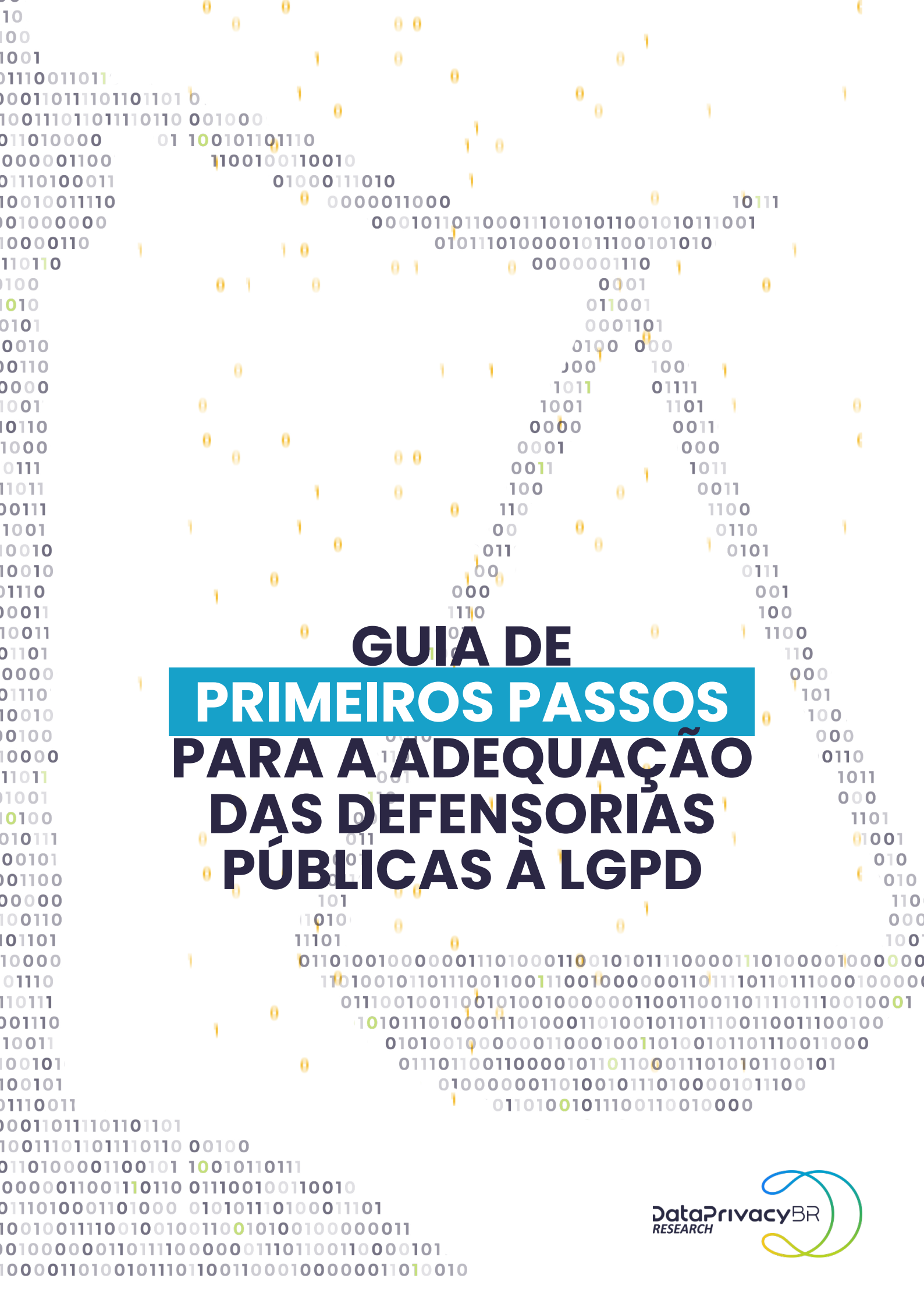
GUIA DE PRIMEIROS PASSOS PARA A ADEQUAÇÃO DAS DEFENSORIAS PÚBLICAS À LGPD



FICHA TÉCNICA

O Data Privacy Brasil é um espaço de intersecção entre a escola Data Privacy Ensino e a entidade civil Associação Data Privacy Brasil de Pesquisa. Este relatório foi produzido exclusivamente pela Associação. A Associação Data Privacy Brasil de Pesquisa é uma 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 desenvolve projetos estratégicos de pesquisa em proteção de dados pessoais, mobilizando conhecimentos que podem ajudar reguladores, juízes e profissionais do direito a lidar com questões complexas que exigem conhecimento profundo sobre como tecnologias e sistemas sócio-técnicos afetam os direitos fundamentais. A Associação possui financiamento de filantropias internacionais como Ford Foundation, Open Society Foundations e AccessNow. Para mais informações, visite www.dataprivacybr.org.

DIRETORES
Bruno Bioni e Rafael Zanatta

COORDENADORA GERAL DE PROJETOS
Mariana Rielli

COORDENADORES
Bruna Martins dos Santos, Daniela Dora Eilberg e João Paulo Vicente

PESQUISADORES
Aline Hercocivi, Brenda Cunha, Gabriela Vergili, Helena Secaf, Izabel Nuñez, Jaqueline Pigatto, Júlia Mendonça, Marina Kitayama, Pedro Saliba e Thaís Aguiar

ADMINISTRATIVO E COMUNICAÇÃO
Ana Justi, Fabrício Sanchez, Gustavo Reis, Rafael Guimarães, Roberto Júnior e Victor Scarlato

IMPRENSA

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

APOIO

Ford Foundation

COMO CITAR ESSE DOCUMENTO

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.

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 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[1]

"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.

[1] Doutora em Ciência Política pela Universidade de São Paulo e Pós-Doutora pelas Universidades da Califórnia, de São Paulo e de Londres. Colaboradora da Fundação Getúlio Vargas RJ, pesquisadora sênior e diretora de pesquisas do Centro Brasileiro de Estudos e Pesquisas Judiciais, membra da Comissão de Pesquisa e Inovação da Fundação Getúlio Vargas, é Professora Doutora da Universidade de São Paulo e Professora no Mestrado Profissional do CEDES. Foi membra da Comissão de Altos Estudos em Administração da Justiça, integrante do Conselho Consultivo Interinstitucional do Tribunal de Justiça do Estado de São Paulo e Conselheira do Conselho Nacional de Autorregulamentação Publicitária. Além disso, foi integrante do Conselho de Pesquisas e Estudos Eleitorais do Tribunal Superior Eleitoral, Diretora Executiva do Departamento de Pesquisas Judiciárias do Conselho Nacional de Justiça.

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 Defensoria 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.

SUMÁRIO

PARTE I

Contextualização do projeto, desafios e perspectivas de um processo de adequação à LGPD

1. 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[2].

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 digitalização 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.

[2] 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.

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[3]. 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?

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

[3] 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.

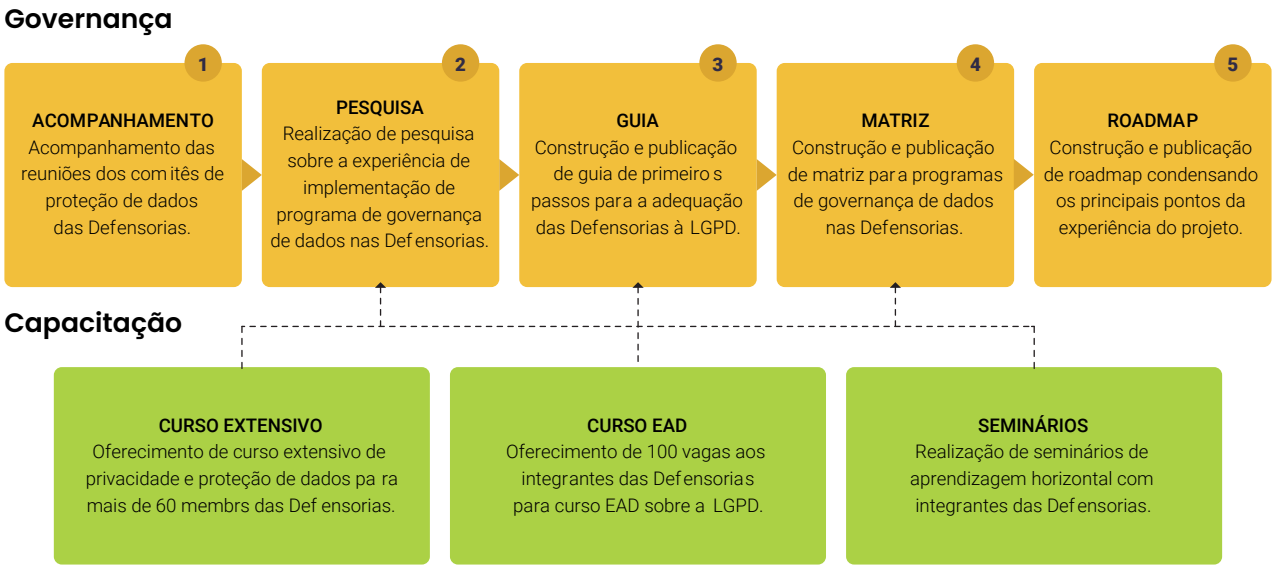
modo colaborativo. Tendo em vista a complexidade do projeto, não seria possível estabelecer parcerias formais com todas as Defensorias Públicas do país, de modo que a Associação optou por firmar convênios com os dois maiores entes (em termos de número de defensores e de atendimentos realizados) sendo 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[4]. A série de diálogos e trocas, além de aproximar a Associação dos membros das Defensorias, deu origem ao seminário de lançamento do projeto[5], 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.

[4] 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.

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

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[6], 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 n° 1090[7], que institui sua política de governança de dados.

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[8]. 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

[6] 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

[7] DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO. Resolução DPGERJ n° 1090 de 09 de abril de 2021.

[8] 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

adaptarem a normativas de proteção de dados no âmbito internacional, tais como a GDPR[9] e instruções da OCDE[10]. Apesar de empresas 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[11]) e também acentuaram o aparecimento de questões diretamente relacionadas à redução de renda da população (como casos de pensão alimentícia[12]). 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

[9] 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/

[10] 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/

[11] Ver: https://www.defensoria.to.def.br/list_tag/UTI e http://www.defensoriapublica.go.gov.br/depego/index.php?option=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

[12] 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

Defensorias, de modo que práticas como o compartilhamento 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[13]. 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.

[13] 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"[14] 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.

[14] A expressão "gratuito" é utilizada em razão da impossibilidade de precificação das informações pessoais compartilhadas pelo usuário, as quais, neste tipo de modelo de negócio, servem como ativo para diversos usos comerciais, sendo o direcionamento de anúncios o mais conhecido destes.

- 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 II

Lei Geral de Proteção de Dados: origem e estrutura

2. 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)[15].

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 seus usuários.

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

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[16], 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[17].

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[18]. 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[19].

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 atuação 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.

[16] 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

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

[18] 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.

[19] 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.

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.

3. 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 interoperabilidade, 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.

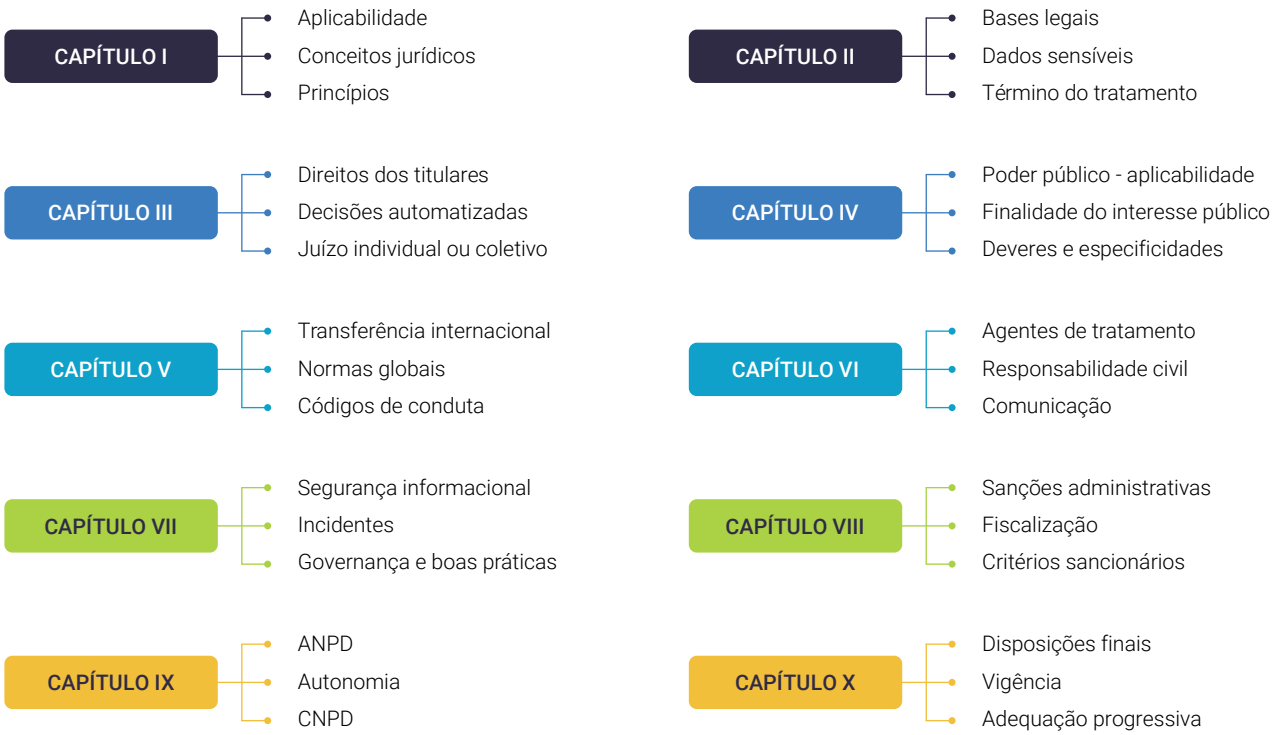
O capítulo oito, sobre fiscalização, abarca disposições sobre as sanções administrativas aplicáveis pela Autoridade no caso de descumprimento da Lei. Além de prever os diferentes tipos de penalidades, que variam entre advertências, multas até o valor de 50 milhões de reais e a proibição das atividades 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 III

Desmistificando o Processo de Adequação à LGPD

4. 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[20]. 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:

[20] 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

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 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[21]

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.

5. 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,

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

promoção de políticas públicas e da justiça em um sentido amplo -, destacamos em seguida alguns pontos de reflexão sobre cada um desses aspectos.

a. Atividado-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[22]: prevenção e proatividade, privacidade como padrão, privacidade incorporada ao design, funcionalidade ampla, segurança de ponta a ponta, transparência, respeito à privacidade do usuário.

Planejamento estratégico e política para área de tecnologia da informação

Planejamento estratégico[23]: 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:

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

[23] 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

- **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[24]**:** 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.

- 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.

[24] 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

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[25]. 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 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.

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

- **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.

As Defensorias no processo de fiscalização e interpretação da LGPD

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[26] 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

[26] 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.

de profundas desigualdades[27]. Assim, sem as devidas precauções, a tendência é 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 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.

[27] 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_coletivizacao_da_protecao_de_dados_pessoais/links/60764caf92851cb4a9dc18e6/Tutela-coletiva-e-coletivizacao-da-protecao-de-dados-pessoais.pdf

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[28], 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.

[28] 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 IV

Colocando em prática um Projeto de Adequação

6. 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[29], 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.

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.

[29] 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.

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[30] ou, por exemplo, quando fatores discriminatórios influenciam o preço pago para se adquirir um plano de saúde ou ter acesso à crédito[31]. 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 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:

30 https://www.nexojornal.com.br/expresso/2020/06/14/Reconhecimento-facial-a-suspens%C3%A3o-da-venda-para-a-pol%C3%ADcia

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

- 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 importantes para endereçar objetivos concretos e compartilhados pelo agente[32].
- 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[33].
- Demonstrar bons resultados já obtidos por meio da transformação tem grande valia[34]. Já existem exemplos, inclusive citados neste guia[35], 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[36].
- Os movimentos de mudança são baseados em uma visão compartilhada de futuro da instituição[37], tratando-se de um processo cíclico[38]:

  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.
  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.

[32] WALKER, Bryan e SOULE, Sarah A. Changing Company Culture Requires a Movement, Not a Mandate. Harvard Business Review. Jun. 2017.

[33] Ibidem.

[34] Ibidem.

[35] Como na atuação da DPE-RJ sobre o aumento das demandas relativas à falta de vagas em creches, p. 29.

[36] WALKER, Bryan e SOULE, Sarah A.

[37] Medium. How to change your company culture: a four step framework. 2018.

[38] Ibidem.

- Entender como e por que padrões de rotina indesejados se repetem é outra questão a ser considerada[39]. 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[40].

7. 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 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

[39] Medium. Changing Culture: Shift Small Habits for Big Wins. 2016.

[40] Ibidem.

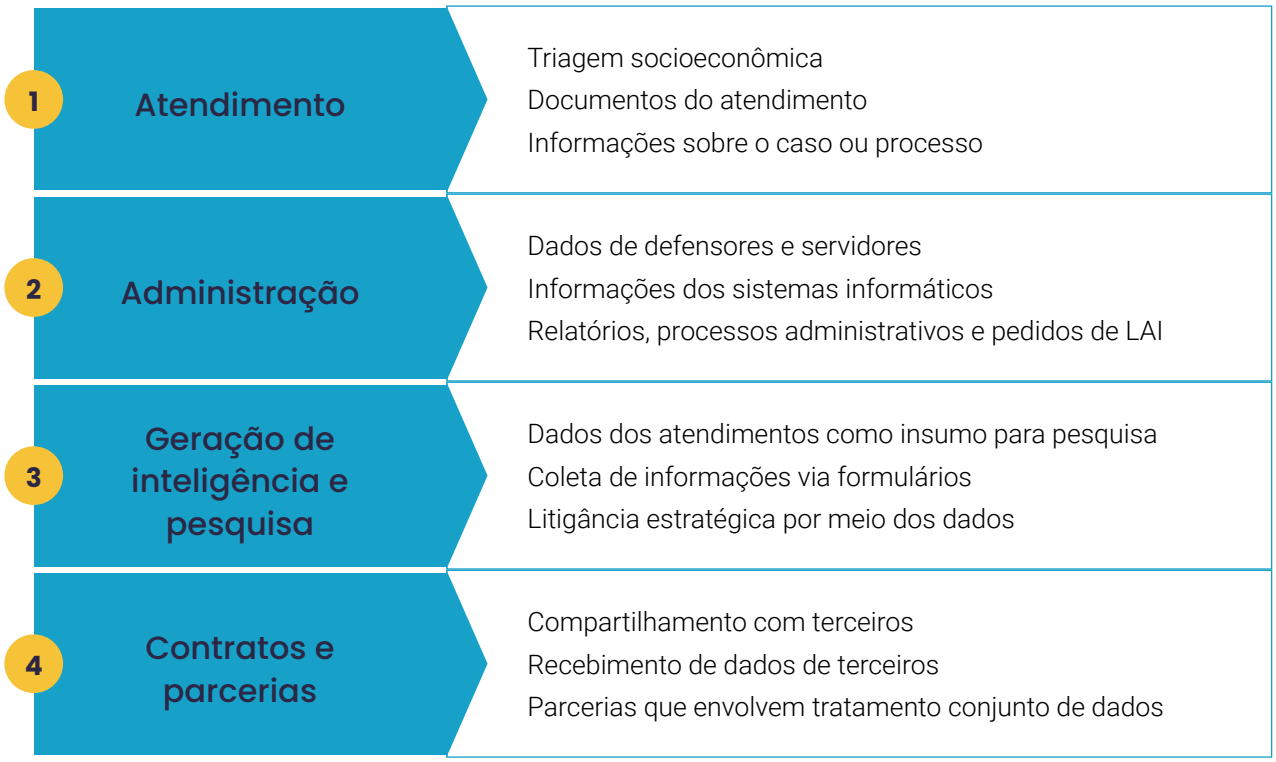
para que com isso seja possível mitigá-los sem o comprometimento das atividades necessárias ou importantes. Assim, o objetivo deste Guia vai além de trazer aspectos para que a instituição garanta sua conformidade em relação à LGPD, mas principalmente busca mostrar como os processos de adequação e de 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.



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