responderão qual a forma mais adequada de restringir a acessibilidade das informações disponíveis em seus sistemas, mas algumas medidas são possíveis, como limitar o acesso a determinados casos ao defensor responsável, restringir o acesso a determinadas informações conforme a função do cargo exercido, identificar o acesso de defensores a casos de outros responsáveis, etc. Plataformas de unificação de serviços e recursos, pela sua natureza de acumulação de bases de dados, devem preferencialmente ser associadas à construção de perfis de acesso, respeitar o princípio de need to know e prever ampla publicização interna de suas Políticas de Segurança da Informação. Estes são exemplos de medidas que podem ser discutidas e projetadas com o envolvimento dos profissionais das áreas de TI e SI.

Por fim, cabe citar o envolvimento central que essas equipes terão sobre os aspectos de segurança das informações constantes em qualquer dos sistemas digitais sob responsabilidade das Defensorias. Nesse sentido, é interessante que os profissionais liderem a formulação de protocolos de respostas a incidentes informáticos e, também, que estejam capacitados a manejar os padrões exigidos por recomendações internacionais, como os padrões ISO. Além disso, a equipe tem potencial para colaborar com a estruturação de ferramentas e plataformas virtuais utilizadas pelas Defensorias que levem em conta princípios do *privacy by design*[23]: prevenção e proatividade, privacidade como padrão, privacidade incorporada ao design, funcionalidade ampla, segurança de ponta a ponta, transparência, respeito à privacidade do usuário.

23 CAVOUKIAN, Ann et al. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, v. 5, p. 12, 2009.

Planejamento estratégico e política para área de tecnologia da informação

Planejamento estratégico[24]: a adoção de um planejamento estratégico ou um plano diretor para a área de tecnologia da informação é uma medida interessante para fornecer direcionamentos para uma atuação alinhada e que incorpore as perspectivas e objetivos da Defensoria como um todo, inclusive questões relacionadas à governança e uso inovador dos dados. Um documento como este pode trazer elementos como:

- Missão: um alinhamento da missão específica da área com a missão da Defensoria.
- Visão: o compromisso com um projeto de futuro e a projeção em sociedade, partindo daquela que é a visão da própria Defensoria.
- Valores: ética e transparência como princípios, eficiência, credibilidade, segurança, inovação e até mesmo direcionamentos específicos sobre as ferramentas utilizadas (como uso de softwares livres).
- Alinhamento estratégico: atuação estrategicamente direcionada aos objetivos da Defensoria.
- Compromisso com a incorporação dos princípios de *privacy by design*.

Política[25]: documento que dispõe e comunica sobre as regras e boas práticas das atividades da área de tecnologia da informação, podendo também nomear responsáveis pela execução e coordenação das previsões.

24 Inspirado em: Defensoria Pública do Estado do Ceará. Plano Diretor de Tecnologia da Informação DPGE 2016-2017. Disponível em: https://www.defensoria.ce.def.br/wp-content/uploads/downloads/2016/04/PLANO-DIRETOR-DE-TECNOLOGIA-DA-INFORMACAO.pdf

25 Inspirado em: Defensoria Pública do Estado de São Paulo. Ato Normativo DPG nº 55, de 20 de outubro de 2011. Institui a Política de Uso de Recursos de Tecnologia da Informação e Comunicação – TIC e dá outras providências. Disponível em: <https://www.defensoria.sp.def.br/dpesp/Conteudos/Materia/MateriaMostra.aspx?idItem=57859&idModulo=9788>.

- Criação de uma coordenadoria responsável pelos processos de informatização e gestão de recursos tecnológicos.
- Determinação de regras e boas práticas para aquisição de recursos da área de tecnologia da informação.
- Determinação de regras e boas práticas para o uso dos recursos TIC.
- Determinação de regras e boas práticas para uso de recursos disponíveis na web.
- Determinação de parâmetros mínimos de segurança da informação, como o atendimento aos padrões ISO.
- Estabelecimento de protocolos de respostas a incidentes, incluindo medidas preventivas e mitigadoras.
- Estabelecimento de medidas concretas a serem adotadas para garantir o atendimento aos princípios do *privacy by design*.

Gestão de pessoas

Pensar na consolidação de um sistema integrado e padronizado também é oportunidade para as equipes que cuidam da gestão de pessoas nas Defensorias. Um ambiente organizado permite uma gestão interna mais eficiente ao traçar um quadro com maior fidedignidade sobre o trabalho que tem sido realizado pelos órgãos. Isso serve para, por exemplo, uma melhor alocação de funcionários, distribuição de tarefas, percepção de sobrecargas, etc, e pode ser útil também para a simplificação de algumas tarefas mecânicas como, por exemplo, automatização de férias, controle de ponto e entrada de processos administrativos, o que abre espaço para que esses profissionais tenham mais disponibilidade para cuidar das estratégias de funcionamento eficiente da instituição.

Essa percepção de oportunidades para uma melhora na gestão de pessoas foi levantada pelos próprios membros das Defensorias. Durante a fase de entrevistas, foram citados exemplos sobre como seria positiva a existência de um controle da quantidade de atendimentos e demandas realizadas pelos órgãos, para que a gestão pudesse compreender melhor a sobrecarga de determinadas regiões e a necessidade de contratação de pessoal ou alocação de colaboradores. A queixa,

nesse caso, se resume aos problemas de padronização da forma como o reporte do trabalho é realizado. Em uma mesma Defensoria, é comum que alguns órgãos ainda registrem seus atendimentos de forma física ou em sistemas não institucionais, enquanto outros já possuem acesso a um local de registro institucional, e, em ambas as situações, foi relatado que ainda é comum que o devido registro do atendimento não seja realizado. Em termos estatísticos e de recursos humanos essa falta de padronização é muito prejudicial, justamente por impedir que a gestão tenha uma visão clara do trabalho que vem sendo realizado.

Reitera-se aqui a importância que a organização e compromisso com as informações fornecidas em sistemas digitais integrados desempenham sobre os processos de tomadas de decisão de uma Defensoria. Sendo responsável pela gestão das pessoas que colaboram com o trabalho da instituição, a necessidade de confiabilidade das informações ganha contornos ainda mais evidentes para estas equipes. A disponibilidade de pessoal e recursos de um ente do setor público apresenta limitações diferenciadas se em comparação com instituições privadas, de modo que a automatização de determinados processos (como férias, pontos, relatórios de atividades, etc.) e a tomada de decisão baseada em dados confiáveis (como a alocação de servidores, a necessidade de novos defensores em determinadas áreas, etc) colaboram diretamente para um melhor aproveitamento dos recursos humanos e financeiros.

Organização informacional como ferramenta de gestão

A capacidade de obter dados confiáveis sobre o trabalho desempenhado tem o potencial de tornar uma série de processos de tomada de decisão e de gestão de pessoas mais eficientes.

Gestão de pessoas

- Automatização de controles como férias e controle de ponto.
- Checagem de sobrecarga de trabalho: percepção de que determinadas unidades, órgãos ou núcleos precisam de mais colaboradores em determinados setores.
- Contratações: necessidade de novas contratações, padrões de admissão e desligamento de estagiários, controle responsável das informações de candidatos em processo seletivo.

Tomadas de decisão

- Automatização de relatórios: uso das informações constantes em sistemas integrados para a geração automática de relatórios e outras burocracias legalmente demandadas.
- Tomadas de decisão baseadas em dados: possibilidade de perceber insuficiências, dificuldades, necessidade de recursos em determinadas áreas ou setores.
- Comprovação da necessidade de recursos: utilização dos dados sobre o trabalho desempenhado como forma de apresentar à classe política a urgência de determinadas medidas, como referentes a recursos ou à abertura de editais.

Pesquisa

Ainda sobre a perspectiva interna, a organização do sistema possibilita seu uso como fonte de dados para fins de produção de pesquisas. Quanto à gestão, a produção de pesquisas pode auxiliar da perspectiva administrativa ao extrair informações estatísticas do trabalho prestado pelos órgãos, ou mesmo buscar compreender melhor quais as demandas mais atendidas, perfis de usuário, satisfação com o atendimento, pontos de maiores fragilidades e maiores forças dentro dos órgãos.

Como será abordado com mais detalhes na seção seguinte, os dados como fonte para pesquisas são preciosos para uma atuação estratégica da Defensoria. As constatações estatísticas e qualitativas do trabalho do órgão têm múltiplas utilidades que são compatíveis com o papel mais amplo da Defensoria, o de defesa de direitos daqueles em situação de vulnerabilidade. Pesquisas fornecem fundamentos científicos que têm grande potencial para ajudar a instituição a entender o Judiciário, além de servirem como argumento de convencimento forte na defesa de uma tese ou até mesmo como base para pressionar a concretização de políticas públicas.

Pensando na delimitação de estratégias de atuação, dois exemplos levantados por membros das Defensorias entrevistados podem ser citados: um diretamente ligado a ação sobre políticas públicas e o outro sobre a incidência perante o Judiciário. O primeiro relato retrata situação que se repete durante a pandemia de COVID-19: conforme conta o(a) entrevistado(a), o governo local negava veementemente a falta de leitos de UTI na região, e a Defensoria, em ação conjunta com o Ministério Público, apontou a inverdade da declaração dos governantes, demonstrando a grande quantidade de pedidos que chegavam à Defensoria para judicialização pela falta de vagas em leito. O segundo relato baseou-se em um levantamento que verificou que determinados juízes continuamente contrariavam, em suas decisões, os entendimentos consolidados e súmulas dos tribunais superiores, dado que poderia ser forte argumento de sustentação de teses jurídicas e questionamento da atuação dos magistrados em questão.

b. Atividado-fim - litigância estratégica à litigância dadocêntrica

Para além das oportunidades que um projeto de adequação abre em relação às atividades administrativas e estruturais de uma Defensoria, há também

uma oportunidade no que toca a atividades fim da instituição. Uma melhora organizacional em termos de verificação de dados coletados, armazenados, do fluxo informacional e das finalidades dos tratamentos possibilita seu uso estratégico em demandas que chegam aos órgãos.

Para ilustrar essa possibilidade, pode-se citar a atuação da DPE-RJ, a qual, analisando seu trabalho, percebeu a existência de grande aumento das demandas relativas à falta de vagas em creches, tendo esse número mais que dobrado de um ano para outro. Isso permitiu que o órgão identificasse a viabilidade de entrar com uma ação civil pública para requerer a criação de novas vagas. A Defensoria, nesse caso, não só ganhou a ação, como também foi convidada a, no ano seguinte, participar da constituição de políticas públicas sobre o tema junto à prefeitura da cidade do Rio de Janeiro. Em uma sociedade movida e orientada por dados, é crucial que agentes como as Defensorias Públicas estejam abertos às possibilidades de uma litigância dadocêntrica, que se apoia em análises agregadas de dados pessoais como estratégia argumentativa e de convencimento de entes decisórios em casos complexos.

Outro exemplo concreto nesse sentido é o do relatório produzido também pela Defensoria Pública do Estado do Rio de Janeiro e que foi citado como fundamentação decisória pelo Superior Tribunal de Justiça, que decidiu pela absolvição de um homem então condenado[26]. No caso em questão, o indivíduo era réu de um processo de crime de assalto e sua condenação em instâncias anteriores se dera exclusivamente em razão de reconhecimento fotográfico. No relatório citado, a Defensoria apontou a existência de erro em pelo menos 58 casos de reconhecimento fotográfico, que resultaram em acusações e até em prisões equivocadas, entre junho de 2019 e março de 2020, percebendo ainda indícios de existência de racismo estrutural pela avaliação das condenações injustas principalmente de pessoas negras. Assim, a pesquisa contribuiu para o julgamento da Corte sobre a insuficiência de provas naquele caso, levando o Tribunal Superior a reformar a sentença, o que mostra o poder que a argumentação baseada em dados possui.

A produção estatística e a compreensão de padrões a partir do uso de dados, inclusive pessoais, abre caminho para diferentes formas de atuação estratégica, como a percepção de perfis mais afetados por uma determinada demanda, casos repetidos que podem levar à propositura de ações civis públicas ou coletivas, análises que podem ser utilizadas como argumentos perante o Judiciário ou até

26 Ver: https://defensoria.rj.def.br/noticia/detalhes/10808-Relatorio-da-DPRJ-e-citado-em-HC-que--absolveu-homem-preso-por-engano

mesmo colaborações na formação de acordos ou como pressão para a construção ou efetivação de políticas públicas.

Pesquisa e litigância dadocêntrica

Uma base de dados com informações organizadas, padronizadas e confiáveis é valiosa para a produção de conhecimentos, pesquisas e formulação de estratégias para atuação das Defensorias.

- **Compreensão das demandas:** indicadores dos atendimentos realizados podem servir para pesquisas relacionadas às demandas mais recorrentes nas unidades, órgãos ou na Defensoria como um todo.
- **Compreensão de perfis:** indicadores dos atendimentos também poderão servir de insumo para a melhor compreensão do perfil dos usuários das Defensorias, mostrando, por exemplo, quais regiões ou perfil de indivíduo encontram-se recorrentemente em determinada situação de vulnerabilidade.
- **Potencial de motivar políticas públicas:** com indicadores do atendimento é possível mobilizar a atuação de setores políticos, do Legislativo ou Executivo, para a tomada de determinadas medidas.
- **Potencial estratégico em litígios:** com os indicadores do atendimento ou de eventuais surveys promovidas pela Defensorias, é possível agir de forma estratégica em determinados litígios, ou mesmo utilizá-los como reforço argumentativo em demandas perante o poder judiciário.
- **Indicador de possíveis ações civis públicas ou coletivas:** dados do atendimento também podem apontar padrões de demandas e partes envolvidas, servindo como fonte para a identificação de possíveis ações civis públicas e coletivas.

A proteção de dados pessoais é um direito fundamental em razão dos bens que pretende tutelar, dentre estes, a dignidade humana, a liberdade e a não discriminação, bens que, vale lembrar, são reiteradamente ignorados quando se trata da população estigmatizada. Assim, é função da proteção de dados assegurar que agentes de tratamento mantenham suas atividades que dependem do fluxo informacional, mas que o façam a partir de critérios e procedimentos que impeçam o uso abusivo dos dados pessoais.

Uma das formas mais evidentes de abuso diz respeito à coleta excessiva de informações e tratamentos que levam a tomadas de decisão discriminatórias. O avanço tecnológico difundiu uma série de ferramentas que operam a partir da modelagem de perfis, que buscam, a partir de técnicas estatísticas de análise preditivo-comportamental, enquadrar os cidadãos em categorias e identificar seus comportamentos futuros com base nos seus dados. Um exemplo desse tipo de ferramenta é aquele utilizado para realização de credit scoring, procedimento pelo qual os indivíduos recebem uma nota que irá indicar sua qualidade como bom ou mau pagador, utilizando o risco atribuído para determinar os juros a serem cobrados. Os dados utilizados para tais análises de risco alimentam algoritmos[27] muito avançados, que em certos casos não permitem aferir ao certo quais tipos de relação foram estabelecidos; além disso, são variados os tipos de informação nele inseridos, sendo que a grande maioria das empresas de credit scoring não resumem suas análises apenas aos dados de pagamento do consumidor. A falta de clareza sobre o que compõe as análises de tais máquinas pode levar a sérios problemas de ordem discriminatória, replicando padrões sociais de um contexto de profundas desigualdades[28]. Assim, sem as devidas precauções, a tendência é

27 Algoritmos são programas computacionais que com base em insumos fornecem determinadas respostas ou realizam determinadas funções. Estruturados em forma de código, eles funcionam como uma máquina que executa receitas, são inseridos "ingredientes" que serão processados e trarão resultados. O avanço tecnológico permitiu o desenvolvimento de algoritmos que não só executam estritamente as ordens de seu programa (sua receita), mas que também criam seus próprios códigos. Chama-se de machine learning os algoritmos com essa capacidade, que permite que a máquina, sem a ação diretamente humana, desenvolva e aprimore seu próprio programa, o que se realiza pela identificação de padrões originados dos dados que a alimentam.

28 A questão evoca que os problemas de proteção de dados pessoais são problemas de ordem coletiva, envolvendo interesses difusos, nesse sentido, entende-se que a tutela coletiva desempenhará um papel importante na constituição de um regime jurídico brasileiro de proteção de dados pessoais: ZANATTA, Rafael. Tutela coletiva e coletivização da proteção de dados, in: PALHARES, Felipe (org.). Temas Atuais de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2020, p. 345-374. Disponível em: <**https://www.researchgate.net/profile/Rafael-Zanatta/publication/350852661_Tutela_coletiva_e_coletiviza-**

que estas desigualdades se tornem ainda mais profundas.

Para além dos potenciais riscos discriminatórios originados pelos instrumentos de análise preditivo-comportamental desses agentes de mercado, também encontram-se problemas relacionados ao modelo de negócios de muitas empresas digitais, as quais oferecem serviços em troca da atenção ou dos dados pessoais de seus consumidores. A questão pauta um dilema, uma vez que esse modelo de fato permite àqueles que não possuem recursos financeiros amplos acessem uma miríade de serviços, algo positivo da perspectiva de inclusão social. O impasse, entretanto, só será observado com uma análise mais profunda e menos imediata. Apesar dos ganhos aparentes e instantâneos do consumidor, é essencial que sejam amplamente conhecidas as finalidades múltiplas do uso e do tratamento de seus dados pessoais, verificando-se a existência dos riscos de tais informações servirem em prejuízo futuro de seu titular. Esta, contudo, não é análise simplória: exige transparência dos mercados e exige o aprimoramento de uma cultura de proteção de dados que promova investigações sobre potenciais riscos do uso abusivo de informações.

Esse dilema impacta também, e de forma ainda mais sensível, o setor público. Principalmente quando pensamos na oferta de serviços essenciais, cuja prestação deveria ser assegurada pelo Estado, é essencial que as autoridades tenham em mente o problema de vincular a prestação de serviços públicos à concessão de dados, sem que estes sejam de fato necessários. Um exemplo prático dessa problemática surgiu quando, em 2017, o governo municipal de São Paulo pretendeu tornar obrigatório o compartilhamento de dados dos usuários das redes de wi-fi da cidade para fins de marketing direcionado da empresa privada que concederia a estrutura de fornecimento de Internet. Sem dúvidas, o compartilhamento representaria uma baixa de custos aos cofres governamentais. Por outro lado, não são todos que saem ganhando, pois quem está pagando de fato são os usuários do serviço público.

Indagações semelhantes surgiram quando a concessionária da linha quatro do metrô de São Paulo resolveu instalar câmeras de identificação de expressões faciais dos usuários do transporte, as quais serviriam para mensurar os impactos das campanhas publicitárias da linha. A situação levou o Instituto Brasileiro de Defesa do Consumidor (Idec) a mover um processo contra a manutenção da prática. A Defensoria Pública do Estado de São Paulo também atuou no caso, participando

cao_da_protecao_de_dados_pessoais/links/60764caf92851cb4a9dc18e6/Tutela-coletiva-e-coletivizacao-da-protecao-de-dados-pessoais.pdf>.

enquanto assistente litisconsorcial. Os entes sustentavam que a conduta da concessionária era abusiva, justamente por sujeitar aqueles que não têm a escolha de usar ou não o transporte público à tal situação.

Ambas as ocorrências convergem para a mesma questão à qual as Defensorias devem estar atentas: a de que os serviços públicos, por seu caráter de essencialidade e de dever prestacional do Estado, não podem ser condicionados ao compartilhamento de dados do usuário, sem que exista uma real necessidade para tanto. Assim, às Defensorias cabe, primeiramente, observar a adequação de seu próprio serviço em relação à questão e, ao mesmo tempo, estarem atentas para atuar em defesa do direito à proteção de dados frente aos constantes abusos tanto de agentes privados, como de agentes públicos.

Ainda dentro da perspectiva da atuação das Defensorias enquanto agentes do processo de fiscalização e interpretação da LGPD, um outro exemplo a ser citado é a iniciativa da Defensoria Pública do Estado do Rio de Janeiro ao criar um departamento especializado em proteção de dados pessoais dos consumidores, parte de seu Núcleo de Defesa do Consumidor. A ação demonstra como um programa de adequação à LGPD ecoa em aspectos diretamente relacionados à atividade fim das Defensorias. Conforme divulgado pela própria DPE-RJ[29], a criação do departamento faz parte de uma série de medidas da Defensoria do Rio para se adequar à Lei Geral de Proteção de Dados (LGPD) e sua finalidade é a de assegurar os direitos dos consumidores, de forma estratégica e especializada, na proteção e correto manejo de seus dados pessoais, atuando diretamente junto às empresas e entidades responsáveis pela guarda e tratamento destas informações,

29 Defensoria Pública do Estado do Rio de Janeiro. DPRJ cria departamento para proteção de dados dos consumidores. 13 de abril de 2021. Disponível em: <**http://defensoria.rj.def.br/noticia/detalhes/11244-DPRJ-cria-departamento-para-protecao-de-dados-dos-consumidores**>.

Parte 4
COLOCANDO EM PRÁTICA UM PROJETO DE ADEQUAÇÃO

Como gestar um projeto de adequação: primeiros passos

Com base nas experiências observadas neste projeto, alguns pontos se mostraram de grande importância estratégica no momento inicial de estruturação de um programa de governança de dados de uma Defensoria Pública. Como antes pontuado, estamos diante de um ente que possui elevada complexidade estrutural e funcional, o que demanda esforços próprios, principalmente no que toca à estipulação de grupos de trabalho de diferentes segmentos, divisão de tarefas, determinação de responsáveis e comunicação entre todos estes agentes.

a. Apoio da direção

Uma das constatações centrais é que o projeto de adequação irá exigir uma condução que parta da administração. Primeiro porque a LGPD afeta questões que estão sob responsabilidade dos órgãos de gestão como, por exemplo, contratos e convênios entre a Defensoria e terceiros. Mas a importância de seu envolvimento não se limita a questões como estas. As Defensorias operam sob a égide da autonomia funcional dos órgãos que as compõem, o que garante a não interferência política por um lado e, por outro, limita a padronização de seus trabalhos. Um projeto de implementação, contudo, para que faça mais que adequar o ente à lei, aproveitando para também promover uma melhora de eficiência de gestão, demanda, em alguma medida, uma condução centralizada.

Este é um projeto de âmbito geral, que exige uma harmonia entre todos aqueles que compõem uma Defensoria Pública. Seria impossível, por exemplo, utilizar dados pessoais para a gestão de pessoas da instituição se as informações de produtividade fossem coletadas por critérios distintos em cada unidade. No mesmo sentido, se os dados de assistidos ora são inseridos em um sistema integrado, ora em servidores de cada unidade, torna-se muito mais complexo olhar para o todo

e identificar padrões de atendimento, de demandas e, portanto, identificar possíveis estratégias de incidência em políticas públicas. São detalhes que dificultam o exercício da administração e da atuação eficiente.

Além disso, uma figura que centralize e lidere a condução do projeto é importante da perspectiva da própria segurança das informações que estão sendo prestadas, da formação de precedentes e geração de conhecimento. Quando surgirem dúvidas a respeito de algum aspecto de uma atividade de tratamento de dados pessoais, é importante que exista um ponto de suporte ao qual os membros possam recorrer e é importante que exista um local que consolide as informações sobre a matéria.

A experiência que tivemos ao longo dos trabalhos com as Defensorias demonstrou a relevância desse tipo de medida. Em uma das reuniões com o encarregado da Defensoria de São Paulo, foi apontada justamente a necessidade de oferecimento de um canal de comunicação em que as dúvidas ou pedidos a respeito da matéria de proteção de dados possam ser encaminhados. E mais, em que local ficarão armazenadas as respostas aos problemas enfrentados pelo encarregado, sendo de suma importância concentrar tais informações e torná-las acessíveis para que possam existir precedentes e se possa construir conhecimento sobre questões já enfrentadas anteriormente.

b. Criação de um comitê e a função do encarregado

A existência de uma figura que dê o norte e centralize questões gerais, contudo, não representa o todo necessário para garantir a implementação de um projeto de governança da complexidade exigida por uma Defensoria. Duas outras figuras precisam ser destacadas nesse sentido, a do encarregado e a de um comitê de proteção de dados. A Defensoria Pública é instituição dotada de múltiplos órgãos, de diferentes composições, distintos focos de atuação, particularidades de gerenciamento e que são dotados de autonomia funcional para exercer seu trabalho, sem contar o fato de se tratar de um ente público, que, portanto, está sujeito a uma série de deveres e obrigações legais particulares. Tal complexidade institucional e a quantidade massiva de dados tratados sugere a importância das Defensorias indicarem um encarregado, aquele responsável pelo tratamento das informações do controlador. Além do encarregado, sua complexidade sugere também a importância da criação de um comitê de proteção de dados, o que permitiria

uma atuação mais capilarizada do programa sobre as diferentes frentes de trabalho das Defensorias.

No caso do encarregado, em verdade a LGPD determina a obrigatoriedade do agente de tratamento indicar uma pessoa responsável para o cargo. Acerca dessa obrigatoriedade, cabe ressaltar que, por ora, todo controlador deverá atender à previsão, entretanto, conforme previsto no § 3º, art. 41, ficará a cargo da ANPD estabelecer hipóteses de dispensa. Definido no art. 5º, VII da LGPD, o encarregado é aquele com a missão de atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade, além de cuidar da orientação sobre boas práticas a serem seguidas pelos colaboradores e contratados do controlador e outras eventuais atribuições definidas pela Autoridade.

Diferentemente, em relação ao comitê de proteção de dados pessoais, a LGPD não traz menções quanto à obrigatoriedade de criação ou indicação. Entretanto, destacamos a relevância de um comitê[30], por ser esta uma boa solução para iniciar um projeto de governança. A função do comitê é a de gerir o programa de adequação: o grupo será responsável pela verificação das obrigações legais e regulatórias do ente, por aconselhar os diferentes setores da Defensoria sobre o tema da proteção de dados, além de administrar funções técnicas (sistemas e TI, por exemplo) e supervisionar a execução das etapas do programa e o atendimento aos requisitos de conformidade estabelecidos.

Cabe ainda lembrar que a LGPD, diferentemente da GDPR, não determinou que a figura do encarregado deva ser de uma pessoa física, de modo que é possível que um controlador indique uma pessoa jurídica, o que irá depender da conveniência e interpretação legal realizada pelas próprias Defensorias, que irão compreender qual o modelo mais adequado ao seu caso. A Defensoria Pública do Estado de São Paulo, por exemplo, instituiu um órgão encarregado colegiado, composto por um grupo de defensores. Ainda, nesse sentido, é possível que haja uma correspondência entre aqueles que compõem um órgão encarregado e os integrantes do comitê de proteção de dados.

30 Em Santa Catarina, o Comitê Gestor de Proteção de Dados Pessoais - CGPDP foi instituído no Tribunal de Justiça de Santa Catarina pela Resolução GP n. 28/2019. É formado por uma equipe multidisciplinar, composta de magistrados e servidores, que cumulam as suas atividades ordinárias com aquelas do Comitê. O CGPDP está vinculado à Presidência do Tribunal de Justiça, que desempenha o papel de controlador de dados, nos termos da LGPD. No Rio de Janeiro, o presidente do Tribunal de Justiça do Rio de Janeiro, Claudio Mello, designou os integrantes do Comitê Gestor de Proteção de Dados Pessoais (CGPDP) em setembro de 2020. O CGPDP será presidido pelo desembargador Arthur Narciso de Oliveira Neto e coordenado pelo juiz-auxiliar da presidência do TJ-RJ Fábio Porto. Também compõem o comitê os juízes Gustavo Quintanilha de Menezes (auxiliar da Corregedoria Geral de Justiça), Afonso Henrique Barbosa (auxiliar da presidência do TJ) e Aroldo Pereira Junior.

Quanto a um dos estágios iniciais de implementação de programa de governança, o mapeamento e identificação do fluxo de dados da Defensoria, o método de trabalho desenvolvido pela Defensoria de São Paulo representa bem essa divisão de tarefas. Nesse caso, o encarregado determinou responsáveis para cuidar do mapeamento de distintas atividades do trabalho da Defensoria, tais como o atendimento dos órgãos, a administração dos funcionários, as respostas de pedidos de LAI, os trabalhos dos núcleos especializados e do centro de pesquisas. Cada responsável por esses segmentos tem a função de coordenar a ação de demais membros envolvidos nessas atividades para que, em conjunto, sejam identificados os dados e o fluxo informacional das atividades e, posteriormente, seja gerado um quadro geral e amplo sobre o trabalho da instituição como um todo.

Essa visão logo no início do projeto tem uma função central de identificar as prioridades e os pontos de maior urgência a serem endereçados no processo de adequação. A definição clara de quais são essas prioridades virá na fase seguinte, a partir de uma análise de risco dos processos encontrados.

c. Conscientização

De todas as questões que permeiam a implementação de um programa de governança, aquela que talvez seja a mais esquecida, mas de relevância central, é a conscientização. A LGPD, ao entrar em vigor, direcionou os holofotes à proteção de dados, de modo que as instituições parecem ter se dado conta da urgência de se adequar à normativa. A preocupação de que a questão seja solucionada o mais rápido possível, apesar de não equivocada, pode levar a tomadas de decisão precipitadas, como a de despender menos tempo com medidas de conscientização sobre o processo de adequação, partindo logo à implementação em si.

A conscientização dos membros de qualquer instituição é, contudo, etapa essencial de um projeto de adequação à LGPD, cuja atenção não pode ser abreviada pela necessidade de iminente adequação à lei. No caso das Defensorias Públicas, em decorrência de algumas de suas particularidades funcionais e operacionais, a relevância dessa fase é ainda mais evidente.

Uma primeira razão para tanto é uma equivocada percepção de que a matéria da proteção de dados ainda é distante da realidade da maioria dos brasileiros, que não atinge diretamente a vida da população vulnerável, não se tratando, portanto, de uma prioridade do trabalho prestado pelas Defensorias. Essa percepção

pode levar a instituição a encarar o processo de adequação como mera formalidade perante a lei, esvaindo seu potencial transformador. É necessário que os membros das Defensorias tenham consciência de que, na sociedade atual, a representação feita por dados determina as oportunidades e as barreiras a serem enfrentadas por pessoas concretas, com potencial de se tornar um replicador de desigualdades e discriminações. Não se trata apenas de garantir o direito de não receber um anúncio direcionado ou de se proteger de golpes cibernéticos: mais que isso, é uma questão de proteção da personalidade, de defesa da não discriminação e garantia da dignidade humana.

Ainda que no Brasil persista a exclusão digital, é necessário ter em mente que os abusos à proteção de dados pessoais, principalmente sobre a população de baixa renda, já são uma realidade concreta e que se medidas para combatê-los não forem efetivadas, o cenário tende a se agravar. Primeiramente, cabe lembrar que a matéria não só abarca as informações pessoais inscritas em ambiente online pelos próprios usuários, e que dados armazenados e coletados de forma física também estão sob o guarda-chuva da LGPD. Também, a população em situação econômica desfavorável é quem mais tem que recorrer aos benefícios governamentais, os quais estão condicionados ao fornecimento de uma série de dados, que não menos que os de qualquer outro indivíduo, devem estar protegidos de usos abusivos tanto do setor público quanto do privado. Ainda, mesmo sem nunca fornecer diretamente informações pessoais, populações em situação de vulnerabilidade e minorias podem ser vítimas de tecnologias baseadas em dados. Exemplo disso são as ferramentas de reconhecimento facial, as quais apresentam índices de erros desproporcionalmente mais altos em relação à população negra[31] ou, por exemplo, quando fatores discriminatórios influenciam o preço pago para se adquirir um plano de saúde ou ter acesso à crédito[32]. A questão, portanto, não está adstrita a um cenário futurista distante ou aos problemas de um pequeno grupo digitalmente conectado, mas é muito mais ampla e evoca a necessidade de defesa da dignidade humana.

A percepção da relevância da matéria por si é apenas o primeiro dos desafios. Para além dele, a implementação de um projeto de governança de dados irá implicar uma profunda mudança de hábitos e o estabelecimento de determinados

31 <https://www.nexojornal.com.br/expresso/2020/06/14/Reconhecimento-facial-a-suspens%-C3%A3o-da-venda-para-a-pol%C3%ADcia>.

32 O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. Nova York: Crown, 2016.

padrões de trabalho. Como previamente mencionado, os órgãos das Defensorias possuem autonomia funcional, o que garante a liberdade dos defensores para atuar de acordo com suas considerações e melhores entendimentos sobre um caso. A prerrogativa também é entendida como uma garantia da liberdade para que os órgãos determinem seus procedimentos de trabalho. O que sucede com um programa de governança de dados é que parte desse procedimento, que ficava antes a critério de cada defensor, passará a exigir um certo nível de padronização, implicando mudanças de hábitos que nem sempre são fáceis ou compreendidas a priori.

Deve-se ter em mente que essa nova forma de organização e realização do trabalho também não é uma solução pronta e que se resolve pontualmente, mas um exercício constante que perdura no tempo. Até que se criem novos hábitos, o processo exige que os envolvidos percebam a importância do que estão fazendo e que acreditem nos resultados positivos de seu esforço inicial. Como antes ressaltado, a Defensoria é composta por vários entes, diversos órgãos, unidades e colaboradores. Ter um controle direto sobre todas as atividades que envolvem o tratamento de dados é impossível, o que reforça a necessidade de que todos os envolvidos tenham consciência do que buscam alcançar, tratando-se de um esforço eminentemente coletivo.

Conscientização e mudança de cultura

A implementação de um programa de governança de dados implicará algumas mudanças na rotina de trabalho das Defensorias. É nesse sentido que a conscientização e a promoção de uma cultura de proteção de dados desempenha um papel central em um programa como esse. Sendo esta etapa essencial, trazemos aqui alguns pontos importantes para se ter em mente durante sua implementação:

- Muitas vezes pensamos que os movimentos de mudança de cultura se iniciam com uma “chamada para ação”, mas há indícios de que o convite para a transformação é muito mais funcional quando os agentes acreditam que as mudanças são importan-

tes para endereçar objetivos concretos e compartilhados pelo agente[33].

- Em termos organizacionais, apenas conscientizar sobre a necessidade de mudança ou criar um senso de urgência pode ser uma saída que não perdurará por muito tempo. Para que o comprometimento com a causa se estenda, é preciso que os envolvidos valorizem a transformação e sintam responsabilidade sobre ela. Nesse sentido, é importante pensar nos objetivos da Defensoria enquanto instituição e de que forma a incorporação de uma cultura de proteção de dados relaciona-se com sua missão[34].
- Demonstrar bons resultados já obtidos por meio da transformação tem grande valia[35]. Já existem exemplos, inclusive citados neste guia[36], de como uma visão estratégica sobre os dados serviu para promover ações de políticas públicas.
- Envolver os agentes nesse processo de adequação também é importante. Quanto mais as pessoas participam da mudança e se engajam, mais elas tomam consciência dos problemas relacionados e mais se comprometem com a causa[37].
- Os movimentos de mudança são baseados em uma visão compartilhada de futuro da instituição[38], tratando-se de um processo cíclico[39]:

    1. Se inicia em uma etapa de entendimento do problema.
    2. Segue para o estágio de clarificação de onde se deseja chegar.
    3. Desenvolve-se para o estágio de implementação das mudanças.

33 WALKER, Bryan e SOULE, Sarah A. Changing Company Culture Requires a Movement, Not a Mandate. Harvard Business Review. Jun. 2017.

34 Ibidem.

35 Ibidem.

36 Como na atuação da DPE-RJ sobre o aumento das demandas relativas à falta de vagas em creches, p. 29.

37 WALKER, Bryan e SOULE, Sarah A.

38 Medium. How to change your company culture: a four step framework. 2018.

39 Ibidem.

4. Segue para a verificação da efetividade e da avaliação do que de fato melhorou e o que pode ser melhorado. Após, retorna-se para o estágio 1.

- Entender como e por que padrões de rotina indesejados se repetem é outra questão a ser considerada[40]. Por que, por exemplo, o cadastro do atendimento não é realizado ou por que ferramentas institucionais são preteridas em relação a outras disponíveis no mercado? É importante perceber que tais padrões ocorrem como uma combinação do indivíduo e fatores do ambiente, para serem mudados, ambos os aspectos precisam ser trabalhados. Por isso, devem ser oferecidas condições satisfatórias para que as pessoas possam adotar uma rotina alternativa[41].

Adequação da Defensoria Pública à LGPD

A seguir, trataremos de algumas possíveis etapas e processos relativos a um programa de adequação à LGPD. Contudo, antes cabe um adendo para reforçarmos um sentimento "não paralisante" em relação aos pontos e desafios apresentados.

Nesse sentido, ressaltamos que não há tratamento de dados que não envolva algum tipo de risco, o que não significa que todo o uso de dados é ilegítimo ou prejudicial. Essa perspectiva vai de encontro com a própria conformação jurídica da proteção de dados, que se origina da análise de que os dados representam ativo importante para uma série de atividades, algumas das quais essenciais, dentro do contexto atual de uma sociedade informacional. Assim, nem sempre será possível incorporar todas as salvaguardas possíveis, garantir a segurança máxima ou a

40 Medium. Changing Culture: Shift Small Habits for Big Wins. 2016.

41 Ibidem.

anonimização completa de um processo.

Tais questões são ainda mais marcantes no contexto das Defensorias Públicas, que prestam serviços essenciais e possuem missão institucional ampla. Enquanto parte do setor público, e tendo como objetivo garantir o acesso à justiça (que vai muito além do Judiciário), há o enorme potencial de que as Defensorias se utilizem das informações em mãos para automatizar processos, gerar inteligência e conhecimento, atuar estrategicamente, e melhorar trâmites internos. Evidentemente, esse uso inovador dos dados implica a ampliação do tratamento realizado, porém, pode também colaborar com o atendimento de sua função pública e essencial.

Por esse motivo, destacamos o valor de uma análise que considere o tratamento a partir da perspectiva de seus riscos e benefícios. Reforçamos que os gaps sempre existirão, mas estes não podem paralisar o importante trabalho desempenhado pelas Defensorias. O objetivo é identificá-los para que com isso seja possível mitigá-los sem o comprometimento das atividades necessárias ou importantes. Assim, o objetivo deste Guia vai além de trazer aspectos para que a instituição garanta sua conformidade em relação à LGPD, mas principalmente busca mostrar como os processos de adequação e de implementação de programas de governança podem contribuir com a missão institucional das Defensorias.

Aspectos de um programa de adequação

Equipe envolvida: As Defensorias Públicas são entes organizacionalmente complexos, no sentido de que cada uma delas é composta por diversos setores funcionais, administrativos, de coordenação, de gestão interna, relação externa, núcleos especializados e órgãos que contam com autonomia funcional. Um projeto de adequação do ente exigirá a colaboração e participação de todas as partes que o compõem, uma vez que, em última instância, todas operam em prol da missão institucional da Defensoria e, legalmente, se encontram sob seu guarda-chuva.

Para que se promova um projeto de adequação, é importante compor, para além de um comitê de proteção de dados, equipes de trabalho que abarquem os diferentes setores de atividades de uma Defensoria. Cada ente tem a melhor capacidade de compreender qual a subdivisão mais adequada para seu caso, mas deixamos a sugestão de uma primeira subdivisão mais ampla, entre:

- **Atendimento:** pode envolver equipes específicas para áreas como (i) atendimento de balcão e (ii) atividades de núcleos especializados, ou mesmo podem se subdividir por unidades e órgãos regionais.

- **Administração:** pode envolver equipes específicas para áreas como (i) recursos humanos, (ii) TI e sistemas informacionais, (iii) setor financeiro, etc.

- **Geração de inteligência e pesquisa:** se a Defensoria possuir uma área própria para a realização de pesquisas, é importante que ela também esteja engajada nesse processo, tanto no tocante ao fornecimento de dados para pesquisas acadêmicas, se ela for demandada por estudantes e pesquisadores dos mais diversos níveis, quanto pesquisas internas direcionadas para gerar inteligência quanto aos dados da própria Defensoria Pública, por exemplo, para saber qual unidade do estado atende mais vítimas de violência doméstica e, portanto, deveria receber mais defensoras(es) especializados neste tema.

- **Contratos e parcerias:** as Defensorias recorrentemente realizam uma série de parcerias e convênios, seja com cartórios, órgãos do governo em diferentes níveis da federação, empresas e terceiro setor. Muito provavelmente as relações estabelecidas envolvem maior ou menor grau de tratamento de dados pessoais, de modo que pode ser interessante tratar do cuidado com esse aspecto de forma específica.

1 **ATENDIMENTO**	Triagem socioeconômica Documentos do atendimento Informações sobre o caso ou processo
2 **ADMINISTRAÇÃO**	Dados de defensores e servidores Informações dos sistemas informáticos Relatórios, processos administrativos e pedidos de LAI
3 **GERAÇÃO DE INTELIGÊNCIA E PESQUISA**	Dados dos atendimentos como insumo para pesquisa Coleta de informações via formulários Litigância estratégica por meio dos dados
4 **CONTRATOS E PARCERIAS**	Compartilhamento com terceiros Recebimento de dados de terceiros Parcerias que envolvem tratamento conjunto de dados

Etapas mínimas

Algumas etapas bases terão que ser percorridas e a Associação Data Privacy Brasil de Pesquisa futuramente publicará materiais que exploram com maior profundidade cada uma das etapas necessárias para um projeto de adequação. Neste documento, deixamos, por enquanto, algumas breves indicações das etapas recomendadas para um momento inicial. Também destacamos que não há uma ordem estrita de etapas a serem seguidas, de modo que cada Defensoria, em observância a sua realidade particular, é quem poderá estabelecer seu cronograma de adequação:

- **Conscientização:** O primeiro passo é, sem dúvidas, o trabalho de conscientização junto aos membros da Defensoria. Como antes levantado, a adequação do ente não se encerra com a instituição de uma política, trata-se de um trabalho contínuo que exigirá a mudança de hábitos, o que não é algo fácil de ser executado. Para vencer esse desafio, é essencial que os envolvidos acreditem na importância e no valor de seu esforço. A conscientização pode já vir acompanhada da identificação de pontos críticos de desconformidade da unidade com a Lei; além disso, muitas vezes quem está participando das etapas de conscientização já tem o poder de

alterar processos que estejam em desconformidade. Assim, é importante orientar essas pessoas para que elas registrem as eventuais desconformidades que notarem e as medidas que adotaram para resolvê-las ou mitigá-las de alguma forma, porque posteriormente isso poderá diminuir o trabalho na etapa de mapeamento.

- **Mapeamento:** Ter em mãos o fluxo dos dados e das atividades a que estes se referem é também um dos trabalhos iniciais a ser desenvolvido durante o programa de adequação. Destacamos que o processo de mapeamento é mais amplo do que a compreensão de quais dados se encontram sob o controle da Defensoria, sendo necessário um quadro que relacione dados e finalidades, primárias e secundárias, que são, por sua vez, centrais para pensar em bases legais de tratamento. Indicamos nesse momento que os responsáveis identifiquem:

  (i) Quais os dados coletados?
  (ii) Para que finalidade é realizada a coleta?
  (iii) Qual a base legal que a sustenta?
  (iii) Há alguma outra atividade que faz uso desses dados? Se sim, qual base legal a sustenta?
  (iv) Há o compartilhamento desses dados com outros setores da Defensoria?
  (v) há o compartilhamento desses dados com agentes externos à Defensoria?

  Pode ser que as pessoas que preencham o mapeamento não reúnam conhecimento suficiente para atribuir uma base legal ao tratamento de dados. Nesse caso, é importante definir quem ficará responsável por esse procedimento: pode ser, por exemplo, o comitê de proteção de dados, a partir do mapeamento apresentado por cada área. Uma outra dica interessante pode ser a de dividir o mapeamento entre as áreas, conforme sugerimos anteriormente e, internamente, as áreas podem se dividir para organizar um cronograma quanto às atividades que mapearão no decorrer do processo de adequação.

- **Matriz de risco:** a partir do mapeamento, será possível construir uma matriz de risco, tomando como base as atividades e os dados por ela utilizados. Os responsáveis por essa etapa construirão uma matriz que comporta dois eixos, um de ganhos e outro de riscos referentes a cada atividade de tratamento desempenhada. Alguns critérios possíveis para mensurar cada um dos eixos são:

    » Ganhos: necessidade do tratamento para a consecução de uma finalidade, ganhos em termos de recursos, melhora da capacidade de compreensão do trabalho realizado, cumprimento de determinação legal, melhora do atendimento ao assistido, possibilidade de melhorar o respeito aos direitos dos titulares de dados, melhora na prestação do serviço de advocacia para os assistidos, etc.
    » Riscos: sensibilidade dos dados, vulnerabilidade dos titulares de dados, potenciais vazamentos e outros incidentes de segurança e os seus riscos para os titulares de dados, potenciais usos abusivos, riscos reputacionais, riscos financeiros (como multa) em caso de irregularidades, etc.

- **Delimitação de prioridades:** Com base nas conclusões da matriz de risco será possível que o comitê de proteção de dados compreenda quais são os pontos mais sensíveis e de maior potencial de risco dentre as inúmeras atividades da Defensoria que envolvem o tratamento de dados. Isso tornará possível priorizar os trabalhos sobre determinadas atividades mais fragilizadas.

Organização

Para concretizar as etapas descritas e os passos que as seguem é necessário organização e clareza. Assim, é essencial criar um programa de trabalho com cronograma das etapas, equipes responsáveis, além da ordem de prioridades, método de comunicação e local de armazenamento de informações. Nesse tipo de planejamento a padronização é muito importante, pois é provável que diferentes equipes estejam envolvidas em uma mesma etapa.

No caso, por exemplo, de existir uma equipe responsável pelo mapeamento e construção de matriz de risco para atividades fins e outra para atividades meio, será imprescindível que os critérios de avaliação de riscos utilizados sejam os mesmos. A determinação de qual o método a ser seguido em cada fase do projeto pode variar de Defensoria para Defensoria, porém, é importante que este padrão interno exista.

Recursos

Caso opte por realizar seu próprio programa de adequação, talvez o maior desafio de uma Defensoria, em termos de recursos, seja o tempo. Os membros, defensores, servidores e outros colaboradores, já desempenham suas atividades rotineiras para manter o funcionamento da instituição, de modo que acrescentar mais um comprometimento nessas circunstâncias se torna um grande desafio. Saber dividir as tarefas e manter um método de trabalho que permita essa divisão é um ponto chave.

Além do tempo, é provável também que surjam demandas de infraestrutura, por exemplo a contratação de um sistema operacional próprio ou a instalação de mecanismos de autenticação de usuários. Nesses casos, a Defensoria, por ser uma instituição pública e renomada, pode encontrar soluções criativas por meio de parcerias com Universidades ou com outros entes governamentais.

Tempo estimado

Estima-se que pelo porte da Defensoria, em comparativo com o tamanho de uma grande empresa, o programa de adequação poderia ser realizado no período aproximado de 1 (um) ano. Porém, existe o mencionado desafio de tempo de dedicação possível dos membros envolvidos. Além disso, é provável que existam, ainda, percalços extras que não são costumeiramente observados em empresas, como o nível de autonomia funcional dos órgãos. Assim, em vista do longo período de execução do projeto, compreender quais são os pontos prioritários é ainda mais relevante.

Construção de políticas

A instituição de algumas políticas relativas ao tratamento dos dados é mais um dos trabalhos a ser desenvolvido e aprimorado ao longo da execução do programa. A Defensoria terá que encontrar formas de garantir o devido cumprimento da LGPD que comportem as necessidades dos trabalhos por ela desenvolvidos. Dentre algumas dessas políticas, são de suma importância:

- **Política de coleta:** compreender quais os meios empregados durante a coleta de dados pessoais, qual a base legal que a justifica e quais as finalidades e usos secundários.

- **Políticas de descarte:** compreender por quanto tempo as informações ficarão armazenadas nos servidores das Defensorias, tendo em vista a finalidade do tratamento.

- **Políticas em relação aos convênios:** compreender, no caso de convênios que envolvam o compartilhamento de dados da ou para a Defensoria, quais as finalidades e as bases legais que sustentam esse compartilhamento, como garantir a adequação dos termos em relação à LGPD.

- **Políticas sobre a requisição de direitos:** compreender como o titular pode requisitar direitos relativos à proteção de seus dados, como exclusão, retificação e confirmação de existência, de que forma se garantirá a autenticidade e a legitimidade do pedido.

- **Políticas de Transparência:** além de uma obrigação legal, é uma boa prática ser ativamente transparente em relação ao tratamento de dados realizado, sendo interessante a existência de um portal que explique os diferentes tipos de atividades e finalidades do uso dos dados. No caso da Defensoria, um portal como este pode ter ainda uma função educativa, demonstrando aos usuários quais seus direitos perante qualquer ente que realize o tratamento de suas informações pessoais.

- **Política de Governança:** documento que contém os aspectos gerais, éticos e procedimentais a respeito de todo tipo de tratamento de dados pessoais realizados pela Defensoria.

Pensando em medidas em termos de esforços e medidas

Em sequência, apresentaremos uma tabela que ilustra uma das formas possíveis de compreender como algumas das medidas tratadas neste Guia podem ser visualizadas sob a perspectiva de esforços empenhados e benefícios adquiridos, tomando a conformidade como algo positivo, sem se restringir a ela.

Contudo, antes fazemos o importante adendo de que a tabela se trata de um exemplo metodológico. Nesse sentido, os critérios, os pesos, a escala e os valores atribuídos não têm a pretensão de representar toda a complexidade do que poderá ser considerado por uma Defensoria na prática. Além de que, não acreditamos ser possível trazer um modelo pronto e adequado à realidade particular de diferentes Defensorias. Nesse sentido, para além da imagem, trazemos um detalhamento metodológico de como é possível criar um gráfico como este, adequando-o às especificidades e entendimentos que somente os integrantes da instituição poderiam ter.

	ESFORÇO EMPENHADO			BENEFÍCIOS CONQUISTADOS			
Medidas possíveis	Recursos financeiros	Mobilização de pessoal	Tempo	Conformidade com a lei	Potencial inovador e melhora de processos	Relação de confiança e reputação	Relação esforço/ benefício
Designar um encarregado	1	2	2	4	4	4	**9,5**
Criar um comitê de Proteção de Dados	1	3	3	4	4	4	**9**
Criar canal para usuários	3	3	3	4	3	5	**7**
Mapear dados	4	4	4	4	5	4	**5,5**
Estabelecer um programa de conscientização	4	4	4	4	5	4	**5,5**
Criar a matriz de risco	4	3	3	4	3	4	**4,5**
Criar políticas	2	4	4	4	4	4	**6**
Criar portal de transparência	4	3	4	4	3	5	**5**

Na coluna "esforço empenhado" adicionamos três critérios possíveis a se considerar em relação aos esforços ou custos de uma determinada medida. Do mesmo modo, adicionamos três critérios possíveis a serem considerados quanto aos benefícios de uma determinada medida. Para cada um dos critérios atribuímos um valor dentro de uma escala de 1 a 5. Considerando que determinados critérios podem ter uma relevância mais proeminente, atribuímos pesos diferenciados - neste caso, optamos por dar peso 1,5 (um e meio) para os benefícios referentes ao "potencial inovador" e ao "reforço da relação de confiança com os usuário e reputação no sistema de Justiça".

Com a determinação de critérios, pesos, graus de atribuição, relacionamos os valores entre esforços empenhados e benefícios conquistados. O gradiente de tons da coluna 1 (um), "Medidas possíveis: relação esforço benefício em cores", representa, dos tons mais escuros aos tons mais claros, o que pode trazer um benefício mais alto em relação ao empenho exigido pela medida.

O processo de atribuição de valores dependerá da realidade concreta de cada Defensoria. Ainda assim, a título explicativo, apresentaremos os pontos considerados em nossa avaliação. A designação de um encarregado, por exemplo, apesar de demandar uma análise não trivial de um indivíduo (ou grupo) com conhecimento em proteção de dados (*hard skill*) e gestão de pessoas e processos (*soft skill*), é facilmente operacionalizada. Para formalizar a nomeação, as Defensorias têm editado portarias, algo que não demanda a alocação de recursos financeiros (item 1), novas contratações e engajamento de muitos colaboradores (item 2), ou mesmo um período de tempo demasiado (item 3). Em termos de benefício, é uma das principais obrigações previstas na LGPD (item 4), sendo o encarregado o representante, de dentro para fora (item 5) e de fora para dentro (item 6), das Defensorias em todos os aspectos da proteção de dados. No que toca, por exemplo, a um programa de conscientização, há uma maior complexidade tanto no possível empenho de recursos (item 1) - para a produção e aquisição de materiais ou eventual contratação de especialistas - como na necessidade de engajamento de um número muito maior de colaboradores (item 2) por um período prolongado de tempo (item 3). Ainda que não seja diretamente uma obrigação legal, a conscientização desempenha papel fundamental para que outros processos de adequação à LGPD operem apropriadamente (item 4), projetando-se de uma perspectiva interna (item 5) e externa (item 6).

Essa tabela pode ser construída por ferramentas simples, como uma tabela de Excel, que automaticamente indicam o gradiente de cores e calculam os pesos

conforme determinado por seus formuladores. Essa mesma metodologia também pode ser aplicada na avaliação de priorização de processos. Nesse caso, a única diferença é que se recomenda utilizar a escala de valores em uma sequência Fibonacci (ex. em uma escala de 1 a 8, poder-se-ia atribuir valores 1, 2, 3, 5 e 8), o que servirá para que as atribuições não fiquem presas à uma média, o que seria um problema quando o objetivo é comparação de prioridades.

Medidas emergenciais

Muitas das etapas e medidas apresentadas neste Guia podem ter um prazo de execução extenso e apresentar um grau de complexidade que inviabiliza sua implementação imediata. Nesse sentido, propomos aqui algumas medidas mais céleres e que podem contribuir desde logo para garantir um nível de adequação mínimo antes de se dar início a um programa de governança de dados completo.

- **Canal de acesso aos titulares:** criação de um meio de comunicação para que os titulares possam requerer à Defensoria informações acerca do tratamento, solicitar a retificação ou exclusão dos dados.
  - » Possíveis canais: telefone, e-mail, plataformas no site e requisição pessoal são todos meios possíveis para se disponibilizar esse espaço ao usuário.
  - » Pontos de atenção: a depender da solicitação, irá variar o nível de segurança a se impor sobre a autenticação do indivíduo. Essa verificação é mais sensível no caso de requisições feitas por vias remotas, que dificultam a comprovação de que o solicitante é o titular dos dados.

- **Trâmite das análises de solicitações:** criação de uma estrutura organizacional de (i) recebimento, (ii) análise, (iii) reporte das solicitações recebidas e (iv) análise de possíveis recursos.
  - » Responsáveis: identificar quem serão os responsáveis por cada uma das etapas indicadas.

» Possibilidades: uma possibilidade viável é se basear na estrutura utilizada na análise de pedidos de LAI. Não se trata de unificar os processos em um mesmo canal, mas tomar a estrutura organizacional do trâmite das solicitações via LAI como um modelo para os processos de requisição de direitos dos titulares.

Conclusão

A adequação à Lei Geral de Proteção de Dados é uma tarefa complexa, porém plenamente factível pelas entidades do sistema de Justiça no Brasil. O simples transplante de soluções do setor privado é incabível, diante das inúmeras especificidades das Defensorias Públicas e sua natureza única de atendimento à população, produção de conhecimento sobre políticas públicas e exercício de direitos e sua possibilidade de litigância e defesa de direitos.

As Defensorias Públicas podem ser líderes de um processo de transformação cultural do sistema de Justiça. Essa transformação passa pelo reconhecimento de que os dados são das pessoas e que há uma relação de confiança e de obrigações ao realizarmos os tratamentos desses dados. Além disso, há uma questão de responsabilidade e ética pelo tratamento correto desses dados, impedindo utilizações abusivas e indevidas.

A construção de programas de governança de dados pessoais pode ser vista por uma chave dupla: tanto pelo lado da inovação, permitindo o encaixe no planejamento estratégico e a possibilidade de um trabalho verdadeiramente interdisciplinar, como pelo lado da cidadania, garantindo o respeito aos titulares dos dados e usuários deste importante serviço público prestado pelas Defensorias. A realização desse "dever de casa" deve ser vista também como oportunidade de inovação institucional e aproveitamento das potencialidades dos dados, que podem e devem circular dentro de condições de confiança e máxima transparência perante a sociedade.

A Lei Geral de Proteção de Dados não impede a inovação e o fluxo dos dados. Pelo contrário, ela garante que os dados possam ser utilizados de forma legítima, com respeito aos direitos dos titulares e procedimentos para que haja documentação, avaliação de risco e fluxos adequados para a sua utilização conforme finalidades específicas. Este Guia é um convite à ação e à inovação, partindo do desejo coletivo de assegurarmos cidadania e acesso à justiça no Brasil.

Este documento é o primeiro de uma série de guias e relatórios sobre o projeto desenvolvido entre as Defensorias Públicas e a Associação Data Privacy Brasil de Pesquisa. Nosso objetivo foi de trazer explicações sobre essa parceria, quais seus objetivos e procedimentos, além de algumas constatações acerca do momento inicial de implementação de um programa de governança de dados de uma Defensoria Pública. Os trabalhos junto aos órgãos de São Paulo e do Rio de

Janeiro continuam e, com isso, esperamos publicar novos guias que relatam essas experiências e que possam servir de material de apoio para outras Defensorias de todo o país.

Anexo I

CRONOGRAMA DE AULAS - CURSO PRIVACIDADE E PROTEÇÃO DE DADOS	
Aula 15/09/2021 Arquitetura da privacidade e proteção de dados pessoais: evolução, princípios e desafios atuais	Boas-vindas e apresentação da estrutura do curso. Foram abordados os aspectos históricos dos direitos à privacidade e proteção de dados.
Aula 22/09/2021 Conceito de Dado Pessoal e Base Legal do Legítimo Interesse	Atividade prática de estudo de caso que discutiu a instalação de um sistema integrado de registro de informações dentro de uma Defensoria Pública. Os alunos deveriam exercitar os conceitos de bases legais e finalidades do tratamento, assim como refletir sobre o possível uso das informações do sistema para o aprimoramento das atividades meio e fim das Defensorias.
Aula 29/09/2021 Consentimento e a Jornada do Atendimento	Atividade prática de estudo de caso que discutiu o cenário de implementação de um aplicativo de agendamento e triagem dentro de uma Defensoria. Os alunos foram desafiados a refletir sobre a coleta de dados de seus usuários, políticas de privacidade, maneiras de informar o titular acerca do uso de suas informações pessoais e os requisitos da base legal do consentimento.
Aula 06/10/2021 Concessão do Sistema de Bilhetagem e a Proteção de Dados e Setor Público	Atividade prática de estudo de caso que discutiu situação em que o governo resolve implementar um sistema de bilhetagem no transporte público, realizando a coleta de dados pessoais dos usuários para diversas finalidades, como publicidade e funcionalidades financeiras. Os alunos foram convidados a refletir sobre os diversos aspectos dessa ação e a exercitar uma possível atuação (atividade fim) da Defensorias na defesa de direitos relativos à proteção de dados.
Aula 13/10/2021 Credit Scoring	Atividade prática de estudo de caso que discutiu a situação de uma empresa que realizava a coleta de dados pessoais de indivíduos para realizar modelagem de crédito. Os alunos foram convidados a conhecer a cadeia desse tipo de modelo de negócio e a refletir sobre os potenciais abusos da prática. Reflexão voltada principalmente à atividade fim das Defensorias, seu objetivo era explorar possível caso em que a Defensoria poderia atuar em defesa dos direitos à proteção de dados.

CRONOGRAMA DE AULAS - CURSO PRIVACIDADE E PROTEÇÃO DE DADOS	
Aula 20/10/2021 Requisição de Direitos: Dados sensíveis, de saúde e direitos do titular	Atividade prática de estudo de caso que discutiu a situação em que os usuários da Defensoria e terceiros entraram com requisições de direitos à proteção de dados em relação ao ente. O cenário explorou os diferentes tipos de dados coletados pelas Defensorias e os diferentes tipos de requisição previstos pela LGPD. O caso foca especialmente nas atividades meio da Defensoria, visto que a administração terá que construir uma estrutura para atender a este tipo de demanda.
Aula 27/10/2021 Proteção de Dados e Incidentes de Vazamento	Atividade prática de estudo de caso que discutiu as possibilidades de ação de uma instituição frente a incidentes de vazamento de dados. Nessa atividade, focada principalmente nas atividades meio das Defensorias, os alunos foram convidados a refletir sobre como proceder em casos de incidentes, ameaças de hackers e como se posicionar em termos de transparência, publicidade e informe dos titulares atingidos.
Aula 03/11/2021 Direitos coletivos e proteção de dados pessoais nas Cortes	Atividade prática de estudo de caso que discute a legalidade e constitucionalidade do uso dos dados no contexto de combate à COVID-19. Os alunos, representando grupos com distintos interesses na causa, deveriam refletir sobre o caso em que uma Medida Provisória determina o compartilhamento de dados entre agentes do setor privado e público para fins de combate à pandemia.
Aula 11/11/2021 Relatório de impacto e análise de risco	Atividade prática de estudo de caso que discutiu uma medida do Governo Federal de implementação de um sistema de reconhecimento facial em aeroportos, situação hipotética em que os dados seriam integrados a sistemas de segurança do governo. Os alunos foram convidados a representar grupos com distintos interesses e refletir sobre a legalidade ou abusividade da medida.
Aula 17/11/2021 Desenvolvimento e Implementação de Programas de Governança de Privacidade e Proteção de Dados.	Aula que abordou aspectos práticos sobre o Data Protection Officer (DPO) e o time de Proteção de Dados, Projeto de Adequação às Normas de Proteção de Dados, Relatório de Diagnóstico de Proteção de Dados (RDPD), Regime de Responsabilidade Civil mitigação por meio de Data Processing Agreements (contratos).
Aula 28/11/2021 Simulação Final: Programa de Adequação e Relatório de Diagnóstico de Proteção de Dados Pessoais	Atividade prática final em que os alunos deveriam realizar as etapas de um programa de adequação à LGPD. Divididos em equipes, cada uma delas deveria focar em um macroprocesso da Defensoria. Durante o dia, os alunos produziram documentos de mapeamento e fluxo de dados, de identificação das bases legais, de matriz de risco, protocolos de atuação e dossiês sobre pontos sensíveis a serem incorporados em uma política de governança de dados.

Anexo II

ENTREVISTADO	CARGO	DEFENSORIA (RJ/SP)
Entrevistado(a) 1	Servidor(a) Público(a) - Área TI	DPE RJ
Entrevistado(a) 2	Defensor(a) Público(a) - Direito de Família	DPE RJ
Entrevistado(a) 3	Defensor(a) Público(a) - Direito do Consumidor	DPE RJ
Entrevistado(a) 4	Defensor(a) Público(a) - Direito da Criança e do Adolescente	DPE RJ
Entrevistado(a) 5	Defensor(a) Público(a) - Direito Penal	DPE RJ
Entrevistado(a) 6	Defensor(a) Público(a) - Direito de Família	DPE RJ
Entrevistado(a) 7	Servidor(a) Público(a) - Área TI	DPE RJ
Entrevistado(a) 8	Defensor(a) Público(a) - Direito Civil	DPE RJ
Entrevistado(a) 9	Defensor(a) Público(a) - Direito Civil e Fazenda Pública	DPE SP
Entrevistado(a) 10	Defensor(a) Público(a) - Admnistração	DPE SP
Entrevistado(a) 11	Defensor(a) Público(a) - Setor de Pesquisa	DPE RJ
Entrevistado(a) 12	Defensor(a) Público(a) - Setor de Pesquisa	DPE SP
Entrevistado(a) 13	Defensor(a) Público(a) - Direito do Consumidor	DPE SP
Entrevistado(a) 14	Servidor(a) Público(a) - Área TI	DPE SP

RELATÓRIO DE DISCUSSÕES DA OFICINA PRÁTICA DE **ADEQUAÇÃO À LGPD**

RELATÓRIO DE DISCUSSÕES DA OFICINA PRÁTICA DE ADEQUAÇÃO À LGPD[1]

BRUNO R. BIONI
HANA MESQUITA
RAFAEL A. F. ZANATTA

Introdução[2]

A Associação Data Privacy Brasil de Pesquisa realizou o evento **Oficina Prática de Adequação à Lei Geral de Proteção de Dados** nos dias 05 e 07 de julho e 12 de agosto de 2021 com o objetivo de promover o intercâmbio de experiências horizontais entre Defensorias Públicas de todo o país no que diz respeito aos desafios da adequação do ente à Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), considerando a vigência da legislação desde setembro de 2020[3].

A Oficina ocorreu dentro do escopo do projeto **Defensorias Públicas e Proteção de Dados**, promovido pela Data Privacy Brasil em parceria com o Conselho Nacional das Defensoras e Defensores Públicos-Gerais (**Condege**) e as Defensorias Públicas Estaduais do **Rio de Janeiro** e de **São Paulo**. O projeto nasceu a partir da necessidade de se pensar na adequação do sistema de Justiça à LGPD e no papel das Defensorias na promoção do acesso à justiça.

1 Esse material foi resultado da Oficina Prática realizada no âmbito do projeto "Defensorias Públicas e Proteção de Dados". O documento sistematiza as principais reflexões e achados do evento. Originalmente foi disponibilizado no site <**https://www.dataprivacybr.org/projeto/expandindo-o-papel-dos-defensores-publicos-na-protecao-de-dados-pessoais-no-brasil/**>

2 A Associação Data Privacy Brasil de Pesquisa registra a valiosa e imprescindível contribuição da pesquisadora Marina Kitayama que trabalhou empenhadamente ao longo dos últimos meses no projeto Defensorias Públicas e Proteção de Dados. Kitayama foi responsável pela condução da Oficina Prática, coletando grande parte dos dados utilizados na elaboração deste relatório.

3 Sobre a história da LGPD, ver o documentário "Memória da LGPD" disponível no Observatório da Privacidade da Associação Data Privacy Brasil de Pesquisa. Disponível em: <**https://www.observatorioprivacidade.com.br/memorias/**>.

Afinal, ao realizar o atendimento de milhões de cidadãos brasileiros por ano, as Defensorias Públicas tratam dados pessoais de milhões de pessoas em situação de maior vulnerabilidade que buscam esse serviço público garantido constitucionalmente. Além disso, as Defensorias também são agentes centrais na defesa de direitos da população frente ao uso abusivo de dados pessoais de modo que a LGPD impacta tanto a atividade-fim quanto a atividade-meio.

Nesse sentido, o projeto foi estruturado para contemplar duas frentes de atuação: a primeira delas, implementada em parceria com a Escola Data Privacy Brasil, foi a de realizar a formação das pessoas designadas para participar nos comitês de proteção de dados, constituídos para promover a adequação da instituição.

Assim, houve a promoção de um curso extensivo, no segundo semestre de 2020, que contou com a participação de 66 alunos, membros de 14 Defensorias Públicas estaduais brasileiras, reunindo as 5 regiões brasileiras.

Em seguida, em parceria com o Condege, foram disponibilizados acessos ao curso EAD do Data Privacy Brasil, para diversas Defensorias Públicas ao redor do Brasil. O curso EAD foi finalizado em abril de 2021 e disponibilizou o total de 121 vagas. Posteriormente, existe a expectativa de realização de alguns seminários sobre temas importantes para destravar a adequação da instituição à LGPD.

É importante ressaltar que, antes da formulação do programa desses cursos, foram realizadas uma série de entrevistas para compreender que tipo de conteúdo poderia ser interessante de apresentar aos integrantes das defensorias, diante das especificidades das atividades de tratamento de dados dentro dessas instituições.

Já a segunda frente, de Governança, é voltada ao acompanhamento das reuniões dos comitês de proteção de dados que se formaram no Rio de Janeiro e em São Paulo. Nessa segunda parte do projeto, o Data Privacy Brasil participou como ouvinte de cinco reuniões com a Defensoria Pública de São Paulo e três reuniões com a Defensoria Pública do Rio de Janeiro no intuito de compreender o que tem sido feito para promover a conformidade das Defensorias Públicas Estaduais à LGPD, bem como quais são os principais desafios enfrentados pela instituição.

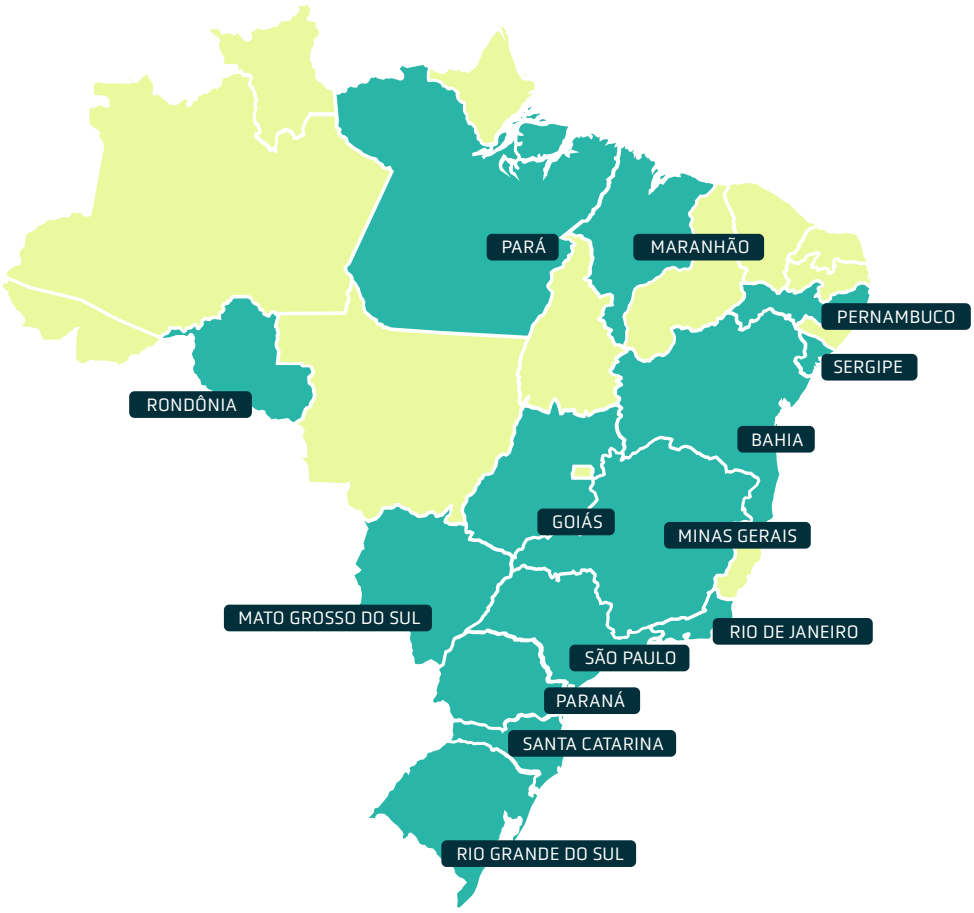
Devido à compreensão derivada da presença nesses espaços, foram produzidos um Guia de Adequação para essas instituições e outros materiais que poderão auxiliar a destravar o processo de adequação, como, por exemplo, templates de formulários que poderão ser mobilizados para o mapeamento e, depois, para a compreensão contínua do nível de adequação atingido pelas Defensorias, além de um *roadmap* de adequação para essas instituições.

As duas frentes estão relacionadas com o caráter cíclico que se deseja dar ao projeto defensorias, ou seja, ao mesmo tempo em que buscamos formar as pessoas que trabalham na instituição, também buscamos compreender quais são as potencialidades e desafios desse processo, a fim de produzir materiais que possam facilitar a tarefa de estar em conformidade com a LGPD. Isso porque, entendemos que um projeto de adequação de uma instituição como a Defensoria Pública é permeado por particularidades que não são contempladas pela metodologia usualmente utilizada para a adequação em organizações privadas.

Nesse sentido, muito do trabalho nesta segunda frente do projeto diz respeito ao enfrentamento da necessidade de moldar a metodologia de adequação à LGPD, usualmente utilizada no setor privado, aos desafios e potencialidades expostos pelos defensores nas reuniões dos Comitês de Proteção de Dados no Rio de Janeiro e em São Paulo, por meio da nossa participação como ouvintes nesses espaços. Assim, é importante reforçar a atuação passiva do Data Privacy Brasil nesses espaços, onde o que se buscou foi a compreensão dos desafios enfrentados pelas Defensorias e não a resolução de dúvidas ou realização de sugestões práticas para promover a conformidade com a LGPD.

Isso é necessário para que a conformidade com a lei não seja encarada como um processo paralisante, mas, pelo contrário, como um projeto que traz a possibilidade de rever atividades ou fluxos de tratamento que ocorrem de forma ineficiente ou desatualizada.

Assim, o presente relatório consolida as discussões realizadas no bojo da **Oficina Prática** que reuniu representantes de Defensorias de todo o Brasil e contou com a presença de cerca de 60 participantes:



No primeiro dia de oficina, 05 de julho, discutiu-se aspectos da proteção de dados em sistemas integrados de cadastramento e a realização do atendimento por vias remotas. No segundo dia, a discussão girou em torno dos convênios e contratos que envolvem o compartilhamento de dados e das estratégias e pontos sensíveis da estruturação e implementação de um programa de adequação à LGPD.

No terceiro dia, a discussão se baseou nos enunciados elaborados pelos participantes. Os enunciados partem dos tópicos de discussão dos primeiros dois dias de Oficina e indicam a interpretação do grupo acerca de um dispositivo da LGPD. Alguns grupos não desenvolveram os enunciados, porém isso não inviabilizou o debate acerca dos temas propostos pela equipe do Data Privacy Brasil.

Para conferir a programação e os casos práticos trabalhados na Oficina, basta conferir o Anexo (**Dossiê Oficina Prática**).

Organização do evento

1. Objetivo pedagógico

O principal objetivo da Oficina foi promover o intercâmbio de experiências horizontais entre Defensorias Públicas, dando maior protagonismo aos Defensores para debater os desafios da adequação do ente à LGPD e à implementação de programas de governança de dados. Nesse sentido, o evento reuniu integrantes de diferentes Defensorias brasileiras, as quais se encontram em estágios distintos de processos de adequação e apresentam inúmeras particularidades que afetam a implementação de seus programas. A pluralidade e as diferentes perspectivas sobre o tema foram fundamentais para a construção deste relatório que sintetiza esse rico debate entre os membros da instituição.

Assim, o evento se propôs a: (i) estabelecer uma rede de contatos entre integrantes de diferentes Defensorias Públicas engajados no processo de adequação; (ii) colaborar com a identificação de desafios particulares da instituição no tocante à implementação de um programa de governança de dados; (iii) colaborar com possíveis saídas de enfrentamento para os problemas identificados; (iv) identificar aspectos positivos de um programa de adequação que vão além da conformação legal e que contribuam com a missão institucional das Defensorias e; (iv) gerar materiais de pesquisa para a construção de documentos de suporte que poderão servir de apoio a todas as Defensorias do país e outros entes público.

2. Metodologia

Todos os temas abordados na Oficina são casos concretos compartilhados por diferentes Defensorias Públicas ao redor do Brasil. Foram constituídos dois comitês: um Comitê de Defensores formado por representantes das Defensorias envolvidos nos programas de adequação do ente à LGPD e um Comitê Executivo formado pelos pesquisadores da Associação Data Privacy Brasil de Pesquisa.

O Comitê de Defensores enviou à equipe do Data Privacy Brasil relatos sobre as experiências de seus respectivos órgãos durante o processo de adequação à LGPD. A partir da coleta e análise de experiências, os casos foram divididos em **três eixos temáticos**:

1. Estruturação do comitê de proteção de dados, desafios organizacionais, divisão de tarefas, nomeação de encarregado, programa de conscientização interna;

2. Atividade-meio, desafios relacionados ao tratamento de dados envolvidos nas atividades administrativas e gerenciais da Defensoria, incluindo registros de relatórios, tratamento de dados de defensores e servidores, segurança de sistemas informáticos, contratos e parcerias;

3. Atividade-fim, desafios relacionados ao tratamento de dados envolvidos nas atividades finais das Defensoria, incluindo triagem, registro em sistemas integrados, trocas de documentos e informações por aplicativos, etc.

3. Dinâmica do evento

A Oficina contou com a presença de cerca de 60 participantes, número estabelecido a fim de comportar uma média de ao menos dois representantes por cada Defensoria Estadual brasileira. Em virtude da pandemia e, também, pensando na inclusão de integrantes de diversas regiões, o evento teve duas horas de duração em cada dia e foi realizado remotamente através da plataforma Zoom.

Nos dois primeiros dias foram discutidos dois grandes tópicos, sendo que cada encontro foi estruturado em quatro partes:

1. **Primeira parte:** Apresentação dos tópicos identificados a partir do compartilhamento de casos.
2. **Segunda parte:** Apresentação de algumas das experiências relacionadas ao tópico e observadas pelos integrantes do comitê de Defensores.
3. **Terceira parte:** Discussão em grupos menores sobre alguns aspectos específicos a respeito de determinado tópico (apresentados em formato de casos), aqui ainda foi reservado um espaço para apresentações e feedbacks dos demais participantes.

4. **Quarta parte:** Considerações finais da equipe da Data Privacy sobre os pontos apresentados e discutidos.

No último dia de Oficina, os participantes discutiram de forma mais livre sobre os tópicos trabalhados anteriormente a partir dos enunciados elaborados de forma assíncrona.

O texto que segue abaixo representa um esforço de sistematização das discussões e experiências compartilhadas na Oficina, buscando sintetizar, no formato de enunciados, os principais entendimentos sobre os desafios e potencialidades da adequação à LGPD das Defensorias Públicas brasileiras. Cumpre destacar que o presente relatório expressa as diferentes visões e percepções dos participantes, porém, não reflete necessariamente a posição do Data Privacy Brasil.

Síntese das discussões

Ao longo dos três dias de Oficina, as principais reflexões e desafios identificados foram:

- Restrição de acesso ao sistema integrado e as implicações na rotina de trabalho do defensor;
- Padronização do cadastramento de informações em um sistema integrado e o potencial comprometimento da autonomia funcional dos defensores;
- Institucionalização do uso do *WhatsApp* e possíveis alternativas ao aplicativo para agendamento e atendimento remoto;
- Existência de duas categorias de dados pessoais (essenciais para o peticionamento x utilizados para fins de políticas públicas) e a atribuição de bases legais para tratamento (art. 7º e art. 11 da LGPD);
- Riscos do compartilhamento, com outros entes privados e públicos, de dados por meio de contratos e convênios e, portanto risco de violação aos princípios da finalidade e da transparência;
- Identificação do controlador x operador nas relações contratuais;

- Dificuldade de exercer o controle sobre o que é realizado com os dados compartilhados para fins de pesquisa;

- Definição das atribuições do Encarregado[4] e o papel do Comitê de Proteção de Dados no curso do processo de adequação;

1. Dinâmica do evento

Os sistemas integrados são ambientes digitais que concentram todas as informações necessárias à efetivação das atividades fim das Defensorias, ou seja, a atividade de atendimento e de ingresso com ações em nome dos assistidos. Esses sistemas, concentram dados cadastrais, dados da triagem e dados referentes aos casos, por exemplo documentos probatórios utilizados para ingressar com a ação.

As Defensorias Públicas brasileiras utilizam sistemas integrados de armazenamento e cadastro de dados pessoais dos usuários, por exemplo, o sistema Solar (Solução Avançada em Atendimento de Referência)[5]. Desenvolvido pela Defensoria Pública do Estado do Tocantins (DPE-TO), o Solar se tornou referência nacional, sendo amplamente utilizado pelas Defensorias de todo o país. Por sua vez, a Defensoria Pública do Estado do Rio de Janeiro utiliza o sistema Verde[6], enquanto a Defensoria de São Paulo trabalha com o sistema DOL[7].

4 O encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

5 O Solar compila informações desde o primeiro atendimento, registrando todo o histórico processual. Além disso, o sistema permite a checagem das informações do assistido por meio da realização de cadastro, bem como o acesso a documentos, à matéria do caso, e a peças processuais. Existe ainda a possibilidade da criação de agendas dos atendimentos, com a inserção de datas e prazos, a produção de relatórios e obtenção de dados estatísticos, como número total de atendimentos, ou número de atendimentos de determinada natureza, por exemplo. Fonte: <https://www.defensoria.ro.def.br/site/index.php/componente/content/article/1-ultimas-noticias/1754-2018-07-23-19-52-01>.

6 O Sistema Verde foi criado por técnicos da Coope/UFRJ com a finalidade de oferecer à Defensoria do Rio ferramentas de informática capazes de integrar rotinas e procedimentos de todos os órgãos de atuação. O sistema tem como objetivo automatizar tarefas repetitivas e registrar e organizar informações que os defensores públicos recebam e produzam, além de tornar possível a formulação de estatísticas, importação de dados de outros sistemas e, consequentemente, dispensa de buscas e pesquisas de dados em outros ambientes. Fonte: <https://defensoria.rj.def.br/noticia/detalhes/3883-Sistema-Verde-e-apresentado-aosdefensores-de-primeiro-atendimento>.

7 O sistema DOL é um conjunto de módulos de sistemas computacionais com finalidade de organizar e armazenar dados cadastrais e processuais, oficiais e de mero expediente, referentes aos usuários, Unidades e Regionais da Defensoria Pública. O DOL foi desenvolvido a partir de três premissas: usabilidade,

Esses sistemas trouxeram mudanças significativas para a rotina de trabalho dos defensores uma vez que permitem a centralização das informações, otimizando as atividades empenhadas. Tendo em vista que a unidade é um princípio institucional, é fundamental que todas as informações sejam registradas e possam ser acessadas por todos.

Um único repositório de informações garante maior governabilidade, reduzindo as chances de eventuais duplicidades e inconsistências do cadastro de modo que o princípio da qualidade dos dados pessoais seja respeitado. Ao mesmo tempo, entende-se que há um risco atrelado a esse benefício, qual seja o de garantir o controle de acesso às informações inseridas nesses sistemas. Uma solução para esta falha é estabelecer um gerenciamento de identidade para acesso ao sistema.

Nesse contexto, as Defensorias enfrentam no seu dia-a-dia alguns desafios quanto ao acesso ao sistema, bem como quanto à padronização e centralização do cadastramento.

Principais preocupações e riscos identificados

- Possibilidade da Defensoria atender partes distintas de um mesmo processo, o que em determinadas circunstâncias gera receio dos defensores de inserir certas informações em sistemas integrados e abertos a outros membros da instituição;
- Receio de que as informações confiadas pelo usuário dos serviços da Defensorias possam ser utilizadas em seu desfavor pela própria instituição.

    - **Exemplo 1**: Em processo de alimentos, ambas as partes são representadas por membros da Defensoria. Um defensor acessa o sistema e obtém os dados da parte adversa sobre a renda.
    - **Exemplo 2**: Em uma situação que os dados de residência de um atendimento sejam utilizados para realizar a citação do próprio usuário em outro processo ou dados de vínculo empregatício sejam utilizados para indicar a possível penhora de verbas.

- A padronização de cadastramento de informações, dificuldade de estabelecer o mínimo de informações que deve ser coletado, bem como o acesso

otimização das informações e produção de dados estratégicos e foi estruturado em três grandes áreas: (1) atendimentos; (2) acompanhamento de processos e seus respectivos atendimentos e (3) atividades administrativas relacionadas diretamente à atividade fim. Fonte: <https://www.defensoria.sp.def.br/dpesp/Repositorio/0/Documentos/Manual%20Defensoria%20Online%20-%20fev2014.pdf>.

ao sistema integrado pode afetar a autonomia funcional dos defensores. Em muitas Defensorias, cada Defensor dispõe de liberdade para determinar se um caso deveria ter acesso mais restrito ou não, tratando-se de uma escolha notadamente individual.

- Fomento ao uso dos sistemas criados para integrar o tratamento de dados. Muitos defensores ou pessoas em cargos administrativos, podem utilizar programas próprios, com os quais já existe familiaridade como o Pacote Office, para tratar os dados pessoais e existe resistência à mudança dessa cultura de "autonomia".
- Dificuldade de mobilizar os defensores para responder a outros dados pessoais que podem gerar a produção de políticas públicas, e que não necessariamente são utilizados para o atendimento do usuário
- Perigo de desumanização do atendimento quando há a opção pelo Chatbot para o atendimento;
- Servidores de aplicativos de mensagens como o *Whatsapp*;
- Autenticação do titular de dados que está pedindo informações às Defensorias. Existem hipótese nas quais o usuário da Defensoria se encontra impedido de solicitar informações diretamente à instituição de modo que seus familiares ou demais interessados no caso fazem as solicitações em nome do usuário. Nesses casos, existe o desafio de autenticar a titularidade dos dados pessoais, bem como do vínculo entre o solicitante e o usuário.

Medidas de mitigação de risco sugeridas

- Criação de restrições conforme a área e nível de atuação, estabelecendo critérios granulares (Ex: diferenciar acesso de quem está alocado na área civil e criminal ou diferenciar estagiário, servidor e defensor);

- Construção de Perfis de Acesso;

- Imposição de sigilo em determinados procedimentos, para que somente o defensor ou acessor daquela área específica pode acessar o procedimento;

- Utilização de ferramentas como logs de acesso que tornam possível identificar quem acessou determinado procedimento.

- Buscar acordos institucionais entre a empresa e a Defensoria.

- **Exemplo:** Estabelecer um acordo institucional entre a Defensoria Pública e o *Whatsapp* para a garantia do direito à proteção de dados dos cidadãos.

Observação: Destacou-se que não necessariamente deve-se replicar o mesmo procedimento de sigilo adotado pelos tribunais de justiça.

Tendo em mente os desafios em questão, os participantes elaboraram o enunciado abaixo:

Enunciado

Art 6º, caput e incisos: Os usuários de um sistema integrado da Defensoria Pública precisam ter perfis de acesso limitados aos casos vinculados às respectivas atribuições do cargo, a fim de que sejam respeitados os princípios da prevenção e da segurança no tratamento de dados pela Defensoria. Os times de segurança da informação devem implementar respectivos controles e sistemas de gerenciamento de identidades.

2. Atendimento remoto

Afora a quantidade massiva de atendimentos e, consequentemente, de dados pessoais tratados, ainda deve-se somar o processo de digitalização da sociedade. Acelerado pela crise do COVID 19, esse processo acentua uma série de desigualdades e torna extremamente desafiador o trabalho das Defensorias Públicas, no Brasil, sendo uma das consequências imediatas do isolamento social a necessidade de digitalização de seu atendimento.

A instituição, sem uma grande disponibilidade de ferramentas tecnológicas próprias para tanto, se viu obrigada a encontrar soluções alternativas disponíveis no mercado, as quais eram, muitas vezes, financeiramente bancadas pelos próprios defensores[8]. Nesse contexto, a principal ferramenta utilizada foi o *WhatsApp*,

8 ZANATTA, Rafael; KITAYAMA, Marina. O desafio da LGPD para as Defensorias Públicas no Brasil. In. Lei Geral de Proteção de Dados e o Poder Público. Organizadores: Daniela Copetti Cravo, Daniela Zago

que funciona como um portal de acesso à instituição. Por meio da ferramenta, os usuários entram em contato com a Defensoria Pública, agendam atendimento, esclarecem dúvidas e enviam documentos e demais informações pessoais.

Assim, a utilização do *WhatsApp* tem sido uma das grandes aflições desde a entrada em vigor da LGPD na medida em que alguns defensores não conseguem visualizar um cenário em que não se utilize a ferramenta. As Defensorias Públicas brasileiras vivem o seguinte dilema: Considerando que o *WhatsApp* é uma ferramenta acessível e democrática, o que facilita o acesso à Justiça, caberia às Defensorias Públicas abandonarem o atendimento e agendamento via *WhatsApp*?

Pensando em enfrentar tal desafio, elaboraram o seguinte enunciado:

Enunciado

Art 6º, caput e incisos: O uso de aplicativos de comunicação para contato com usuários da Defensoria Pública deve ser realizado com observância aos princípios da segurança e prevenção (art. 6º, incisos VII e VIII da LGPD).

A utilização de tais aplicativos deve ser regulamentada pela instituição, a fim de que sejam adotadas boas práticas para prevenir incidentes, como a utilização de autenticação de dois fatores e a exclusão periódica de documentos e informações pessoais armazenadas em nuvem.

PARA REFLETIR

- Seria possível criar uma política de uso para utilização do *WhatsApp*? Ex. Nenhum número de *WhatsApp* pessoal seria utilizado, somente o número institucional;
- Quem seria responsável pela regulamentação do uso de aplicativos de mensageria? O encarregado ou a própria Defensoria Pública por meio de resolução?
- A regulamentação também seria aplicável para a comunicação entre defensores e não somente entre defensor e usuário?
- Considerando o compartilhamento de dados entre o *WhatsApp* e o *Facebook*, caberia à Defensoria Pública avisar o usuário sobre o compartilhamento, já que

Gonçalves da Cunda e Rafael Ramos. Tribunal de Contas do Estado do RS. Prefeitura de Porto Alegre Porto Alegre. 2021. p. 171 - 183.

utiliza a ferramenta como principal meio de comunicação?

- Tem se observado uma tendência de desenvolvimento de aplicativos próprios pelas Defensorias Públicas com eventual integração com o *WhatsApp*;
- Ainda haveria a necessidade de se utilizar o *WhatsApp* se fosse desenvolvido um aplicativo de fácil navegabilidade e compreensão pelas Defensorias?

Trocando experiências

Como uma alternativa ao *WhatsApp*, a Defensoria Pública do Estado de São Paulo adotou a ferramenta de *chatbot* (*LiveChat*) na página inicial da Defensoria. A ferramenta, lançada em agosto de 2020, busca agilizar e garantir um atendimento mais célere e dinâmico, diminuindo também a necessidade de deslocamentos físicos a prédios da Defensoria, que, em razão da pandemia de Covid-19, recebem apenas atendimentos agendados e em número reduzido. O assistente virtual "DEFI" é um sistema de conversa online (chat) com respostas automatizadas por meio de inteligência artificial, criado para receber informações básicas dos usuários da Defensoria (ex: nome, CPF e renda familiar), compreender a demanda e encaminhar à unidade competente para atendimento. Por meio desse sistema, os usuários podem optar por um dentre os horários e datas disponíveis na agenda da unidade e marcar seu atendimento. Feito o agendamento, a pessoa recebe uma senha para acesso a um chat com a equipe de atendentes da Defensoria na data e no horário marcados, por meio do qual é possível também enviar e receber documentos[9].

A Defensoria Pública de Mato Grosso do Sul, por outro lado, buscou desenvolver uma plataforma para buscar desencorajar o uso do *WhatsApp*, mas enfrentou um grande problema de analfabetismo digital. O sistema funcionaria a partir do cadastro do assistido no site da defensoria, e, precisaria validar os dados por e-mail, o que é uma raridade entre os assistidos As pessoas até chegaram a criar e-mails,

9 Disponível em: <https://www.defensoria.sp.def.br/dpesp/Conteudos/Noticias/NoticiaMostra.aspx?idItem=92057&idPagina=1&flaDestaque=V>. Acessado em 16 de setembro de 2021.

> apesar da dificuldade mas, depois começaram a esquecer as senhas inseridas no cadastro no site da Defensoria para o envio dos documentos. Isso acabou por gerar um grande número de requerimentos de reformulação do acesso e isso ocupou o setor de tecnologia da informação dessa unidade da defensoria durante dias.

É importante destacar que a utilização do *WhatsApp* envolve uma discussão eminentemente estrutural e de monopólio de grandes empresas de tecnologia. Assim, uma regulamentação e diretiva de boas práticas precisam ser encaixadas numa discussão mais ampla do que significa utilizar *WhatsApp* para prestação de serviços públicos. No entanto, isso não significa abolir completamente a utilização da ferramenta uma vez que existem outros fatores em jogo quando se fala de acesso à justiça.

Bases legais para o atendimento ao usuário

Um dos maiores desafios em qualquer processo de adequação à LGPD é a atribuição das bases legais - e não seria diferente para as Defensorias Públicas.

As bases legais são "*pré-condições jurídicas que precisam ser cumpridas para que o controlador possa tratar os dados de forma lícita*"[10] e se encontram no rol específico dos arts. 7º e 11 da Lei. Portanto, a LGPD impôs um modelo de regulação ex ante, ou seja, o controlador precisa identificar e documentar a base legal para então realizar o tratamento de dados licitamente.

Nesse ponto, é importante destacar que não há hierarquização ou priorização entre as bases legais. Por exemplo, o consentimento é uma base legal bastante conhecida, mas, em muitos casos, não é a mais adequada.

No caso particular das Defensorias Públicas, no qual o usuário se encontra em uma situação de maior vulnerabilidade socioeconômica, dificilmente o consentimento será livre, informado e inequívoco, conforme exigido na LGPD. Portanto,

10 BIONI, Bruno; ZANATTA, Rafael; KITAYAMA, Marina. Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021.

no contexto das Defensorias Públicas, a base legal do consentimento apresenta três principais desafios que devem ser levados em conta[11]:

1. As desigualdades sociais existentes no Brasil implicam a ausência de letramento da população sobre o tratamento de dados pessoais. A complexidade das informações disponibilizadas, bem como a utilização de conceitos técnico-jurídicos muito específicos dificultam a plena compreensão dos usuários das Defensorias e, consequentemente, a obtenção do consentimento de acordo com os termos da Lei;

2. A quantidade e a velocidade de informações trafegadas inviabilizam a tomada de decisão plenamente consciente;

3. A etapa de obtenção do consentimento inequívoco e informado para cada cidadão atendido implicaria uma demora sem sentido no fluxo de demandas urgentes.

Nessa linha, Rodrigo Pacheco, Defensor Público-Geral do Estado do Rio de Janeiro, sustenta que "*o consentimento do usuário é dispensável na atividade da Defensoria quando do atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.*"

Tendo isso em vista, os participantes da Oficina elaboraram o seguinte enunciado:

Enunciado

Arts. 7º e 11: O consentimento é uma base legal mais arriscada para legitimar o tratamento de dados necessários ao início ou prosseguimento de atendimento. Em vista da condição de vulnerabilidade e assimetria do usuário frente às Defensorias, dificilmente seu consentimento seria livre e, por conseguinte, válido.

11 Ibid.

3. Convênios e contratos

Comumente as Defensorias firmam uma série de parcerias, contratos e convênios, com cartórios, órgãos do governo em diferentes níveis da federação, universidades e centros de pesquisa, empresas e entidades de terceiro setor. Naturalmente cada caso deve ser analisado cuidadosamente na medida em que o volume, a natureza dos dados envolvidos, bem como a finalidade de cada parceria varia e, com isso, as medidas a serem adotadas também irão variar.

No caso de algumas defensorias, foi mencionada a existência de comitês específicos de pesquisa e, quando isso ocorre, seria importante estabelecer padrões comuns de como esse grupo poderia lidar com os pedidos de compartilhamento de dados que são viabilizados pelo comitê.

Durante os encontros foi mencionada a inserção dos terceiros na posição de operador, e não de co-controlador ou controlador independente, para que esses terceiros fiquem inteiramente vinculados às diretrizes da defensoria pública. Além disso, foi mencionada a boa prática de enviar a s bases de dados já anonimizadas.

Ao longo da Oficina, foram identificadas duas principais questões que envolvem o tema de convênios e contratos:

1. **Finalidade:** O compartilhamento de dados das Defensorias com terceiros envolve desafios técnicos e administrativos no tocante ao controle sobre a utilização dos dados e finalidade do tratamento. Em outras palavras, fiscalizar se o terceiro está cumprindo com os termos do contrato ou convênio não é uma tarefa simples.

2. **Revisão de cláusulas contratuais:** É necessário rever todas as cláusulas dos contratos e convênios já firmados a fim de fazer os ajustes necessários à nova realidade de proteção de dados. Além disso, a revisão contratual é fundamental para determinação das finalidades de uso dos dados acessados, responsabilidades e deveres das partes envolvidas, bem como para a identificação dos agentes de tratamento como operador, controlador e co-controlador.

3. **Responsabilidade:** para além da definição de controlador, ope-

rador e etc. Notou-se a importância de definir como fica a responsabilização no caso de um incidente de segurança ou outras situações de ilicitude ou desconformidade provocadas pelo uso dos dados por esses terceiros. Mais do que isso, estipular deveres de notificação, bem como planos de gestão de incidentes de segurança a cargo de cada um dos agentes que fazem parte da cadeia de tratamento de dados.

Assim, recomenda-se que no momento de elaborar as políticas de convênios deve-se levar em conta: (i) quais os dados são compartilhados, (ii) o fluxo de dados, (iii) quais as finalidades e (iv) quais as bases legais que sustentam esse compartilhamento.

Principais preocupações e riscos identificados

- Possibilidade de vazamento dos dados;
- Desvio de finalidade;
- Duplicação da base de dados para posterior utilização para outros propósitos;
- Dificuldade de exercer controle sobre o acesso e restrição ao banco de dados, diante do fornecimento de um único acesso compartilhado entre os terceiros;
- Ausência de transparência a respeito da transferência dos dados para outros atores;
- Ausência de consentimento dos assistidos para realização do compartilhamento. Ex. Quando o compartilhamento se dá entre entes que têm uma atribuição funcional oposta a da defensoria, como órgão de segurança pública;
- Ausência de regulação da transferência de dados pessoais públicos para entes privados.

Medidas de mitigação de risco sugeridas

- Incluir cláusula de delimitação de responsabilidades e indicação detalhada das finalidades do tratamento de dados;
- Prever cláusulas de responsabilidade exclusiva do agente caso ele descumpra com aquilo determinado contratualmente;
- Na revisão contratual, deve-se levar em conta, para fins de priorização, o

volume e a sensibilidade dos dados objeto do compartilhamento (priorizar contratos nos quais há o compartilhamento de dados sensíveis);

- Na revisão contratual, deve-se levar em conta, para fins de priorização, o volume e a sensibilidade dos dados objeto do compartilhamento (priorizar contratos nos quais há o compartilhamento de dados sensíveis);
- Na hipótese de compartilhamento com instituições de pesquisa é fundamental que se preste informações sobre a natureza da pesquisa, financiamento, metodologia e os objetivos pretendidos, principalmente no sentido de garantir a confiabilidade da pesquisa e dessa instituição/pesquisador para os quais os dados são transferidos;
- Sempre que possível deve-se proceder à anonimização de modo que somente dados como números e percentuais sejam repassados[12];
- Expor o tipo de tratamento de compartilhamento para pesquisa, por exemplo, nas Políticas de Privacidade das Defensorias ou no próprio termo de hipossuficiência como forma de dar transparência ao tratamento.

PARA REFLETIR

- As Defensorias recebem e tratam muitos dados vindos de terceiros estranhos à organização. Por exemplo, a instituição tem acesso à base de dados do SUS e de concessionárias de água e energia. No entanto, ultimamente os defensores têm recebido notificações no sentido de que não terão mais acesso aos dados em razão da LGPD. Como isso afeta o trabalho das Defensorias em garantir assistência aos mais vulneráveis?
- Para realizar empréstimo consignado, a Defensoria compartilha dados dos defensores com ferramentas de consignação. A Defensoria faz um termo de consignação com uma instituição privada que operacionaliza o processo, fazendo a ponte entre o servidor e o órgão público. Isto é, existe um convênio feito entre a administração superior e a empresa que oferece o software, permitindo que os dados dos defensores sejam coletados e compartilhados com as instituições financeiras. Tendo em vista que essa prática ocorre sem o consentimento do servidor, haveria violação à LGPD?

12 Em razão da falta de recursos humano e financeiro, os participantes destacaram que ainda existem desafios técnicos e práticos para a implementação de medidas de anonimização de forma segura e eficiente. Contudo, recomenda-se prosseguir com a anonimização sempre que possível.

Caracterização do controlador, operador e co-controlador

A identificação dos papéis de controlador e operador é uma etapa fundamental quando falamos de contratos e convênios. Determinar "quem é quem" na relação contratual é imprescindível para a atribuição dos deveres e responsabilidades dos agentes de tratamento.

De acordo com a LGPD, o **controlador**, pessoa natural ou jurídica, é o sujeito a quem compete a tomada de decisões referentes ao tratamento: finalidades, condições e meios de processamento de dados pessoais[13].

Já o **operador**, pessoa natural ou jurídica, de direito público ou privado, é responsável por executar tarefas específicas com o objetivo de atingir metas previamente definidas pelo controlador[14]. Falta ao controlador autonomia para alterar os meios e finalidade do tratamento de modo que este se coloca em uma posição de subordinação[15]. Seria o caso, por exemplo, de um convênio por força do qual a defensoria pública utiliza dados pessoais para uma finalidade definida por um terceiro com quem tem convênio. Nesse caso, se houver uma finalidade própria da defensoria, que extrapola o convênio, ela se tornaria controladora dos dados pessoais.

Pensando nisso, os participantes fizeram os seguintes comentários:

> Na grande maioria dos convênios, a Defensoria seria a controladora. A única hipótese para co-controladoria seria a de convênios entre duas Defensorias dentro do escopo de um projeto conjunto;
> Em se tratando de compartilhamento de dados para fins de pesquisa, sugere-se a utilização de cláusulas "guarda-chuva" de maneira que nos contratos de convênio a Defensoria e o conveniado figurem como co-controladores;
> De toda forma, foi feita a ressalva de que se deve analisar caso a

13 KREMER, Bianca. Os agentes de tratamento de dados pessoais. In: A LGPD e o Novo Marco Normativo no Brasil. Org. Caitlin Mulholland. Porto Alegre: Arquipélago, 2020. p. 290.

14 Ibid. p. 305.

15 Sobre os métodos para identificar o poder de influência nas atividades de tratamento de dados, consultar o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado" da Autoridade Nacional de Proteção de Dados Pessoais.

caso. A análise individualizada dos casos concretos permite identificar se as entidades públicas e privadas envolvidas no contrato também podem tomar decisões acerca do tratamento de dados, caso no qual devem ser consideradas co-controladoras.

Esse arranjo beneficia as Defensorias Públicas e, em última análise, o próprio cidadão uma vez que divide e aloca a responsabilidade de acordo com o poder de cada agente envolvido na operação.

4. Programa de adequação

A adequação à LGPD deve ser encarada não somente como uma obrigação legal, mas também como uma janela de oportunidade[16]. Assim, a conformidade à LGPD força as instituições a se organizarem, a reverem processos, a verificarem o fluxo de dados e as razões do tratamento. Essa visão ampla fornecida pelo processo de adequação pode influenciar diretamente na rapidez da resposta a situações de incidente de segurança, mau uso dos dados pessoais e/ou alocação de recursos de tecnologia da informação, ou seja, o programa de adequação tem muito a contribuir com o processo de gestão administrativa da organização.

A Defensoria Pública, como instituição permanente e essencial à função jurisdicional do Estado, apresenta suas particularidades e, portanto, seus programas de governança de dados não podem ser construídos a partir de modelos, templates, tabelas prontas e documentos ao estilo "copia e cola" produzidos pelo setor privado[17]. Em outras palavras, não se trata de simplesmente adaptar o método observado na iniciativa privada, mas sim de uma indispensável customização dos projetos de adequação à Lei Geral de Proteção de Dados Pessoais, levando em considerando as especificidades das Defensorias e a importância dos dados pessoais para atividades-meio e atividades-fim[18].

16 BIONI, Bruno. A Era dos Dados: Inovar pela Lei. GV - Executivo. Vol. 18. nº 4. Julho/Agosto 2019 Disponível em: <https://brunobioni.com.br/home/wp-content/uploads/2019/08/gv_0184ce5.pdf>.

17 ZANATTA, Rafael; KITAYAMA, Marina. O desafio da LGPD para as Defensorias Públicas no Brasil. In. Lei Geral de Proteção de Dados e o Poder Público. Organizadores: Daniela Copetti Cravo, Daniela Zago Gonçalves da Cunda e Rafael Ramos. Tribunal de Contas do Estado do RS. Prefeitura de Porto Alegre Porto Alegre. Disponível em: <https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf>.

18 Ibid. p. 181.

Considerando tais desafios, os participantes elencaram as duas principais prioridades do processo de adequação:

1. Criar um comitê ou indicar o encarregado para então...
2. Realizar o mapeamento mais aprofundado sobre os fluxo de dados da instituição

Criação de comitê de proteção de dados e indicação de encarregado

A complexidade institucional das Defensorias Públicas, bem como a quantidade massiva de dados tratados denuncia a necessidade da instituição indicar um Encarregado, aquele responsável pelo tratamento das informações do controlador. A complexidade das funções atribuídas ao encarregado de proteção de dados, face ao volume de atividades que os defensores públicos realizam no seu dia a dia, destravou, em São Paulo, a criação de um órgão colegiado para endereçar a função. Nesse caso, é o próprio comitê, que de forma conjunta, endereça as atribuições de um encarregado de proteção de dados.

Entretanto, mesmo que o comitê não tenha sido criado, inicialmente, para endereçar essa função, a complexidade do projeto de adequação de uma defensoria sugere também a importância de instituição deste grupo de proteção de dados, o que permitiria uma atuação mais capilarizada do programa sobre as diferentes frentes de trabalho das Defensorias.

A LGPD traz a obrigatoriedade de indicação de um Encarregado, mas não de um comitê nos termos mencionados, mas, destacamos a relevância desse órgão interno[19], por ser esta uma boa solução para iniciar um projeto de governança e uma boa prática, nos termos do artigo 50 da LGPD.

A função do comitê é a de gerir o programa de adequação: o grupo será responsável pela verificação das obrigações legais e regulatórias do ente, por acon-

19 Em Santa Catarina, o Comitê Gestor de Proteção de Dados Pessoais - CGPDP foi instituído no Tribunal de Justiça de Santa Catarina pela Resolução GP n. 28/2019. É formado por uma equipe multidisciplinar, composta de magistrados e servidores, que cumulam as suas atividades ordinárias com aquelas do Comitê. O CGPDP está vinculado à Presidência do Tribunal de Justiça, que desempenha o papel de controlador de dados, nos termos da LGPD. No Rio de Janeiro, o presidente do Tribunal de Justiça do Rio de Janeiro, Claudio Mello, designou os integrantes do Comitê Gestor de Proteção de Dados Pessoais (CGPDP) em setembro de 2020. O CGPDP será presidido pelo desembargador Arthur Narciso de Oliveira Neto e coordenado pelo juiz-auxiliar da presidência do TJ-RJ Fábio Porto. Também compõem o comitê os juízes Gustavo Quintanilha de Menezes (auxiliar da Corregedoria Geral de Justiça), Afonso Henrique Barbosa (auxiliar da presidência do TJ) e Aroldo Pereira Junior.

selhar os diferentes setores da Defensoria sobre o tema da proteção de dados, além de administrar funções técnicas (sistemas e TI, por exemplo) e supervisionar a execução das etapas do programa e o atendimento aos requisitos de conformidade estabelecidos[20]. É importante mencionar, que durante os exercícios práticos identificou-se a necessidade de um comitê para o momento inicial da adequação e outro comitê para destravar o monitoramento contínuo e atualização da estrutura de governança de dados criada inicialmente (esse segundo comitê seria aquele que mais tem a ver com as funções de encarregado).

Eventualmente, esse comitê ou parte dele, pode endereçar conjuntamente as funções do encarregado de proteção de dados, conforme exposto anteriormente. Contudo, é importante destacar que algumas defensorias não enxergam essa possibilidade de colegiado diante da redação da lei, que lhes parece individualizar o cargo de encarregado de proteção de dados.

Ainda, foi mencionada a dificuldade de se criar um novo cargo ou órgão diante do estrangulamento orçamentário vivenciado por algumas unidades da defensoria pública no cenário atual, como foi o caso da Defensoria de Pernambuco. Além disso, menciona-se a falta de diretiva interna e normativas para orientar a criação do comitê, de utilizar aplicativos de comunicação ou de criação de um comitê para promover a adequação. No caso da nomeação do encarregado, durante a resolução dos exercícios práticos, no dia 07 de julho, foi mencionada a possibilidade de que o Defensor Público-Geral ou o Conselho Superior realizasse essa nomeação.

PARA REFLETIR

- A criação de políticas não é responsabilidade exclusiva do Encarregado. Existe um processo de adequação propriamente dito e outro de manutenção e atualização das políticas de governança (este último caberia ao Encarregado).
- As Defensorias Públicas podem criar órgãos para serem encarregados, sendo fundamental que os comitês sejam diversificados.
- Deve haver uma relação de proximidade entre o Encarregado e a estrutura da

20 BIONI, Bruno; ZANATTA, Rafael; KITAYAMA, Marina. Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2021/06/guia_adequacao_defensorias_vf.pdf>.

Ouvidoria, tendo em vista que é o encarregado responsável por responder as requisições de direitos dos titulares.

- Quanto às atribuições do Comitê de Proteção de Dados, este deve atuar como protetor de dados da instituição, ouvindo e fiscalizando internamente a instituição.
- Comitê de implementação da LGPD x Comitê de monitoramento: Há uma distinção entre o comitê responsável pela adequação e o comitê que atua continuamente atualizando e supervisionando a aplicação das políticas de governança. O comitê de implementação da LGPD atua ao longo do processo de adequação, já o outro comitê realiza o monitoramento das atividades de tratamento de dados da instituição.

Criação de comitê de proteção de dados e indicação de encarregado

Quanto ao mapeamento, os participantes entenderam ser fundamental responder às seguintes perguntas de acordo com as etapas do mapeamento:

1. Quais canais serão utilizados para a coleta de dados?
2. Qual é o local de tratamento do dado para a partir disso pensar no fluxo?
3. Qual é o local de armazenamento?
4. Qual a finalidade de determinada operação de tratamento?

PARA REFLETIR

- Destacou-se a existência de duas categorias de dados:
  Aqueles essenciais para o peticionamento;
  Aqueles utilizados para fins de políticas públicas.
- Os dados utilizados para fins de políticas públicas também podem ser utilizados posteriormente para defesa da tutela coletiva.
- A melhor forma de obter informações acerca dos processos de cada área é através de entrevistas com os respectivos responsáveis.

Considerações finais

A adequação à proteção de dados pessoais no sistema de justiça encontra especificidades que são próprias do poder público em uma dimensão republicana. Conforme nos ensina Miriam Wimmer, "*no setor público, o tratamento de dados pessoais não se inicia, em geral, a partir de uma decisão voluntária do titular, mas como decorrência das exigências do próprio pacto social*"[21]. Não à toa, a Constituição Federal atribuiu às Defensorias Públicas o papel primordial de defesa de direitos e garantias fundamentais, o que naturalmente inclui aqueles relacionados à proteção de dados.

Com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais, algumas Defensorias Públicas iniciaram um pioneiro processo de internalização dos valores da proteção de dados pessoais em viés estratégico. Em 2021, diversos processos ocorreram paralelamente, como (i) criação de comitês de adequação dentro das Defensorias Públicas, (ii) publicação de Guias de Adequação para Defensorias Públicas, (iii) publicação de livros específicos sobre LGPD no Poder Público, (iv) realização de seminários de formação com Defensores Públicos e (v) intercâmbio e trocas de experiências entre Defensores sobre aspectos práticos da LGPD.

As Oficinas realizadas entre julho e agosto de 2021 revelaram a centralidade da proteção de dados pessoais como aspecto de justiça e efetivação de direitos na relação entre Defensorias e cidadãos. A instituição guarda uma quantidade expressiva de dados pessoais, muitos dos quais sensíveis. Considerando o perfil dos usuários das Defensorias, os dados tratados pela instituição merecem um cuidado especial dado seu potencial discriminatório. As pessoas atendidas pelo órgão são socioeconomicamente vulneráveis o que torna elas ainda mais suscetíveis de sofrer pelo uso abusivo de dados pessoais, seja em virtude de processos de tomada de decisões automatizadas discriminatórias, seja em virtude do assédio de empresas que colocam a privacidade de seus consumidores em detrimento do acesso "gratuito" de serviços.

Nesse sentido, a instituição possui duas missões no tocante à proteção de dados pessoais: a primeira, relaciona-se com a adequação do órgão às exigências legais; já a segunda, refere-se à proteção dos cidadãos por meio da tutela coletiva e da atuação direta em novos casos individuais que envolvam proteção de dados pessoais.

21 WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades. Revista dos Advogados da AASP, n. 144, nov., 2019, p. 127.

Este documento apresentou nossos esforços de sistematização das discussões travadas ao longo dos três encontros. A Oficina foi um espaço de aprendizagem horizontal que permitiu aos Defensores e servidores compartilharem suas experiências e percepções sobre os desafios impostos pela LGPD. Acreditamos que a construção conjunta é a chave para pavimentar o caminho rumo à disseminação da cultura de proteção de dados dentro e fora da instituição.

As Oficinas trouxeram à tona a necessidade de (i) construir mecanismos e ferramentas de trocas constantes de experiências práticas entre Defensores na adequação à LGPD, (ii) dar visibilidade a ideias inovadoras e experimentações conduzidas pelos Defensores Públicos no processo de adequação à LGPD e (iii) produzir documentações e estudos, em formato aberto e de forma transparente, sobre rotinas, processos e projetos formulados em contextos específicos e as dificuldades de adaptação de arranjos organizacionais em Defensorias que operam em territórios distintos e com condições institucionais e de recursos humanos variantes.

Bibliografia recomendada

BIONI, Bruno; JÚNIOR, Florisvaldo Fiorentino; KITAYAMA, Marina; PACHECO, Rodrigo Baptista; ZANATTA, Rafael. LGPD e sistema de Justiça: a voz e a vez das Defensorias Públicas. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-e-sistema-de-justica-a-voz-e-a-vez-das-defensorias-publicas-09062021>.

BIONI, Bruno; ZANATTA, Rafael; KITAYAMA, Marina. Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2021/06/guia_adequacao_defensorias_vf.pdf>.

BIONI, Bruno Ricardo. Inovar pela lei. GV EXECUTIVO, v. 18, n. 4, p. 30-33, 2019. Disponível em: <https://rae.fgv.br/sites/rae.fgv.br/files/gv_0184ce5.pdf>.

CERIONI, Clara. Assistentes virtuais aceleram modernização tecnológica nas Defensorias Públicas. Disponível em: <https://www.jota.info/coberturas-especiais/inova-e-acao/assistentes-virtuais-modernizacao-defensorias-publicas-05012021>.

GOMES, Rodrigo Dias de Pinho; ZANATTA, Rafael. Carregando o piano? Notas sobre o encarregado de dados no setor público. 22 de julho de 2021. Disponível em: <https://www.migalhas.com.br/depeso/348961/notas-sobre-o-encarregado-de-dados-no-setor-publico>.

PACHECO, Rodrigo Baptista. LGPD e Defensoria Pública: uma análise da necessidade do consentimento. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-defensoria-publica-uma-analise-da-necessidade-do-consentimento-14042021>.

WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades. Revista dos Advogados da AASP, n. 144, nov., 2019, p. 127. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>.

ZANATTA, Rafael; KITAYAMA. Os desafios da LGPD para as Defensorias Públicas no Brasil, in: CRAVO, Daniela et al. A LGPD no setor público. Porto Alegre: Centro de Estudos Municipais, 2021, p. 172-185.Disponível em: <https://t.co/Oa0C5iwqRp?amp=1>.

ZANATTA, Rafael. Tutela coletiva e coletivização da proteção de dados, in: PALHARES, Felipe (org.). Temas Atuais de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2020, p. 345-374. Disponível em: <https://www.researchgate.net/profile/Rafael-Zanatta/publication/350852661_Tutela_coleti-va_e_coletivizacao_da_protecao_de_dados_pessoais/links/60764caf92851cb4a9dc18e6/Tutela-coletiva--e-coletivizacao--da-protecao-de-dados-pessoais.pdf>.

PRESA NA REDE DE PROTEÇÃO SOCIAL

PRIVACIDADE, GÊNERO E JUSTIÇA DE DADOS NO PROGRAMA BOLSA FAMÍLIA

PRESA NA REDE DE PROTEÇÃO SOCIAL - PRIVACIDADE, GÊNERO E JUSTIÇA DE DADOS NO PROGRAMA BOLSA FAMÍLIA[1]

MARIANA GIORGETTI VALENTE[2]
NATÁLIA NERIS[3]
NATHALIE FRAGOSO[4]

RESUMO

O artigo analisa o Programa Bolsa Família (PBF) como uma "cadeia de valor da informação" e observa, a partir de elementos colhidos em entrevistas e denúncias, aspectos de justiça de dados e impactos da datificação do programa sobre suas beneficiárias, sobretudo quanto à privacidade e ao gênero. Na análise, são consideradas as dimensões procedimental, de direitos e distributiva ao longo da cadeia de dados que informa e alimenta o PBF.

PALAVRAS-CHAVE

Privacidade; justiça de dados; Programa Bolsa Família; proteção social; desigualdade

1 Originalmente publicado em VALENTE, Mariana, NERIS, Natália e FRAGOSO, Nathalie. "Presa na Rede de Proteção Social: privacidade, gênero e justiça de dados no Programa Bolsa Família". Novos estudos CEBRAP, Vol. 40(1), 2021, pp.11-31.

2 Centro Brasileiro de Análise e Planejamento, São Paulo, SP, Brasil. E-mail: mariana@internetlab.org.br.

3 Universidade de São Paulo, São Paulo, SP, Brasil. E-mail: nerisnatalia@gmail.com.

4 Universidade de São Paulo, São Paulo, SP, Brasil. E-mail: nathalie.fragoso@gmail.com.

ABSTRACT

The article analyzes the Bolsa Família Program as an "information value chain" and observes, drawing from interviews and citizen complaints, data justice aspects and impacts of datafication of the cash transfer program for its beneficiaries, in particular regarding privacy and gender. In the analysis, the procedural, the right-s-based and distributive dimensions along the information chain that informs and feeds the PBF are considered.

KEYWORDS

Privacy; *data justice*; *Bolsa Família Program*; *social protection*; *inequality*

Introdução[5]

O Programa Bolsa Família (PBF) nasceu com a vocação de unificar e centralizar: unificar programas sociais de enfrentamento à pobreza e centralizar, no Governo Federal, os processos de normatização, seleção de beneficiários e monitoramento, e de integração com as políticas das áreas da educação e da saúde. Por isso, a relação entre o programa e seu principal instrumento de gestão de dados, o Cadastro Único, pode ser descrita como *simbiótica*. A cadeia de valor da informação que caracteriza os fluxos do PBF, do cadastramento ao controle das condicionalidades, permite considerá-lo um programa *datificado*.

Datificação é definida como o crescente uso de dados e seu impacto na vida social (Heeks; Shekhar, 2019; Masiero; Das, 2019). Embora se trate de uma perspectiva incipiente nos estudos sobre políticas sociais, o fenômeno é global: esquemas de proteção social, nos últimos quinze anos, vêm se tornando cada vez mais computadorizados; paralelamente, dados de beneficiários passam a desempenhar um papel determinante em todas as etapas dos programas sociais e de seus respectivos processos de decisão (Masiero; Das, 2019).

Há muito que dados são usados em políticas públicas, mas o advento das tecnologias digitais em todo o mundo e sua difusão nos países periféricos significaram uma diferença de grau. A datificação traz a promessa de maiores efetividade e responsividade dos programas, já que o cruzamento automatizado de dados possibilita o aperfeiçoamento da identificação e seleção dos beneficiários – pretendendo resolver, em especial, problemas de inclusão de beneficiários que não cumprem as condições e de *exclusão* de quem efetivamente precisaria do benefício (Muralidharan; Niehaus; Sukhtankar, 2016). Para programas focalizados de transferência de renda, não é promessa pequena. A Organização das Nações Unidas (ONU), por exemplo, identificou no uso de dados um potencial revolucionário para se atingir as metas de desenvolvimento sustentável (ONU, 2015).

Vem despontando uma literatura, em especial no campo de estudos de desenvolvimento, que observa o problema a partir da perspectiva da justiça (ou injustiça) de dados, que pode ser definida como "justiça na forma como pessoas

5 Este trabalho é resultado de um projeto de pesquisa realizado no InternetLab – associação de pesquisa em direito e tecnologia, por meio de um financiamento da Privacy International, viabilizado pelo International Development Research Center (IDRC). As autoras agradecem as colaborações da pesquisadora Julia Drummond, a revisão de Clarice Tavares e as contribuições da pesquisadora Jaciane Milanezi e da gestora de políticas públicas Juliana Borim Milanezzi.

se tornam visíveis, representadas e são tratadas em razão de sua produção de dados digitais" (Taylor, 2017). Essa noção permite revelar formas novas e específicas de injustiça na datificação de programas sociais. Como a datificação afeta os beneficiários do PBF?

Nos termos da justiça de dados, as análises podem dizer respeito a desigualdades para a datificação – diante de deficiências digitais e desigualdades de acesso em determinado país e entre países – ou a desvantagens da datificação *em si* – como vigilantismo e riscos à privacidade, captura privada das políticas, ou o aumento de desigualdades decorrente da perda relativa de poder de indivíduos e grupos. Heeks e Shekhar (2019) propõem um modelo que sistematiza a análise de processos de datificação de políticas sociais, a partir do seu sistema de dados, e em cinco diferentes dimensões. Os momentos da cadeia são separados a "subida" (coleta de dados); a "correnteza" (processamento e visualização dos dados); e a "descida" (uso da informação em decisões e ações voltadas para o cidadão)[6]. Em cada um desses momentos, a observação de cinco dimensões serve de auxílio à avaliação de aspectos de justiça:

- Na dimensão procedimental, como os dados são tratados nas diferentes fases da cadeia, a partir de perspectivas de equidade;
- Na dimensão instrumental, avaliação de equidade nos resultados do uso dos dados;
- Na dimensão baseada em direitos, a aderência, em todas as fases da cadeia, aos chamados direitos associados a dados ("*data rights*"), como o direito de estar adequadamente representado no conjunto de dados, mas também direitos relacionados à privacidade, acesso e titularidade;
- Na dimensão estrutural, como a distribuição e fluxo de poder e interesses apoiam resultados equitativos ou não;
- Por fim, na dimensão distributiva, superestrutural e guarda-chuva para as demais, se há resultados equitativos em todas as outras dimensões.

Nossa análise do PBF leva em conta, primariamente, a dimensão baseada em direitos e a procedimental. A principal razão é a metodologia aqui empregada.

6 Em inglês, respectivamente, *upstream*, *midstream* e *downstream*.

Na dimensão baseada em direitos, foca-se quem e o que está visível em uma determinada cadeia de dados – bem como para quem –, ao passo que, na procedimental, se destacam as normas e o funcionamento do programa, em vez de seus resultados.

A visibilidade dos beneficiários de uma política social pode ser lida também a partir do conceito de legibilidade, desenvolvido por J. Scott para referir-se à forma como Estados processam informações sobre seus cidadãos para atingir seus objetivos – um processo de simplificação e padronização de dados para fins de controle social e por meio do qual compreensões locais e nativas são dissolvidas (Scott, 1998). A dinâmica entre visibilidade e legibilidade pode despertar receios, por exemplo, em cidadãos com status de informalidade ou ilegalidade (Heeks; Shekhar, 2019) ou diante da possibilidade da perda de benefícios. Ademais, a legibilidade, uma vez construída, pode apresentar-se a terceiros não esperados; nessa dinâmica, importantes consequências se colocam da perspectiva do direito à privacidade e do direito à autodeterminação informativa. Na dimensão procedimental, observamos a forma como são tratados e protegidos os dados ao longo da cadeia de valor da informação, e, como consequência, sobre quem recaem os riscos do tratamento dos dados.

A literatura mostra como, no caso das políticas sociais de alívio à pobreza, a privacidade é tacitamente negociada e facilmente abdicada quando a contrapartida é o acesso a benefícios (Callander, 2019; Masiero; Das, 2019). Isso aumenta a sensibilidade em torno dos riscos, e demanda atenção para as categorias mobilizadas nas discussões jurídicas com respeito a esse processo, como a do consentimento para coleta e cruzamento de dados. Por fim, este artigo também apresenta contribuições para a dimensão distributiva, a partir da qual se avalia globalmente se resultados justos estão sendo produzidos por ações relacionadas à cadeia de dados, em especial a partir da consideração de que aspectos datificados do PBF reforçam imagens de controle (Collins, 2019), conforme exploramos a seguir.

Para além do aspecto *datificado* da política pública, também levamos em consideração, em nossa análise, seu aspecto *generificado*. Por lei (art. 2º da Lei n. 10.836/2004), o benefício deve ser pago preferencialmente à mulher, como responsável pela unidade familiar. As mulheres representam 88,5% dos responsáveis familiares (Senarc, 2019), e as condicionalidades do programa dizem respeito ao cuidado de seus filhos. Tendo em vista o público prioritário desta política –

mulheres, majoritariamente pardas e pretas[7], em situação de pobreza e extrema pobreza –, examinamos este aspecto do programa à luz do conceito de "matriz de dominação", desenvolvido por Patricia Hill Collins (2019), bem como o potencial de seu reforço através de imagens de controle.

Para a autora, as relações sociais são constituídas por um arranjo de sistemas sobrepostos de opressão baseados em gênero, estrato social, estatuto do cidadão, raça e etnia, e pela organização de quatro esferas de poder: a estrutural, que diz respeito ao poder exercido por meio de leis e políticas públicas; a disciplinar, por meio de hierarquias burocráticas e técnicas de controle e vigilância; a hegemônica, quando ideias e ideologias dominantes se impõem; e a interpessoal, estabelecida nas relações cotidianas (Collins, 2019; Kerner, 2012). As imagens de controle, por sua vez, operam na dimensão ideológica e atribuem significados à vida das mulheres negras que solidificam a matriz de dominação à medida que se tornam hegemônicas e que são percebidas como "naturais" (Collins, 2019; Bueno, 2020). Nesse sentido, adotamos a hipótese, em nossa análise, de que as imagens de controle *welfare mother* e *welfare queen*[8], detalhadas mais adiante, informam o processo de concepção, formulação, implementação e avaliação do programa.

Assim, neste artigo, oferecemos uma análise não exaustiva do PBF a partir das perspectivas de datificação, privacidade e gênero. As conexões entre essas três dimensões são examinadas, aqui, por meio da literatura sobre esses temas e de dados, entrevistas com gestores públicos[9] e material primário (denúncias contra beneficiárias)[10].

7 Os dados da Senarc de 2016 indicam que 75% das beneficiárias do programa são pretas e pardas. Ver dados da Secretaria Nacional de Renda e Cidadania, do Ministério da Cidadania (Senarc/MC, 2016).

8 A autora define outras quatro imagens de controle: *mammy*, matriarca, Jezebel/*hoochie* e dama negra. Para mais detalhes sobre suas características, ver Collins (2019, pp. 135-77) e Bueno (2020).

9 Entre setembro de 2019 e fevereiro de 2020, realizamos oito entrevistas semiestruturadas com funcionários públicos do governo federal e dos municípios de São Paulo e Osasco. A decisão de entrevistar gestores desses dois municípios veio da percepção das singularidades do município de São Paulo e de cidades que integram a região metropolitana no que se refere a seus desafios e estratégias socioassistenciais. Ouvimos pessoas que, conforme a literatura, são consideradas burocracia de médio escalão (Cavalcante; Lotta, 2015), isto é, integram equipes que hierarquicamente se situam entre o alto escalão e a burocracia do nível da rua. São elas: Pierre Rinco (Observatório de Vigilância da Socioassistencial de São Paulo), Marina Carvalho (Senarc/MC), Thadeu Costa (Ouvidoria do MDC), Luiz Francischini (coordenador de gestão de benefícios do município de São Paulo), Osvaldo Santos (gestor municipal do município de Osasco), Sérgio Tadeu Neiva Carvalho (Controladoria-Geral da União [CGU]), João Gabriel Miranda Alves Pereira (CGU), José Roberto Frutuoso (Departamento do Cadastro Único, Secretaria de Avaliação e Gestão da Informação, Ministério da Cidadania [Sagi/MC]).

10 O material foi levantado via Lei de Acesso à Informação (LAI, lei 12.527, de 18 de novembro de 2011). Solicitamos inicialmente dados globais, segundo os quais, entre os anos de 2006 e 2019, foram registradas 44.339 denúncias. O ano de 2018 foi então definido como marco temporal, ao passo que a amostra se

Além desta introdução e da conclusão, o artigo apresenta outras quatro seções: na primeira delas, apresentamos aspectos do desenho do PBF que são centrais nas discussões das seções seguintes; na segunda, tratamos do CadÚnico, de sua arquitetura e do fluxo de dados; na terceira seção, analisamos o programa a partir de um de seus traços constitutivos, a focalização; por fim, na quarta seção, exploramos de forma detida o aspecto generificado da política. A intenção é contribuir não somente para uma agenda de pesquisa que ainda engatinha, como também para a visibilização de perspectivas em torno do direito à privacidade e da justiça de dados, em um momento de fundação do ecossistema de proteção de dados no país e em que transferência de renda volta a ocupar o centro do debate diante do Auxílio Emergencial aprovado como resposta institucional à crise de Covid-19.

O Programa Bolsa Família

O PBF é o maior programa de transferência condicional de renda do mundo (*The Economist*, 2020). Em junho de 2020, compreendia 14,283 milhões de famílias em situação de pobreza e de extrema pobreza, totalizando 43.711.464 de pessoas[11].

Em todo o mundo, programas de transferência de renda foram uma resposta ao desemprego e à pobreza decorrentes de um contexto de reestruturação produtiva e de ajuste econômico. No Brasil, o modelo surgiu nos anos 1990, ainda que, nos anos 1980, a sociedade civil e os debates constituintes já apontassem para essa possibilidade no horizonte. Ele foi positivado de fato na noção de "seguridade social" da Constituição de 1988, em concordância com a pauta da universalização dos direitos sociais. A crise fiscal do Estado e o projeto neoliberal dos governos bra-

constituiu a partir da seleção de um estado de cada uma das cinco regiões federativas. As denúncias de cidadãos do Maranhão, Santa Catarina, Pará, Espírito Santo e Mato Grosso do Sul foram solicitadas por nós, também por não ultrapassarem o número de 100 registros por estado. Assim, nosso corpus constitui-se do conteúdo de 339 denúncias. Uma vez que, a partir de 2019, novas orientações sobre o encaminhamento de denúncias foram transmitidas aos cidadãos, recebemos da Coordenador-Geral da Ouvidoria do Ministério da Cidadania a sugestão de também solicitá-las, a título de comparação. Acessamos então outros 81 casos e trabalhamos com o total de 420 denúncias.

11 Dados obtidos no VIS Data, Painel de Monitoramento Social do MDS. <https://aplicacoes.mds.gov.br/sagi/vis/dash/painel.php?d=55>.

sileiros dos anos 1990 – somados à reação das elites conservadoras no Congresso à regulamentação fragmentada dos direitos sociais – resultaram em programas alinhados às orientações então estabelecidas pelo Banco Mundial e pelo Banco Interamericano de Desenvolvimento (BID) para políticas sociais: descentralização, privatização e focalização (Silva e Silva; Yazbek; Di Giovanni, 2006).

O PBF foi criado em 2003, unificando programas anteriores de transferência de renda do Governo Federal – Bolsa Escola, Bolsa Alimentação, Vale-Gás e Cartão Alimentação. Ainda que tenha se baseado em iniciativas de estados e municípios que vinham sendo implementadas desde 1995, o PBF significou um importante avanço institucional, em especial pela partilha da responsabilidade entre a União, os estados e os municípios, pela articulação entre diferentes políticas sociais e pela eleição do "grupo familiar" como sujeito da proteção (Silva e Silva; Yazbek; Di Giovanni, 2006). É um programa de transferência de renda *condicionada*, ou seja, com condições nas áreas da educação e da saúde de cujo cumprimento depende a permanência no programa.

São elegíveis para o benefício todas as famílias com renda de até R$ 89 mensais por pessoa, ou entre R$ 89 e R$ 178, desde que tenham crianças e adolescentes. O benefício básico repassa o valor de R$ 89 à família e é cumulável com outros benefícios, de acordo com a presença de gestantes, nutrizes e crianças e adolescentes na família, chegando ao máximo de R$ 205. Para fazer parte do programa, a família deve estar registrada no Cadastro Único (CadÚnico) – um sistema federal criado em 2001[12] e que serve não somente ao PBF, mas a todos os programas federais direcionados à população de baixa renda (Brasil, 2017), com exceção da Previdência Social. A seleção das famílias que receberão o benefício é automatizada, com base nos dados do CadÚnico, e de acordo com os limites orçamentários do programa e o teto destinado a cada município. Não há prazo de permanência no programa, o que significa que o benefício continua a ser repassado enquanto os critérios de elegibilidade[13] forem atendidos e as condicionalidades forem cumpridas.

Duas características do programa fazem dele um lócus central de atenção para o debate sobre datificação e políticas sociais. A primeira é a centralidade do CadÚnico em toda a estruturação do programa, da descentralização à coordena-

12 Por meio do decreto nº 3.877/2001.

13 Segundo a regra de permanência, as famílias selecionadas permanecem no PBF por até dois anos após o aumento da renda familiar, desde que não ela não ultrapasse o valor de meio salário mínimo *per capita*. Esse mecanismo considera e ameniza os riscos relacionados à volatilidade de renda das famílias.

ção com outras políticas sociais. Em maio de 2020, havia mais de 73,4 milhões de brasileiros cadastrados (Dataprev, 2020), ou 35% da população. A segunda característica é a focalização do PBF[14] e o tratamento de dados que ela enseja – como o cruzamento com outras bases de dados, seja para encontrar os cidadãos que mais necessitam do benefício, seja para identificar inconsistências que podem levar à exclusão dos beneficiários. Em tais procedimentos, como veremos, inscreve-se a busca por legitimidade por parte de seus gestores, uma meta pretendida desde o momento de formulação do programa.

Descentralização política e gestão centralizada de dados: o CadÚnico

O CadÚnico é mais bem compreendido no contexto da discussão acerca da unificação dos programas de transferência de renda do governo federal, realizada na transição da Presidência de Fernando Henrique Cardoso para Lula (Paiva; Falcão; Bartholo, 2013 ; Soares; Sátyro, 2009). Os relatórios da transição indicaram sobreposição nos programas então existentes e falta de coordenação geral entre os três ministérios distintos que os geriam. Isso significava desperdício de recursos, limitação da efetividade e parca estratégia para a autonomização das famílias com vistas a seu desligamento dos programas, o que os tornava "fins em si mesmos". Nesse sentido, o CadÚnico era identificado como um "ponto de estrangulamento na implementação dos programas" e que, portanto, deveria ser reformulado como um instrumento de planejamento – inclusive para os municípios, que deveriam ter acesso aos dados (Silva e Silva; Yazbek; Di Giovanni, 2006).

As soluções para os problemas de descoordenação dependiam de instrumentos de políticas públicas que dessem conta da intersetorialidade[15]. Entre esses instrumentos, além de regulações e taxações, incluem-se sistemas de monitora-

14 Quando de sua criação, o PBF foi entendido como uma etapa na universalização de direitos sociais. Se é possível identificar um caminho nessa direção, ele é algo paradoxal: de um lado, a redução gradual do PBF e o movimento de austeridade expresso pela emenda constitucional 95/2016 e, de outro, diante da crise decorrente da pandemia do novo coronavírus, a entrada em cena da Renda Básica Emergencial e os debates que ela reinaugurou.

15 Definida por Bichir (2016) como as relações estabelecidas entre diferentes áreas do governo, e também entre elas e atores externos, em torno da questão social.

mento e gestão da informação. Dessa forma, o CadÚnico, embora precedesse o PBF[16], ganharia centralidade e cumpriria essa função.

O CadÚnico é ao mesmo tempo um instrumento de centralização, por permitir ganhos de diagnóstico e de eficiência na alocação de recursos, e de descentralização, na medida em que a existência de uma base de dados única é o que permite a responsabilidade partilhada pelos entes federativos no PBF[17]. A distribuição de papéis entre os distintos níveis da federação pode ser resumida da seguinte forma: o governo federal é a fonte dos recursos, e o ministério responsável pelo programa (atualmente, o Ministério da Cidadania) é o "*hub*", ou ponto de conexão, do PBF (Coutinho, 2013): é responsável pelas "normas de caráter geral", bem como pelo acompanhamento e supervisão da execução do CadÚnico. O Ministério da Educação e o da Saúde acompanham e fiscalizam o cumprimento das condicionalidades. Os municípios, por sua vez, cadastram as famílias no CadÚnico e se responsabilizam por visitar pelo menos 20% delas para verificação dos dados[18]. No nível local ocorre também uma descentralização política, uma vez que a população local pode participar dos processos via conselhos e instâncias de controle social (Silva e Silva; Yazbek; Di Giovanni, 2006; Coutinho, 2013).

O cadastramento das famílias é fundamental para o programa, constituindo, em sua cadeia de dados, o momento principal da etapa de "subida". Para o cadastramento, são utilizados os formulários do CadÚnico. Caso a pessoa cadastrada não tenha o Número de Identificação Social (NIS), identificação do beneficiário de programas sociais do governo, a própria Caixa Econômica Federal (CEF) o emite a partir de nome, documentação e filiação do solicitante.

Em seguida, começa a etapa "correnteza" da cadeia de dados do PBF: a CEF recebe os dados coletados pelos municípios, consolida-os e os repassa mensalmente ao Ministério da Cidadania (MC). Os dados são tratados pela área de tecnologia da informação do ministério, que dá início à etapa de "descida": define quem é elegível, sem qualquer ingerência do município[19]. A lista é então devolvida à CEF, que "opera os pagamentos" por meio de um sistema on-line chamado Sistema de Benefícios ao Cidadão (Sibec), e a folha de pagamentos é então submetida à

16 O CadÚnico foi criado pelo decreto 9.364/2001 – posteriormente substituído pelo decreto 6.135/2007.

17 O fato de o CadÚnico ser federal mas com cadastramento municipal tem sido visto, também, como mecanismo contra corrupção e práticas clientelistas (Coutinho, 2013).

18 O relatório de acompanhamento do Tribunal de Contas da União (TC 030.760/2015-1), no entanto, indica que o percentual de formulários preenchidos em visita familiar foi de 6% em 2015.

19 Informação obtida em conversa com Luiz Francischini em 2019.

Senarc[20].

A coleta de dados: direitos e responsabilidades

O contato entre entrevistado e Estado, mediado pelo entrevistador, envolve importantes aspectos procedimentais e de direitos associados a dados. É um momento de possível estabelecimento de relações de confiança, de identificação proativa de vulnerabilidades e também de realização de alguns direitos e princípios de proteção de dados. A atenção a esses elementos pode diferenciar uma experiência de reforço de autonomia – ou autodeterminação informacional – ou, do seu contrário, a alienação informacional. Do ponto de vista legal, está implicado nesse ponto o princípio da transparência, de acordo com o qual devem ser garantidas aos titulares de dados informações claras, precisas e acessíveis sobre o tratamento de dados e os agentes responsáveis[21]. Exemplos desse princípio são as garantias de que as informações fornecidas serão utilizadas somente para os propósitos descritos, que será obstado o acesso indevido a elas e que a privacidade será preservada.

Para o cadastramento, alguns municípios recrutam assistentes sociais e estagiários de seu corpo técnico, enquanto outros terceirizam a atividade (Bartholo; Araújo, 2008). Os entrevistadores são treinados e seguem um roteiro com as orientações registradas no *Manual do entrevistador* (Brasil, 2017). Ali estão postas diretrizes como a de "tratamento cordial", "respeito" pelas respostas oferecidas, abstenção de "juízos de valor" e tomada de consentimento no registro de observações. Os entrevistadores são orientados a alertar, no início da entrevista, sobre o dever do entrevistado de dizer a verdade e os riscos de responsabilização civil ou criminal pela omissão ou falsidade das informações. No final, devem informar aos respondentes que "as informações prestadas ao Cadastro Único são sigilosas e somente poderão ser utilizadas para formulação e gestão de políticas públicas

20 Informação obtida em conversa com Marina Carvalho (secretária substituta da Senarc) em 2020. Outros dois sistemas apoiam o trabalho da Senarc: o Sistema de Gestão do Programa Bolsa Família (SIGPBF), que cadastra municípios e serve à solicitação de formulários do CadÚnico, e o Sistema de Condicionalidades (Sicon), que é alimentado pelos dados das pastas da Saúde e da Educação.

21 Em diferentes perspectivas, o princípio da transparência pode ser encontrado não somente no artigo 6, parágrafo VI da Lei Geral de Proteção de Dados (LGPD), mas também no artigo 37 da Constituição Federal, bem como no artigo 31 da Lei de Acesso à Informação e no artigo 7, parágrafo III, do Marco Civil da Internet.

e realização de estudos e pesquisas", nos termos das normas aplicáveis[22] – o que corresponderia à finalidade da coleta de dados e deslocaria a questão da segurança no seu tratamento para um nível mais superficial. Devem também lembrar o entrevistado da necessidade de atualização das informações prestadas, da impossibilidade de dar garantias de acesso aos programas e de como entrar em contato para mais informações.

A partir do *Manual* e das entrevistas conduzidas com gestores municipais[23], é possível inferir que o fornecimento de informações sobre o tratamento de dados não é um aspecto adequadamente contemplado na interação. Os alertas sobre possível responsabilização por informações falsas e imprecisas não é acompanhado, por exemplo, de informações acerca dos processos de validação, averiguação ou controle dos dados. A ênfase recai sobre as responsabilidades do beneficiário, enquanto as responsabilidades do Estado — especialmente sensíveis diante da obrigatoriedade da coleta para o acesso ao PBF e da natureza dos dados coletados — são apenas superficialmente mencionadas. O consentimento é solicitado apenas para envio de e-mails e mensagens de texto de celular, pela CEF, e para o registro de observações próprias do entrevistador.

A extensão dos dados

O CadÚnico compreende os formulários de cadastramento, um sistema informatizado e uma base de dados, e pode ser caracterizado como um *Single Registry* (Barca; Chirchir, 2014). Isto é, ele permite a seleção de beneficiários a partir do armazenamento de informações que os identificam e caracterizam, bem como o monitoramento das intervenções, mas não é um sistema de gestão integrada dos programas, os quais contam com sistemas independentes.

Os quesitos constantes dos formulários estabelecem os conceitos para a representação da população-alvo. No processo de coleta de dados, a situação das famílias é traduzida em informações que sobem à base do CadÚnico – é, portanto, um filtro, através do qual os cidadãos tornam-se visíveis e legíveis (Bartholo; Araújo, 2008; Scott, 1998).

Além da renda, do número de pessoas conviventes e da escolaridade, o

22 Decreto 6.135, de 26 de junho de 2007, e portaria 10, de 30 de janeiro de 2012.

23 Informação obtida em conversa com Luiz Francischini em 2019.

formulário registra as condições de moradia, o acesso ao trabalho, a presença de deficiências e o pertencimento a grupos populacionais tradicionais e específicos (GPTE). A pessoa responsável pela unidade familiar tem, no mínimo, de responder ao formulário principal, que demanda informações diferentes[24], com diferentes graus de detalhamento e sensibilidade. O cadastramento permite conhecer detalhes da família, seus antecedentes, as características de seu domicílio e seus hábitos, por exemplo: o material de construção de pisos e paredes, quanto é gasto com energia elétrica, transporte e medicamentos, a condição de abastecimento de água, detalhes sobre trabalhos e outras formas de obtenção de recursos, pertencimento a populações indígenas ou quilombolas e documentos pessoais (RG, CPF, Título de Eleitor, Carteira de Trabalho, Certidão de Nascimento).

O *Manual do entrevistador* prescreve que o responsável deve apresentar, obrigatoriamente, o CPF ou o título de eleitor[25], enquanto os demais membros da família devem apresentar ao menos um documento pessoal – mas, como já apontado, todos os documentos que a pessoa possuir devem ser cadastrados. As pessoas sem documentação devem ser incluídas e receber recomendações para emissão de documentos. Dos membros da família são coletados dados de identificação (38 campos para cada).

Os Formulários Avulsos servem para cadastramento, ou atualização cadastral, de outros membros, e não oferecem novidade. O Formulário Suplementar 1 identifica a vinculação da pessoa ou da família a outros programas ou serviços do governo federal (como Tarifa Social na energia elétrica ou mesmo refeições em restaurantes populares) e seu eventual pertencimento a grupos tradicionais ou específicos. O Formulário Suplementar 2 inclui mais onze perguntas para pessoas em situação de rua, incluindo participação em atividade comunitária e motivos para morar na rua.

Essa significativa extensão dos formulários permite que políticas de saneamento básico, emprego e melhorias habitacionais sejam direcionadas às populações cadastradas. A vocação do CadÚnico para ser polo de articulação de políticas sociais do governo federal é de fato perceptível de forma destacada em distintos momentos. Por exemplo, o Programa Nacional de Acesso ao Ensino Técnico e Emprego (Pronatec), instituído em 2011, direcionou a beneficiários jovens e adultos

24 No cálculo, unificamos campos que dizem respeito a uma mesma informação. Algumas informações não são respondidas por todas as pessoas, caso elas respondam "não" a questões condicionais prévias.

25 Exceto no caso de famílias indígenas ou quilombolas, em que é aceita qualquer outra documentação, incluindo, para as primeiras, o Registro Administrativo de Nascimento do Indígena (Rani).

do PBF vagas em cursos de qualificação profissional – o que, naquele ano, resultou em 600 mil matriculados no Pronatec que eram beneficiários do PBF, sendo 66% deles mulheres (Bartholo; Passos; Fontoura, 2017). Além disso, o CadÚnico passou a ser utilizado, em 2020, também como infraestrutura de dados para a concessão da Renda Básica Emergencial durante a pandemia do novo coronavírus.

Embora a economicidade do formulário seja um dos fundamentos do CadÚnico[26], a sua extensão não sugere uma tendência à minimização, nem no que se refere aos dados nem no que diz respeito aos tratamentos a que são submetidos. Houve, e há, aliás, um esforço experimental de identificação de novos processamentos e possíveis usos para os dados do cadastro (Barros; Carvalho; Mendonça, 2009). Essa perspectiva pode gerar certa apreensão com relação ao princípio da necessidade no tratamento de dados pessoais (art. 6º, III da LGPD), que determina coleta e processamento restritos ao estritamente necessário à finalidade pretendida. Esse apetite por informação, ou tendência maximalista, se não acompanhado de um reforço da lógica precaucionária, deposita nos titulares os riscos da cadeia de valor da informação.

É evidente que esse conjunto de informações – e seu permanente aprimoramento por meio do cruzamento com outras bases de dados – pode servir a terceiros com interesses comerciais (como instituições de crédito) e político-eleitorais (como candidatos), para finalidades de controle moral, social ou ideológico, ou, ainda, para diferentes tipos de fraudes e abusos. É por essa razão, e pelo grau de vulnerabilidade social das pessoas cadastradas, que são centrais os debates em torno do sigilo e segurança dos dados e sobre os impactos de seu uso. Não faltam exemplos dos riscos da exposição indevida: apenas entre 2018 e 2020, houve casos de mensagens eleitorais sendo disparadas especificamente para beneficiárias do PBF, e ao menos três casos amplamente documentados de golpes que, prometendo benefícios adicionais, instalavam vírus nos dispositivos das beneficiárias[27].

Os dados que identificam e caracterizam as famílias cadastradas são sigilosos (de acordo com o decreto 6.135/2017 e a portaria 10/2012). A eficácia e mesmo o sentido dessa garantia dependem, no entanto, dos procedimentos de acesso, compartilhamento, armazenamento e exclusão dos dados. Nesse sentido,

26 Como mencionado no texto do relatório do TCU, TC 030.760/2015-1.

27 Agência Brasil. "Ministério alerta para fraude via WhatsApp sobre 13o do Bolsa Família" (2019): <http://bit.do/fraudeAgBr>. O Estado de S. Paulo. "Golpe no WhatsApp promete benefício do Bolsa Família" (2018): <http://bit.do/fraudeEst>. Folha de S.Paulo. "Golpe no WhatsApp que promete liberar 13° do Bolsa Família instala vírus" (2019): <http://bit.do/fraudeFl>. Folha de S.Paulo. "Campanha de Meirelles enviou WhatsApp a beneficiários do Bolsa Família" (2018): <http://bit.do/eleitFl>.

a partir de uma análise inicial e exploratória, alguns elementos chamam atenção.

O CadÚnico, que hoje informa mais de vinte programas, emprega os dados para ao menos três finalidades: planejamento, concessão de benefícios e controle e auditoria, além da possível disponibilização para pesquisas. O acesso aos dados por atores estatais ou executores descentralizados privados, como organizações da sociedade civil, concessionárias e permissionárias de serviços públicos, ou empresas privadas prestadoras de serviços, ocorre por meio de: (i) sistemas de informação com relativa integração com o CadÚnico, (ii) da extração da base completa, (iii) do produto de cruzamentos solicitados ou, finalmente, (iv) da Cecad/V7, ou seja, o Sistema de CadÚnico ou o Sistema de Consulta, Seleção e Extração de Informações do CadÚnico (Direito; Koga, 2016).

Hoje, todas as formas de acesso aos dados do CadÚnico são reguladas pela política instituída pela portaria 502/2017[28]. Por outro lado, as práticas concretas[29], como é o caso da autorização concedida às distribuidoras de energia elétrica para acessar integral e diretamente a base de dados do CadÚnico, com vistas a conceder o benefício da Tarifa Social de Energia Elétrica (Direito; Koga, 2016), desafiam a eficácia desses dispositivos. A cessão dos dados, de fato, depende da autorização do governo federal e é precedida pela assinatura de termos de responsabilidade e de compromisso de manutenção do sigilo. Embora tais documentos formalizem uma obrigação e viabilizem a responsabilização diante de violação, eles constituem um mecanismo *reativo* de proteção da privacidade – não parecem obstar e diminuir o risco de acesso indevido de maneira proativa. Falham, portanto, em incorporar a privacidade ao sistema ao longo de todo o seu ciclo: por um lado, compartilha-se mais informação que o necessário para o atendimento da finalidade específica; por outro, o controle de acesso se torna mais frágil, mesmo com o emprego de termos de responsabilidade.

Tais fragilidades convivem com outras medidas recentes, que têm afetado os já precários limites para o compartilhamento de dados. O decreto 10.047/2019 insere o CadÚnico entre as 51 bases de dados cujo acesso será disponibilizado

28 A política responde à falha identificada em 2009 em auditoria realizada pela Secretaria de Fiscalização de Tecnologia da Informação (Sefti) em conjunto com a 4a Secretaria de Controle Externo do TCU, em que se identificou a inexistência de uma política de segurança da informação (PSI) e o risco resultante da não formalização dessas regras. O CadÚnico estaria, segundo o relatório da auditoria, vulnerável a acessos não autorizados. Ver: Brasil (2009).

29 Em 2018 foram inauguradas medidas de segurança, como o acesso com autenticação em duas etapas. Em contrapartida, ficou a cargo dos municípios operar as funcionalidades de controle de acesso do sistema e evitar fraudes e acessos indevidos. Ver: Brasil (2019).

ao Instituto Nacional do Seguro Social (INSS) com vistas à análise, concessão, revisão e manutenção de benefícios por ele administrados (art. 9, §2º). O decreto 10.046/2019, por sua vez, criou um Cadastro Base para consolidar "atributos biográficos" constantes de bases de dados federais, permitindo, portanto, a integração do CadÚnico, o que facilita o compartilhamento de dados entre órgãos da administração pública, sem que se prevejam medidas de atenção aos princípios de proteção de dados.

Focalização: cruzamentos, averiguações e o fantasma da fraude

A renda autodeclarada é o principal critério de seleção de beneficiários e atribuição do valor do benefício (Farias, 2016; Barros *et al.*, 2008). Esse traço do programa, no entanto, é alvo frequente de críticas e desconfianças. Dele decorrem também impactos sobre a forma como são tratados os dados de beneficiários, a começar por sua combinação com as cotas por município e com outras bases como estratégias originárias de correção e focalização (Barros *et al.*, 2008).

A imprensa e órgãos de controle vieram, ao longo dos anos, repercutindo que o dado autodeclarado não seria confiável e representaria um incentivo à subdeclaração (Farias, 2016; Lindert; Vincensini, 2019). As perspectivas de que os potenciais beneficiários – em sua ampla maioria, mulheres – teriam incentivos para ludibriar o Estado, por serem enunciadas a partir de lugares de autoridade, reforçam as imagens de controle associadas a essas mulheres, nos termos de Collins (2019). A imagem da *welfare mother* está ligada ao estereótipo da preguiça e à ideia de que mulheres negras e pobres teriam filhos para aumentar o benefício recebido. Embora o termo tenha sido cunhado fora do Brasil, a imagem é bastante conhecida do nosso contexto, como aponta Bueno (2020). A imagem de controle da *welfare queen*[30], por sua vez, diz respeito à mulher que, com ou sem filhos, não tem um marido e, por depender de benefícios sociais, é considerada "casada com o Estado", vivendo, assim, do dinheiro dos cidadãos contribuintes (Collins, 2019,

30 Nos EUA, nos anos 1980, Ronald Reagan cunhou o termo *welfare queen* para referir-se a mães beneficiárias como preguiçosas e promíscuas (Gilman, 2008).

pp. 149-50)[31].

Essas imagens foram amplificadas, mais recentemente, por dois fatores. O primeiro é que o PBF foi atravessado por pressões políticas associadas à conflituosidade construída em torno do Partido dos Trabalhadores, ao qual a imagem do programa esteve ligada[32]. O segundo está relacionado a uma tendência de cortes em programas sociais, materializada nas restrições orçamentárias e financeiras decorrentes do Novo Regime Fiscal (EC 95/2016). Com o teto de gastos públicos veio a demanda por economia, redução do número de benefícios e controles mais rígidos sobre beneficiários de programas assistenciais ou previdenciários do governo. No debate público, os erros de inclusão ganharam centralidade – e a pressão decorrente dessa situação influencia o tratamento de dados.

As intervenções em resposta a essas pressões são variadas e longevas. Um exemplo foi a já extinta Rede Pública de Fiscalização do Bolsa Família, criada em 2005 para dissipar críticas e reforçar a legitimidade do programa; outro, de 2016, foi o Grupo de Trabalho Interinstitucional do Bolsa Família, incumbido de formular estratégias de "pente-fino". O uso de dados e de técnicas de cruzamento de bases tem um lugar privilegiado nas ações e nos discursos a respeito de coibição de fraudes.

Vale lembrar, no entanto, que cruzamentos para qualificação da base e identificação de inconsistências estão ligados originariamente ao traço focalizado do programa. Dada a limitação de recursos destinados ao PBF, os cruzamentos são justificados pelo propósito de alcançar "quem realmente precisa" (Bachtold, 2017). Em contrapartida, os mecanismos de "controle do risco da autodeclaração" são a revisão cadastral, a exclusão lógica e a averiguação[33].

31 Dados do Instituto Brasileiro de Geografia e Estatística (IBGE) apontam que 63% das casas comandadas por mulheres negras e com filhos de até 14 anos encontram-se abaixo da linha da pobreza, com renda de US$ 5,5 *per capita* ao dia, cerca de R$ 420 mensais. O índice representa mais que o dobro de pontos percentuais se comparado à média nacional, igualmente alarmante: 25% de toda a população está abaixo da linha da pobreza. Para mulheres brancas e com filhos, a proporção de casas abaixo da linha da pobreza é de 39,6%. Ver: Ferreira, Bruno e Martins (2019).

32 Entre os elementos da *Ponte para o futuro*, lastro programático das articulações pelo impeachment da presidenta Dilma Rousseff, estava o compromisso de "estabelecer uma agenda de transparência e de avaliação de políticas públicas, que permita a identificação dos beneficiários, e a análise dos impactos dos programas", lastreada na percepção de que "o Brasil gasta muito com políticas públicas com resultados piores do que a maioria dos países relevantes" (PMDB, 2015).

33 O relatório do TCU (TC 030.760/2015-1) é explícito na ligação desses mecanismos com a garantia da qualidade dos dados (ver pars. 106 e 124). Uma primeira qualificação dos dados da base ocorre ainda na fase de "subida", com "mecanismos de unicidade das informações" (regras de atribuição do NIS) e "mecanismos de crítica imediata": na inserção dos dados, alguns campos, como CPF e Título de Eleitor, indicam inconsistências imediatamente, checando a validade do número, a correspondência ao titular ou duplicidade.

A revisão cadastral é realizada sistematicamente desde 2009 para os beneficiários do PBF[34] e, desde 2017, para todo o CadÚnico – famílias que não atualizam dados por dois anos são convocadas; se não comparecem, os benefícios são bloqueados e, depois de dois meses, cancelados[35]. A exclusão lógica do registro cadastral ocorre após 48 meses sem atualização, bem como no caso de má-fé comprovada na omissão ou prestação de informações inverídicas[36]. Finalmente, a averiguação cadastral se dá pela checagem de inconsistências a partir da comparação com outras bases de dados[37]. Nesses casos, os beneficiários são chamados a realizar nova entrevista e a atualizar seus dados; confirmada a inconsistência, a família deve ter a oportunidade de se manifestar, ao passo que o cancelamento do benefício, o ressarcimento dos valores e a responsabilização dos eventuais fraudadores só ocorrem diante de comprovada má-fé ou recusa a prestar esclarecimentos[38]. A oportunidade de defesa, a convocação para atualização, e a possibilidade de bloqueio antes do cancelamento devem ser reconhecidos como importantes garantias e proteções em um sistema datificado: primeiro, defesa e esclarecimento; depois, a decisão.

Os cruzamentos de dados anuais são realizados desde 2005, por recomendação de auditoria do TCU (acórdão 240/2003) e, desde então, novas bases vêm sendo somadas ao processo. Em paralelo, os cruzamentos também são conduzidos diretamente pelos órgãos de controle, como o TCU e a CGU, e os resultados são incorporados no processo de averiguação, seguindo o mesmo fluxo do Ministério da Cidadania[39]. Dessa multiplicidade de atores incumbidos, ou autoincumbidos, do cruzamento simultâneo e intensificado de bases de dados para verificação de inconsistências e controle de fraudes parece decorrer certa redundância fiscalizatória, sobretudo se considerada também a divulgação proativa de todos os pagamentos (como veremos adiante).

34 Portaria 617, de 11 de agosto de 2010.

35 Portaria 555, de 11 de novembro de 2005.

36 Portaria 177, de 16 de junho de 2011.

37 Portaria do Ministério do Desenvolvimento Social (MDS 94, de 4 de setembro de 2013). O artigo 2º menciona registros administrativos dos governos, de empresas concessionárias e prestadoras de serviços públicos, dados de pesquisas do IBGE, e "outras análises, a critério do MDS".

38 Artigo 14-A da lei 10.836/2004; ver também: Brasil (2017).

39 Instrução Operacional nº 79/Senarc/MDS.

Na cidade de São Paulo, desde 2017, foi verificada uma intensificação da busca por fraudes – as averiguações passaram a ser mais frequentes[40]. Nesses processos, o número de cancelamentos é menor que o de inconsistências, indicando que parte dos indícios não é confirmada pelas entrevistas (Bachtold, 2017). No ano de 2020, embora as averiguações tenham sido temporariamente suspensas em decorrência da pandemia de Covid-19 (portaria 335/2020), a previsão era de que a averiguação ocorresse mensalmente[41].

Esses processos vinculam-se a movimentos análogos em outras arenas decisórias: por exemplo, um "Disque-Denúncia do Bolsa Família" em debate no Congresso Nacional, uma proposta do Executivo de vinculação obrigatória dos cadastros a um CPF, e o projeto "Raio X do Bolsa Família", realizado pelo Ministério Público Federal em 2016, que teria identificado 1,4 milhão de "casos suspeitos". Tais processos são entendidos por Bachtold (2017) como conduzentes a uma "constante vigilância" e a uma "luta cotidiana para provar-se pobre" – e, acrescentamos, merecedor.

Vigilância social e seu aspecto generificado

A preocupação com a fraude e suas relações com percepções e contextos aparecem também nos discursos dos cidadãos e moldam relações. As imagens de controle associadas à *welfare queen* e à *welfare mother* vêm sendo debatidas há décadas e são mobilizadas quando as políticas públicas são direcionados a mães de baixa renda em detrimento da "população em geral", entendida a partir dos estereótipos (masculinos) associados a trabalhadores (Gilman, 2008)[42]. No contexto norte-americano, assim como no brasileiro, tais estereótipos, quando associados à maternidade de mulheres negras, vinculam-se a discursos de controle da maternidade dessas mulheres (Collins, 2019; Bueno, 2019). As disputas em torno da "justiça" e do "merecimento" do benefício associadas a essas imagens aparecem em diversas manifestações de vigilância social – uma prática que toca laços comunitá-

40 Informação obtida em conversa com Luiz Francischini em 2019.

41 Instrução Operacional Conjunta nº 03/2020/Sagi/Senarc/Ministério da Cidadania.

42 Nos EUA, nos anos 1980, Ronald Reagan cunhou o termo "*welfare queen*" para referir-se a mães beneficiárias como preguiçosas e promíscuas (Gilman, 2008).

rios e o aspecto de autodeterminação ligado ao direito à privacidade. No caso do PBF, é relevante não somente a massiva titularidade feminina, mas também, como apontamos, que as condicionalidades sejam todas relacionadas a filhos: exame pré-natal, acompanhamento nutricional, acompanhamento da saúde, frequência escolar de 85% em estabelecimento de ensino regular[43].

Além dos mecanismos próprios de controle de riscos de fraudes, fortemente baseados em dados, o PBF incorporou – e promoveu – instrumentos de controle social. Consideramos todas as denúncias feitas na Ouvidoria do MC entre 2006 e 2019 e propusemos um recorte anonimizado de denúncias de 2018 e 2019[44]. A frequência delas não é alta, e, de acordo com gestores federais e municipais consultados, são também inexpressivas no que se refere a causas de bloqueios ou descadastramentos[45]. É, por outro lado, muito expressiva a quantidade de denúncias que apresentam informações pessoais dos denunciados, entre as quais número de CPF, data de nascimento, nome da mãe e NIS[46].

Isso tem relação com a demanda do formulário de denúncia por essas informações, mas também com sua fácil disponibilidade na internet. Há ao menos três caminhos institucionais para acessá-los. No Portal da Transparência, obtêm-se nome e o NIS de todos os beneficiários, por município. No Portal Consulta Cidadão

43 O significado da titularidade feminina e das condicionalidades para as dinâmicas de gênero – e a igualdade entre mulheres e homens – vem sendo objeto de disputas em torno de polos que vão da avaliação de que elas geram "instrumentalização e naturalização do papel de cuidado" (Britto; Soares, 2010; Carloto e Mariano, 2012) até a de que elas "aumentam a autonomia" e "permitem quebra do ciclo de pobreza intergeracional via acesso a outras políticas universais" (ver: Silva e Silva; Yazbek; Di Giovanni, 2006; Coutinho, 2013). Um debate possível, também, é a respeito de como as condicionalidades afetam o aspecto de autodeterminação da privacidade.

44 O processo teve início via LAI e prosseguiu em trocas com gestores. São 44.339 as denúncias registradas entre 2006 e 2019. Recortamos uma amostra ao mesmo tempo representativa dos conteúdos e viável em termos de anonimização. Esse material constituiu fonte relevante para que acessássemos percepções e posicionamentos em torno dos beneficiários do programa e compreendêssemos dinâmicas de controle imperceptíveis a partir da análise do desenho da política em si. Observando o material a partir dessa perspectiva, dialogamos e nos somamos a investigações cujo foco são os efeitos de uma política pública na sociabilidade de seus beneficiários bem como de moralidades construídas em suas relações entre si e/ou entre atores/atrizes da burocracia estatal (Pereira; Ribeiro, 2013; Marins, 2017; Milanezi, 2019).

45 O coordenador-geral da Ouvidoria do MC, Thadeu Normando, afirmou que 95% das manifestações que chegam ao órgão referem-se ao PBF, mas em 2019 pouco mais de 2% eram denúncias (informação verbal, 2019). Luiz Francischini, da Coordenadoria de Gestão de Benefícios da Secretaria Municipal de Assistência Social de São Paulo, relatou serem poucas as denúncias e em geral motivadas por desentendimentos familiares e entre vizinhos e, portanto, não determinantes quanto à continuidade do recebimento de benefício (informação verbal, 2019).

46 A presença de alguns desses campos nos formulários do Fala.br e do portal do Ministério da Cidadania certamente favorece a busca ativa pelos denunciantes. Em 2018, 39% das denúncias incluíam o NIS; 37%, outros dados pessoais; e 16%, ambos. Em 2019, proporções semelhantes: 32% apresentavam o NIS; 37%, outros dados pessoais; e 15%, ambos.

– CadÚnico, a inserção de nome, data de nascimento, nome da mãe e estado e município do beneficiário revelam o NIS. De posse do nome, NIS e CPF, consulta-se também o status do benefício no Portal da CEF. Os dados da Transparência são usados, ademais, por projetos não oficiais – o BolsaFamilia.info, por exemplo, se propõe a "retirar fraudadores do programa", facilita as buscas e o acesso às listas e oferece um botão vermelho para "denunciar fraude", além de listar as informações individualizadas dos pagamentos.

Tudo isso suscita questões sobre a base legal, a proporcionalidade da exposição e a redundância fiscalizatória a que fizemos menção anteriormente – o que pode ser apresentado, da perspectiva distributivista, como uma *injustiça de dados*. Como medida de transparência, a lei 10.836/2004 prevê que será "de acesso público a relação dos beneficiários e dos respectivos benefícios". Por sua vez, o decreto 5.209/2004, que a regulamenta, estabelece que o Conselho de Controle Social terá acesso aos dados e informações do PBF e prevê que a relação de beneficiários será amplamente divulgada. Isso expõe desproporcionalmente os beneficiários a uma gama de violações com base em dados ou na vigilância social. Além disso, pode existir tensão com a LGPD e excesso em relação às exigências da LAI[47]. Diante dos mecanismos institucionais e rotineiros de fiscalização do PBF e do monitoramento por órgãos de controle, a divulgação mensal de beneficiários como medida de transparência ativa integra o que temos chamado de redundância fiscalizatória.

As denúncias envolvem também uma gama de informações sobre a vida dos beneficiários: 70% delas tinham a renda como principal justificativa — na maioria dos casos, em valores próximos ao salário mínimo nacional: "ela possui salão, camping, bar e possui renda de 2.000,00"; "a família possui carro, casa própria e o filho estuda em escola particular"; "possui renda no valor aproximado de R$ 1.200,00... a mesma e seu marido trabalham na roça, tem casa própria, carro e moto". É também comum que incluam justificativas envolvendo ideias de justiça e de moral: "realizando a denúncia não por rancor e sim por justiça"; "fico triste, quem precisa não consegue (sic), já outros deveria ter investigações"; "falar que é solteira porque não é casada no papel tem casa própria acho um desrespeito com tanta gente precisando". Isso corrobora conclusões de estudos como o de

47 Lei 12.527/2011, que estabelece que informações de interesse público devem ser divulgadas independentemente de solicitações (art. 3, II) e que informações pessoais poderão ser divulgadas, quando consentido, conforme previsto em lei (art. 31, II), ou diante de interesse público preponderante (art. 31, § 3° , V), ou ainda diante do envolvimento com irregularidades.

Lavinas et al (2014) sobre percepções dos brasileiros a respeito de políticas sociais: não há oposição total a políticas redistributivas, mas uma visão de que devem ser direcionadas a quem "realmente precisa", bem como ser *restritas e condicionadas*.

O PBF direciona o recurso à responsável familiar, mas a funcionalização de recurso pela presença de crianças, tendo em vista o rompimento do ciclo intergeracional da pobreza, tem eco nas percepções sociais – diversas denúncias mobilizam um argumento como "receber em nome do filho" e o repasse ao filho como pressuposto, e outras pesquisas dão conta de que a política é assim percebida também pelas beneficiárias.

Em trabalho sobre o uso do benefício por quebradeiras de coco em Codó, no Maranhão, Ahlert (2013) aponta que as beneficiárias consideram os filhos a prioridade e, ao lado deles, a casa: "tudo indica que o dinheiro do Bolsa Família aparece como uma contribuição feminina no orçamento". No trabalho de Pereira e Ribeiro (2013) e no de Pires (2012), entrevistas mostram uma forte moralidade na destinação do recurso, ausente em posições a respeito de políticas como a aposentadoria, e a vinculação da percepção do gasto com percepções sobre o papel da mãe. Isso fica evidente em denúncias com descrições detalhadas de gastos não direcionados aos filhos: "gastou R$ 400,00 com salão de beleza, R$ 2.000,00 com prótese dentária e deve R$ 600,00 de cigarro a um comércio e não gasta com os filhos o benefício"; "ela não usa o benefício para seus 04 filhos e sim para manter seus vícios"; "não usa nada com os filhos pode investigar e ver que é pra uma coisa muito ruim".

As percepções sobre programas de transferência de renda, o impacto dos papéis de gênero e das imagens de controle associadas a gênero, raça e classe, e a prática de vigilância social têm fontes múltiplas. Chama a atenção o modo como o Estado pode desempenhar um papel incentivador ou coibidor dessas ações, bem como o que isso revela da perspectiva distributiva. Além da ampla disponibilização de dados pessoais, identificamos ações contraditórias da gestão do PBF no que se refere à criação de uma moral em torno da destinação do recurso. De um lado, a Ouvidoria, em 2019, passou a enviar mensagens aos denunciantes, demovendo-os de registrar denúncias apenas por não concordarem com a destinação dos gastos, já que o PBF não determina nada a esse respeito. De outro, a página do PBF no *Facebook*, postou, em ao menos duas ocasiões, perguntas sobre como os beneficiários gastam[48] – no segundo caso, com uma enquete de fim de ano com as

48 As postagens são de 10 de outubro e 11 de dezembro de 2019. Por meio de um script, raspamos e armazenamos os comentários de respostas.

alternativas “fazer ceia de Natal” e “comprar material escolar”. Os comentários ora reiteram as respostas esperadas (“material escolar e um janta especial pq tenho 4 filho quero dar o melhor pra eles”; “comprei leite do meu bebê que é um leite mais especial pq ele tem problemas de alergia alimentação remédio paguei uma conta de luz fui no mercado e ainda sobrou um pouco pra mim comprar uma roupinha para os três graças a Deus”), ora reforçam a condenação moral e o papel esperado da mãe (“o que vejo por aí é mães pegando bolsa pra colocar mega hair, comprar o melhor celular do momento, e os filhos vivendo na miséria”; “deveria era acabar com o bolsa, ou então fazer de uma outra forma ... mas enquanto dê o $$ vai ser assim, pq infelizmente existem mães que não se preocupam com seus filhos, com o seu vestir, o seu comer, a educação, e sim se preocupam com o bem estar delas, e com o laser (sic) delas”).

Nesse tipo de interação, também estão presentes outras formas de exposição das beneficiárias para a empresa que gere a rede social, e para outros usuários, o que pode ser um disparador de fraudes, abusos e violências *online* – em especial quando se leva em conta as vulnerabilidades dessas mulheres, pobres, majoritariamente pretas e pardas, nortistas e nordestinas. Uma perspectiva de justiça de dados envolve levar em consideração, em cada etapa da execução do programa, direitos como o de privacidade e o de acesso à informação, bem como a justiça distributiva.

Conclusão

A coleta e o processamento de dados são constitutivos do desenho do PBF. Desde sua implementação, o CadÚnico serve para responder aos desafios inaugurais do programa. Sua abrangência censitária, a natureza cadastral e a abundância de informações tornaram-no um instrumento de elaboração de diagnósticos e de formulação e operacionalização de políticas públicas.

Em um país cujo histórico de proteção social carrega fortes traços contributivos e excludentes, o esforço de identificação e caracterização de privações que a população de baixa renda experimenta para a prestação de políticas públicas, é um salto importante. Os processos de datificação, por outro lado, não vieram acompanhados, nesse desenho original, de preocupações quanto à justiça de dados que fizessem frente aos riscos inaugurados.

Na análise do PBF como uma "cadeia de valor da informação", observamos, em uma dimensão procedimental, problemas na forma como são tratados os dados de beneficiários: coleta pouco orientada por imperativos de minimização (necessidade), pouca transparência em relação aos tratamentos, compartilhamentos crescentemente facilitados, desenvolvimento tardio de políticas de segurança e acesso e formas de compartilhamento que fragilizam proteções contra acessos indevidos. Em uma dimensão de direitos, chama a atenção, além da alienação resultante da falta de conhecimento acerca dos tratamentos específicos a que serão submetidos os dados obrigatoriamente coletados para acesso ao PBF, a exposição desigual experimentada por beneficiárias do PBF que ocorre na rotina de fiscalização, cada vez mais intensa, que compreende ações institucionais Ministério da Cidadania, dos órgãos de controle, mas também a habilitação e a visibilização de canais de denúncia e divulgação massiva e proativa de dados de beneficiários.

Essa exposição, inicialmente motivada pela demonstração da eficiência do programa e articulada ao ganho de legitimidade, converteu-se, com o passar dos anos, em instrumento para o escrutínio de políticas públicas, em um momento em que o governo federal passou a arguir contra seu tamanho excessivo e pela necessidade de redução. De uma perspectiva distributiva, como discutido a respeito do reforço de imagens de controle que geram também consequências na vida cotidiana das beneficiárias, observa-se a produção de injustiças.

Uma quantidade massiva de dados, muitos deles sensíveis, "sobe" no sistema; na "correnteza", eles se tornam disponíveis a um número crescente de atores,

sem que haja proteções suficientes contra acessos indevidos e para fins não comunicados; por fim, quando "descem", as informações alimentam violações e práticas sociais difusas de vigilância – as quais, alimentadas por imagens de controle, são pouco relevantes para o controle de fraudes. Essas práticas articulam-se na cadeia com uma demanda crescente pelo endereçamento local de inconsistências de dados e pela retração do programa. Isso não resume o PBF, mas é uma face relevante de sua existência, e uma preocupação a ser levada em consideração.

MARIANA GIORGETTI VALENTE

Diretora do InternetLab, pesquisadora do Núcleo Direito e Democracia do Centro Brasileiro de Análise e Planejamento (Cebrap). É doutora em sociologia jurídica pela Faculdade de Direito da Universidade de São Paulo (USP) e professora no Insper, onde coordena a Certificação em Direito e Tecnologia. Neste artigo foi corresponsável pela redação e formulação dos argumentos, e trabalhou na análise da perspectiva da justiça de dados.

NATÁLIA NERIS

Doutoranda em direitos humanos na Faculdade de Direito da Universidade de São Paulo (USP), mestra em direito e desenvolvimento pela Fundação Getúlio Vargas (FGV) e bacharela em gestão de políticas públicas pela Escola de Artes, Ciências e Humanidades (Each-USP). É autora do livro A voz e a palavra do Movimento Negro na Constituinte de 1988 (Casa do Direito, 2018). Neste artigo foi corresponsável pela redação e formulação dos argumentos, e trabalhou na análise das denúncias e na perspectiva de gênero.

NATHALIE FRAGOSO

Coordenadora da área de Privacidade e Vigilância do InternetLab, com doutorado e graduação em direito pela Faculdade de Direito da Universidade de São Paulo (USP). Possui o Zertifikat in den Grundzügen des deutschen Rechts e o LLM na Ludwig-Maximilians-Universität München. Neste artigo foi corresponsável pela redação e formulação dos argumentos, e na análise do fluxo e proteção de dados.

Recebido para publicação em 25 de julho de 2020.
Aprovado para publicação em 18 de setembro de 2020.

Referências bibliográficas

Ahlert, M. "A 'precisão' e o 'luxo': usos do benefício do Programa Bolsa Família entre as quebradeiras de coco de Codó (MA)". *Revista Política e trabalho*, n. 38, 2013.

Bachtold, I. *"Precisamos encontrá-los!": etnografia dos números do Cadastro Único e dos cruzamentos de base de dados do governo federal brasileiro*. Dissertação (mestrado em antropologia social). Brasília: Universidade de Brasília, 2017.

Barca, V.; Chirchir, R. *Single Registries and Integrated MISs: De-mystifying data and information management concepts*. Canberra: Department of Foreign Affairs and trade of the Australian Government, 2014.

Barros, R.; Carvalho, M.; Mendonça, R. *Sobre as utilidades do Cadastro Único*. Rio de Janeiro: Ipea, 2009. (Texto para discussão, n. 1.414.)

Barros, R.; Carvalho, M.; Franco, S.; Mendonça, R. *A importância das cotas para a focalização do Programa Bolsa Família*. Rio de Janeiro: Ipea, 2008. (Texto para Discussão, n. 1.349.)

Bartholo, L. "Bolsa Família e autonomia feminina: O que nos dizem os estudos qualitativos?". *Research Brief*, Centro Internacional de Políticas para o Crescimento Inclusivo, n. 57, nov. 2016.

_____; Araújo, L. "Em busca das famílias reconstituídas: mapeamento dos arranjos familiares da população brasileira de baixa renda por meio do Cadastro Único de Programas Sociais". *Anais do XVI Encontro Nacional de Estudos Populacionais*, 2008.

Bartholo, L.; Passos, L.; Fontoura, N. *Bolsa família, autonomia feminina e equidade de gênero: o que indicam as pesquisas nacionais?*. Brasília/Rio de Janeiro: Ipea, 2017. (Texto para discussão, n. 2.231.)

Bichir, R. "Novas agendas, novos desafios: reflexões sobre as relações entre transferência de renda e assistência social no Brasil". *Novos Estudos Cebrap*, n. 104, 2016.

Brasil. "Auditoria nos sistemas do cadastro único para programas sociais do governo federal". Relator Ministro Augusto Nardes. Brasília: TCU, 2009.

_____. "Boas práticas para gestão municipal em segurança da informação". *Informe Bolsa e Cadastro, Ministério da Cidadania*, n. 674, 30/08/2019. Disponível em: <https://bit.ly/2Sha5xg>. Acesso em: 05/03/2021.

_____. *Manual do entrevistador*. 4. ed. Brasília: Ministério do Desenvolvimento Social e Agrário, 2017.

Britto, T.; Soares, F. *Bolsa Família e Renda Básica de Cidadania: um passo em falso?*. Brasília: Centro de Estudos da Consultoria do Senado Federal, 2010. (Texto para discussão n. 75.)

Bueno, W. *Imagens de controle: um conceito do pensamento de Patricia Hill Collins*. Porto Alegre: Zouk, 2020.

Callander, A. "Privacy, a precondition for social protection". Scottish Legal Action Group Journal. n. 500, 2019.

Carloto, C. M.; Mariano , S.. "As mulheres nos programas de transferência de renda: manutenção e mudanças nos papéis e desigualdades de gênero". *Congresso Internacional da Rede Mundial de Renda Básica de Cidadania*, 13º, 2010.

Cavalcante P.; Lotta, G. (orgs.). *Burocracia de médio escalão: perfil, trajetória e atuação*. Brasília: Enap, 2015.

Collins, P. H. *Pensamento feminista negro: conhecimento, consciência e a política do empoderamento*. 1. ed. São Paulo: Boitempo, 2019.

Coutinho, D. *Capacidades estatais do Programa Bolsa-Família: o desafio de consolidação do Sistema Único de Assistência Social*. Brasília/Rio de Janeiro: Ipea, 2013. (Texto para discussão n. 1.852.)

Dataprev. "Auxílio Emergencial: Dataprev conclui sistemas e 51,4 milhões de cidadãos serão beneficiados". Dataprev, 13/04/2020. Disponível em: <https://portal2.dataprev.gov.br/auxilio-emergencial-dataprev-conclui-sistemas-e-514-milhoes-de-cidadaos-sao-indicados>. Acesso em: 05/03/2021.

Direito, D.; Koga, N. "Ecossistema do Cadastro Único e seus programas usuários: uma análise relacional". *Anais do 40º Encontro Anual da Anpocs*. Minas Gerais, 2016.

The Economist. "Bolsa Família, Brazil's admired anti-poverty programme, is flailing". *The Economist*, 30/01/2020. Disponível em: <https://www.economist.com/the-americas/2020/01/30/bolsa-familia-brazils-admired-anti-poverty-programme-is-flailing>. Acesso em: 05/03/2021.

Farias, L. *O Cadastro Único: uma infraestrutura para programas sociais*. Dissertação (mestrado em política científica e tecnológica). Campinas: Unicamp, 2016.

Ferreira, L.; Bruno, M. M.; Martins, F. B. "No Brasil, 63% das casas chefiadas por mulheres negras estão abaixo da linha da pobreza". *Gênero e Número*, 12/12/2019. Disponível em: <http://www.generonumero.media/casas-mulheres-negras-pobreza/>. Acesso em: 05/03/2021.

Gilman, M. “Welfare, Privacy, and Feminism”. *University of Baltimore Law Forum*, v. 39, n. 1, 2008.

Heeks, R.; Shekhar, S. “Datafication, Development and Marginalised Urban Communities: An Applied Data Justice Framework”. *Information, Communication & Society*, v. 22, 2019.

Kerner, I. “Tudo é interseccional? Sobre a relação entre racismo e sexismo”. *Novos Estudos Cebrap*, n. 93, jul. 2012, pp. 45-58.

Lavinas, L.; Cobo, B.; Waltenberg, F.; Veiga, A.; Méndez, Y. S. Percepções sobre desigualdade e pobreza. O que pensam os brasileiros da política social? Coleção Pensamento Crítico, vol. 5. 172p Rio de Janeiro: Centro Internacional Celso Furtado de Políticas para o Desenvolvimento e Folio Digital Editora, 2014.

Lindert, K.; Vincensini, V. “Social Policy, Perceptions and the Press: An Analysis of the Media’s Treatment of Conditional Cash Transfers in Brazil”. *Social Protection & Labor Discussion Paper*, World Bank, n. 1.008, 2010.

Marins, M. *Bolsa Família: questões de gênero e moralidades*. Rio de Janeiro: Editora UFRJ/Faperj, 2017.

Masiero, S.; Das, S. “Datafying Anti-Poverty Programmes: Implications for Data Justice”. *Information, Communication & Society*, v. 22, n. 7, 2019, pp. 916-33.

Milanezi, J. *Silêncios e confrontos: a saúde da população negra em burocracias do Sistema Único de Saúde (SUS)*. Tese (doutorado em sociologia e antropologia). Rio de Janeiro: PPGSA/Universidade Federal do Rio de Janeiro, 2019.

Muralidharan, K., Niehaus, P., & Sukhtankar, S. Building state capacity: Evidence from biometric smartcards in India. *American Economic Review*, 106(10), 2895–2929, 2016.

Paiva, L.; Falcão, T.; Bartholo, L. “Do Bolsa Família ao Brasil Sem Miséria: um resumo do percurso brasileiro recente na busca da superação da pobreza extrema”. In: Neri, M. C.; Campello, T. (orgs.). *Programa Bolsa Família: uma década de inclusão e cidadania*. Brasília: Ipea, 2013.

Organização das Nações Unidas (ONU). *Transforming our world: the 2030 Agenda for Sustainable Development*. A/RES/70/1, 2015.

PMDB – Partido do Movimento Democrático Brasileiro. *Uma ponte para o futuro*. Brasília: Fundação Ulysses Guimarães, 2015. Disponível em: <http://bit.do/PBFPonte>. Acesso em: 05/03/2021.

Pereira, M.; Ribeiro, F. "No Areal das mulheres: um benefício em família". *Política & Trabalho*, v. 30, n. 38, 2013, pp. 87-104.

Pires, A. "Orçamento familiar e gênero: percepções do Programa Bolsa Família". *Cad. Pesqui.*, São Paulo, v. 42, n. 145, 2012, pp. 130-61.

_____. "Relações de troca e reciprocidade entre os participantes do Programa Bolsa Família em Campinas (SP)". *Política & Trabalho*, n. 38, 2013, pp. 171-95.

Rego, W.; Pinzani, A. *Vozes do Bolsa Família: autonomia, dinheiro e cidadania*. 2. ed. São Paulo: Editora Unesp, 2014.

Santos, G. *Gênero, desenvolvimento e Programa Bolsa Família: direitos reprodutivos, trabalho e projetos de vida de mulheres do Coque*. Tese (doutorado em antropologia). Recife: PPGA/UFPE, 2014.

Scott, J. C. *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Nova York: Yale University Press, 1998.

Senarc – Secretaria Nacional de Renda de Cidadania. *Boletim Bolsa Família e Cadastro Único*, ano 4, n. 51, 2019.

Silva e Silva, M.; Yazbek, M.; Di Giovanni, G. *A política social brasileira no século XXI: a prevalência dos programas de transferência de renda*. São Paulo: Cortez, 2006.

Soares, S.; Sátyro, N. *O Programa Bolsa Família: desenho institucional, impactos e possibilidades futuras*. Brasília: Ipea, 2009. (Texto para discussão n. 1.424.)

Taylor, L. "What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally". *Big Data & Society*, v. 4, n. 2, 2017, pp. 1-14.

POSFÁCIO

Proteção de dados pessoais: Um instrumento de justiça social[1]

HANA MESQUITA E JOHANNA K. MONAGREDA

Assumir a proteção de dados pessoais desde uma perspectiva de justiça social abre um leque de possibilidades para a defesa de direitos em sociedades estruturadas de forma profundamente desigual, como a sociedade brasileira, e cujos efeitos se refletem de forma individual e coletiva. Primeiro, porque implica assumir que a forma em que se organizam as relações sociais, econômicas e políticas é essencialmente injusta e precisa de reparação; segundo porque implica incluir no debate a forma em que essas injustiças são incorporadas nos processos de tomada de decisão sobre sistemas de dados e como estes podem contribuir para a produção e reprodução de injustiças; terceiro, porque nos convida a idealizar a proteção de dados pessoais e o uso de tecnologias rumo à construção de outras formas de interações sociais, verdadeiramente justas e igualitárias, de um novo pacto civilizatório e ao serviço das lutas emancipatórias.

A discussão sobre justiça de dados (*Data Justice*), que orienta estas reflexões, nos desafia a colocar a justiça social como ponto de partida para as decisões que envolvem uso, coleta e tratamento de dados pessoais. Para isso, é indispensável considerar como o racismo-capitalista-patriarcal-heteronormativo[2] estrutura a

1 Agradecemos ao Grupos de Estudos sobre Justiça de Dados da Associação Data Privacy Brasil de Pesquisa pelo nutridos debates que ajudaram na construção desse posfácio.

2 GONZALEZ, Lélia, **Primavera para as rosas negras**, São Paulo, Brasil: Diáspora Africana, 2018; CURIEL, Ochy, **La nación heterosexual: análisis del discurso jurídico y el régimen heterosexual desde la antropología de la dominación**, Bogotá: Brecha Lésbica y en la frontera, 2013.

sociedade e determina a distribuição da riqueza, a distribuição do poder político, a disposição de bens materiais, o acesso à justiça, as possibilidades de visibilidade e representação simbólica e, inclusive, a existência de alguns grupos sociais, condicionando o acesso a direitos, que deveriam ser universais, a uma lógica de privilégios e exclusões.

Partir de preocupações de justiça social significa estabelecer como parâmetro para pensar sobre processos justos, a experiência de opressão, as necessidades, perspectivas e demandas dos grupos sociais mais marginalizados e vulnerabilizados. Esta é, precisamente, a população que mais sofre com a coleta massiva de dados digitais e com o uso abusivo dos seus dados pessoais, e encontra mais barreiras para exercer seus direitos. Isto não significa, como pode ser argumentado, nivelar por baixo, mas entender que precisamos criar formas para corrigir a distância que existe entre o ideal ou o privilégio, e a realidade de vulnerações materiais e simbólicas que enfrentam a maioria das pessoas no Brasil.

Os impactos sociais do uso abusivo dos dados não se resolvem exclusivamente no campo da infraestrutura tecnológica, nem da garantia de direitos individuais, sendo ambos aspectos fundamentais para intervir nos problemas associados à coleta, ao armazenamento, uso e tratamento de dados pessoais, especialmente, quando consideramos a expansão de meios digitais. A perspectiva de direitos individuais tem limitações frente a problemas que surgem e se expressam na condição de grupo, porque além de ferir a privacidade e restringir a autonomia, dados classificam, hierarquizam e excluem grupos sociais a partir de critérios construídos com base em formas históricas de opressão, produzem ausências e reproduzem uma hierarquização racial que cria sujeitos não-brancos como suspeitos, ilegais, violentos, criminosos, matáveis. Ainda mais, diversos conceitos da legislação, tais como "privacidade", "autonomia", "autodeterminação informativa" e até mesmo "consentimento" não se dão nos mesmos termos entre a população branca e a população não-branca no Brasil[3].

A pretensa neutralidade da tecnologia também é limitante quando consideramos que o tratamento de dados pessoais envolve valores e práticas sociais que podem estar arraigados em preconceitos e interesses políticos e econômicos nem sempre expostos. Esses aspectos, entre outros, tornam necessário considerar a proteção de dados pessoais dentro de uma perspectiva de justiça social, que auxilie nos projetos sociais por visibilidade, participação política, redistribuição,

3 KREMER, Bianca, LGPD em vigor: por que racializar a proteção de dados é tão importante?, **Jota,** 2020.

etc., e que promova efetivamente a garantia de direitos.

Nesse contexto, as Defensorias Públicas podem se configurar como um instrumento para - o que entendemos como uma das dimensões da justiça de dados - a construção e aplicação de uma perspectiva crítica do direito fundamental, não elitista, orientado pela justiça social para resolver os problemas de quem são mais socioeconomicamente vulneráveis e envolvendo questões de dados pessoais. Num país profundamente marcado por desigualdades sociais e assimetrias de poder como o Brasil, a missão constitucional das Defensorias Públicas significa um compromisso real com a concretização de direitos.

A maioria dos processos que envolvem a coleta e o tratamento dos dados pessoais são invisíveis para a população em geral, porque de forma individual, perdemos a capacidade de identificar quando nossos dados estão sendo capturados, armazenados, usados: uma fotografia de *Facebook* pode vir a compor o álbum de fotografias policial, o CPF fornecido na farmácia pode abastecer de informações as seguradoras de saúde que nos classificam como um risco maior, os dados que concedemos a uma base de dados governamental para acesso a benefícios sociais podem nos tornar alvo de campanhas de desinformação, só citando alguns exemplos. Não apenas os dados que proporcionamos explicitamente, mas dados produzidos como resultado do armazenamento de informação nos serviços digitais que consumimos podem ter efeitos negativos sobre nossas vidas.

A falta de informação é um problema que limita a capacidade da cidadania de exercer controle sobre seus dados, porém, mesmo quando é dada informação completa sobre o tratamento dos dados, as desigualdades estruturais deixam determinados grupos em desvantagem na hora de proteger seus direitos. Quando o acesso a serviços ou o acesso a benefícios está atrelado a fornecer informação, a importância da proteção dos dados pessoais pode parecer menos expressiva[4].

Se a população tem pressa por comida ou por medicamentos, o Estado ainda precisa se preocupar pelos problemas éticos associados ao uso abusivo de dados, do contrário, a proteção de dados pessoais será apenas um benefício atrelado ao privilégio socio-econômico.

No sistema de Justiça, as Defensorias Públicas apresentam o maior potencial de estabelecer diálogos com essas populações na medida em que, em muitos casos, são a porta de entrada da cidadania à Justiça. Para além de garantidoras de direitos, as Defensorias Públicas consubstanciam-se na promoção de justiça

4 MASIERO, Silvia; DAS, Soumyo, Datafying anti-poverty programmes: implications for data justice, **Information, Communication & Society**, v. 22, n. 7, p. 916–933, 2019.

de dados no Brasil, cabendo à instituição não só se abrir para as necessidades particulares das populações, mas também agir quanto às antigas e novas barreiras para o acesso à Justiça.

Apesar da participação ativa das Defensorias Públicas, em casos envolvendo a proteção de dados pessoais e o impacto discriminatório dos sistemas automatizados em grupos vulneráveis como, reconhecimento facial e fotográfico, ainda estamos nos estágios iniciais de amadurecimento da cultura de proteção de dados, especialmente em relação ao Poder Público.

Aprovada em agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) marca o momento em que a privacidade e a proteção de dados pessoais começaram a galgar ainda mais espaço na agenda pública brasileira, onde hoje têm um lugar indiscutível[5]. Em 2022, a proteção de dados pessoais alcançou status de direito fundamental na forma da **Emenda Constitucional n.º 115 de 2022**. Embora seja uma grande vitória, a proteção de dados e demais direitos digitais estão longe de ser um direito desfrutado por todas as pessoas no Brasil.

A rápida digitalização do sistema de Justiça, acelerada pela necessidade de atendimento remoto durante a Pandemia de Covid-19, embora celebrada em razão do aumento dos índices de produtividade, impõe novas barreiras ao acesso à Justiça e ao exercício de direitos, agravando o já dramático quadro de exclusão digital. O *WhatsApp*, por exemplo, é o aplicativo usado por diversas Defensorias para o atendimento a usuários e usuárias justamente por estar instalado em 99% dos smartphones nacionais, sendo aberto todo dia em 85% deles[6]. Em muitos casos, pessoas em situação de vulnerabilidade, ainda que utilizem o aplicativo, não têm dados móveis suficientes para enviar os documentos necessários às Defensoras e Defensores[7].

Por outro lado, existe uma parcela da cidadania digitalmente privilegiada, que apresenta grau de instrução e renda maior, habilitando-os a acessar e mobilizar a tecnologia ao seu favor[8]. Estas pessoas são os verdadeiros sujeitos da LGPD, ou seja, são aqueles para os quais a lei foi pensada.

5 BIONI, Bruno; RIELLI, Mariana (Orgs.), Coleção LGPD em movimento - 8 temas chave de implementação: uma visão multissetorial. Associação Data Privacy Brasil de Pesquisa.

6 Panorama Mobile Time/Opinion Box - Mensageria no Brasil - Fevereiro de 2022. Disponível em: <**https://www.mobiletime.com.br/pesquisas/mensageria-no-brasil-fevereiro-de-2022/**>.

7 Disponível em: <**https://www1.folha.uol.com.br/poder/2022/02/virtualizacao-da-justica-se-intensifica-no-brasil-gera-ganhos-e-impoe-desafios.shtml**>. Acessado em 15 de março de 2022.

8 MULDER, F. (2020): *Humanitarian data justice: A structural data justice lens on civic technologies in post-earthquake* Nepal. DOI: 10.1111/1468-5973.12335.

Não se pretende aqui reduzir a importância da LGPD no combate à discriminação, no entanto, é imprescindível reconhecer o contexto racial brasileiro[9] que não pode ser menosprezado. Olhar para a realidade brasileira implica encarar nossa estrutura de racismo por denegação[10] que dificulta o combate à discriminação e redução das desigualdades e, consequentemente, o acesso de determinadas camadas da população à tecnologia e à justiça.

Mais do que nunca, é necessário olhar criticamente para as tecnologias que estão gradativamente mais dependentes do processamento de dados pessoais. Nesse contexto, surgem desafios ligados ao ciclo de vida dos dados, ao devido processo informacional, à discriminação algorítmica, ao exercício dos direitos de titulares de dados, entre outros. A fim de se alcançar uma sociedade verdadeiramente justa e democrática, os problemas derivados da tecnologia e do tratamento abusivo de dados devem ser devidamente endereçados e a justiça de dados deve proporcionar um olhar mais atento às questões sociais relevantes, endereçando os impactos discriminatórios e desiguais do tratamento de dados.

Adentrando-nos nas reflexões acadêmicas, uma vertente entende que a justiça de dados deve ser utilizada como uma espécie de janela de onde se enquadra criticamente o debate sobre os dados. A mobilização deste conceito provoca uma mudança no paradigma dos estudos de dados uma vez que implica o necessário reconhecimento das preocupações trazidas pela justiça social e pelas lutas de movimentos sociais contra a desigualdade, opressão e exploração[11]. Por outro lado, há quem defenda que a justiça social implica inserir a discussão sobre dados nas agendas já existentes de justiça social, cultivando um quadro de justiça de dados apto a reorientar as preocupações éticas sobre a datificação não somente a partir de aspectos morais, tecnocráticos ou tecnológicos, mas também por meio de colaborações entre diferentes movimentos e grupos que trazem dimensões tecnológicas, sociais, econômicas, culturais e ecológicas distintas para a definição

9 *Ibid.*

10 Em sua obra, a intelectual e ativista negra Lélia González sustenta que nas sociedades de origem latina, temos o racismo disfarçado ou o racismo por denegação. No Brasil, prevalecem as "teorias" da miscigenação, da assimilação e da "democracia racial". Devido à colonização luso-espanhola, a América Latina herdou as ideologias de classificação racial e sexual e por serem racialmente estratificadas, dispensam-se formas abertas de segregação. Nas palavras da autora, "O racismo latinoamericano é suficientemente sofisticado para manter negros e índios na condição de segmentos subordinados no interior das classes mais exploradas, graças à sua forma ideológica mais eficaz: a ideologia do branqueamento." GONZALEZ, Lélia. A categoria político-cultural de amefricanidade. In: Tempo Brasileiro. Rio de Janeiro, No. 92/93 (jan./jun.). 1988b, p. 69-82.

11 DENCIK, Lina et al, Exploring Data Justice: Conceptions, Applications and Directions, **Information, Communication & Society**, v. 22, n. 7, p. 873–881, 2019.

e solução dos problemas[12].

Através das lentes da justiça de dados, o letramento em dados se dissocia da abordagem puramente técnica, engajando-se na análise sobre como as práticas de dados correspondem a fenômenos e práticas observados socialmente[13]. Em outras palavras, "justiça de dados" é um termo que tem conquistado os estudos de dados, servindo como uma ferramenta conceitual para analisar a relação entre datificação e justiça social[14].

O conceito ainda se encontra em disputa e, por isso, este é o momento para estabelecer quais são os pontos de partida e acima de tudo, o que justiça de dados não representa. Primeiramente, não se pode negligenciar aspectos materiais da pobreza e desigualdade. A análise estrutural pode ser difícil, contudo, é crucial que seja enfrentada.

Em segundo lugar, a justiça de dados deve levar em conta que a datificação dos programas sociais - tal como o Bolsa Família e o auxílio emergencial - pode dar visibilidade a grupos que já sofrem discriminação, acentuando ainda mais sua condição. De fato, a visibilidade é necessária para a desburocratização e cidadania, porém, pode criar novos riscos e exacerbar assimetrias de poder, como bem observado por Mariana Valente e Nathalie Fragoso[15]. A abordagem de justiça de dados aqui defendida considera que os efeitos da datificação são percebidos de forma diferentes a depender do lugar social.

A experiência sistemática de discriminação e exclusão pode tornar determinados grupos sociais receiosos de se tornarem "visíveis" e mais vulneráveis a novas formas de injustiças (ou injustiças pré-existentes, mas mais sofisticadas em razão do tratamento massivo e em larga escala para a promoção de programas sociais e políticas públicas)[16].

Devemos prestar bastante atenção para não adotarmos uma visão essencialmente funcionalista da justiça de dados. A tendência de instrumentalização e a estruturação em pilares pode levar ao esvaziamento do conceito, simplificando-o

12 ZEFFIRO, Andrea, From Data Ethics to Data Justice in/as Pedagogy (Dispatch), **Studies in Social Justice**, v. 15, n. 3, p. 450–457, 2021.

13 *Ibid.*

14 DAGNE, T, Embracing the Data Revolution for Development: A Data Justice Framework for Farm Data in the Context of African Indigenous Farmers, **The Journal of Law, Social Justice and Global Development**, n. 25, 2020.

15 VALENTE, Mariana; FRAGOSO, Nathalie, Data Rights and Collective Needs: A New Framework for Social Protection in a Digitized World.

16 *Ibid.*

de modo a torná-lo somente um "*checklist*" a ser cumprido pelos setores público ou privado. Devemos fugir da armadilha de limitar a justiça de dados a uma "palavra da moda" a ser cooptada pela iniciativa privada como um ativo para incrementar sua imagem de "*privacy friendly*[17]" e posição no mercado, bem como fortalecer a relação de confiança com quem consome tais serviços. A depender da forma como o conceito é construído, há o risco de ser empregado como estratégia discursiva para criar uma falsa imagem de compromisso com a proteção da pessoa titular, tal como funciona o *privacy washing* - isto é, o falso *marketing* social de empresas que desejam construir uma imagem de responsabilidade com a privacidade de clientes, mas que não realizam ações concretas para garantir a proteção de dados[18]. No bojo deste discurso, existe ainda a possibilidade de reduzir a cidadania à figura de "usuário" ou "consumidor".

Até aqui trouxemos reflexões sobre proteção de dados pessoais e justiça social no sistema de Justiça, no mercado e na literatura. Ainda, um elemento indispensável para pensar a proteção de dados pessoais como um instrumento de justiça social é a democratização do debate público sobre esses temas e o empoderamento da cidadania com conhecimento e ferramentas para demandarem justiça no tratamento dos dados.

Enquanto nós pensamos formas de popularizar o debate, experiências maravilhosas surgem em todos os cantos. Comunidades indígenas que se apropriam da tecnologia para legar para as gerações futuras conhecimento ancestral, pensamento crítico sobre dados e tecnologia sendo desenvolvido nas comunidades marginalizadas e periféricas. Vemos também a produção de uma infraestrutura tecnológica que surge dos próprios grupos marginalizados e a utilização subversiva da tecnologia associada a dados pessoais como maneiras legítimas de denunciar e reagir às injustiças provocadas pelo uso abusivo de dados.

Dar destaque para essas e outras experiências implica, sem dúvida, questionar o atual caráter elitista do ativismo digital e a pouca visibilidade e capacidade de incidência política que detém projetos contra-hegemônicos que vêm das margens. É fundamental, portanto, contribuir para uma diversificação maior do campo do ativismo digital, de modo a contemplar verdadeiramente a pluralidade de saberes,

17 "*Privacy friendly*" é uma característica atribuída a empresas, organizações, produtos, serviços e iniciativas que são pensados de maneira a respeitar e garantir a privacidade do titular. A tradução literal seria "amigo da privacidade" ou "amigável à privacidade".

18 FIORINI, Carolina; AVILA NEGRI, Sergio, Dados não pessoais: a retórica da anonimização no enfrentamento à covid-19 e o privacywashing, 2020.

perspectivas e realidades. Um movimento de abertura para acolher e dialogar com os movimentos sociais é chave para popularizar um debate que precisa ganhar o espaço público.

Com esta obra esperamos contribuir para a ampliar a conversa envolvendo justiça social e proteção de dados pessoais para outros públicos, evitando a mera importação do conceito *Data Justice*. Nela, propomos uma reflexão fundamentada em uma instituição do sistema de justiça que lida, justamente, com os desafios que a realidade brasileira de desigualdade e exclusão social impõe à proteção de dados pessoais para um segmento importante da população.

Por final, se o uso da tecnologia, inclusive tecnologia de dados, não serve para melhorar a vida das pessoas mais marginalizadas, se não contribui a ampliar o horizonte de possibilidades para os grupos historicamente excluídos, para projetar uma sociedade verdadeiramente justa, igualitária e democrática, a quem e para quê serve?

Se o uso de determinada tecnologia contribui para perpetuar relações de opressão, para promover a estigmatização de grupos, para o controle e vigilância dos corpos das mulheres e de pessoas negras, para excluir sexualidades não binárias, por quê insistir no seu uso?

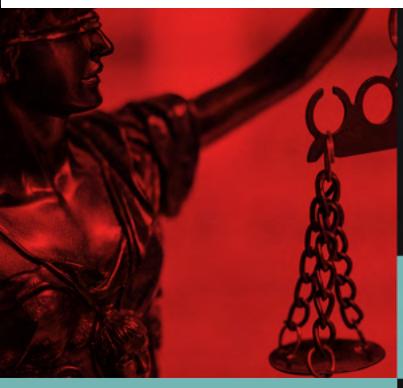
A classificação e organização dos nossos dados pessoais são fundamentais para a tomada de decisões governamentais e para o mercado, em diversos aspectos. Nossa esperança é que o tratamento e a proteção de dados pessoais sejam úteis para criar uma sociedade mais justa, para a reafirmação de direitos, cidadania e democracia, para projetos emancipatórios, assim como para permitir a existência das pessoas que pertencem aos grupos historicamente discriminados e invisibilizados.

O livro "***Construindo caminhos para a justiça de dados no Brasil: o papel das Defensorias Públicas na proteção de dados pessoais***" se soma a um movimento de (re)compreensão da proteção de dados pessoais como um instrumento de justiça social, considerando, ainda, o protagonismo das Defensorias Públicas na concretização dos direitos da população mais vulnerável.

Enquadrar a proteção de dados pessoais a partir de uma perspectiva de justiça social implica reconhecer que a forma em que se organizam as relações sociais, econômicas e políticas neste país é essencialmente desigual e que se requerem ações concretas para a efetivação do direito fundamental à proteção de dados como instrumental ao pleno exercício da cidadania.

Este livro digital revela-se como uma ferramenta relevante não somente para a produção acadêmica, mas também para auxiliar a construção de uma política pública no sistema de justiça, ampliando o debate público sobre proteção de dados e justiça social no Brasil.

Bruno Bioni | Hana Mesquita | Johanna K. Monagreda | Rafael Zanatta



ISBN: 978-65-997956-0-2
9 786599 795602

DataPrivacyBR Research