Oficina Prática de Adequação à LGPD

Defensorias Públicas e Proteção de Dados
05 e 07 de julho de 2021
12 de agosto de 2021

RELATÓRIO DAS DISCUSSÕES DO EVENTO

DataPrivacyBR
Research

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.

Imprensa

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

Diretores

Bruno Bioni e Rafael Zanatta

Coordenadora Geral de Projetos

Mariana Rielli

Líder Geral de Projetos

Marina Meira

Coordenadores

Daniela Dora Eilberg, Johanna Monagreda e Helena Secaf

Pesquisadores

Brenda Cunha, Gabriela Vergili, Hana Mesquita, Jaqueline Pigatto, Júlia Mendonça, Marina Garrote, Nathan Paschoalini, Pedro Saliba e Thaís Aguiar

Administrativo e Comunicação

Erika Jardim, Fabrício Sanchez, Gustavo Reis, Júlio Araújo, Rafael Guimarães, Roberto Júnior, João Paulo Vicente e Victor Scarlato

Revisora

Maraísa Rosa Cezarino

Como citar esse documento

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

Sumário

1. Introdução [1]

A Associação Data Privacy Brasil de Pesquisa realizou o evento **Oficina Prática de Adequação à Lei Geral de Proteção de Dados** nos dias 05 e 07 de julho e 12 de agosto de 2021 com o objetivo de promover o intercâmbio de experiências horizontais entre Defensorias Públicas de todo o país no que diz respeito aos desafios da adequação do ente à Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), considerando a vigência da legislação desde setembro de 2020[2].

A Oficina ocorreu dentro do escopo do projeto Defensorias Públicas e Proteção de Dados, promovido pela Data Privacy Brasil em parceria com o Conselho Nacional das Defensoras e Defensores Públicos-Gerais (Condege) e as Defensorias Públicas Estaduais do Rio de Janeiro e de São Paulo. O projeto nasceu a partir da necessidade de se pensar na adequação do sistema de Justiça à LGPD e no papel das Defensorias na promoção do acesso à justiça.

Afinal, ao realizar o atendimento de milhões de cidadãos brasileiros por ano, as Defensorias Públicas tratam dados pessoais de milhões de pessoas em situação de maior vulnerabilidade que buscam esse serviço público garantido constitucionalmente. Além disso, as Defensorias também são agentes centrais na defesa de direitos da população frente ao uso abusivo de dados pessoais de modo que a LGPD impacta tanto a atividade-fim quanto a atividade-meio.

Nesse sentido, o projeto foi estruturado para contemplar duas frentes de atuação: a primeira delas, implementada em parceria com a Escola Data Privacy Brasil, foi a de realizar a formação das pessoas designadas para participar nos comitês de proteção de dados, constituídos para promover a adequação da instituição.

Assim, houve a promoção de um curso extensivo, no segundo semestre de 2020, que contou com a participação de 66 alunos, membros de 14 Defensorias Públicas estaduais brasileiras, reunindo as 5 regiões brasileiras.

1 A Associação Data Privacy Brasil de Pesquisa registra a valiosa e imprescindível contribuição da pesquisadora Marina Kitayama que trabalhou empenhadamente ao longo dos últimos meses no projeto Defensorias Públicas e Proteção de Dados. Kitayama foi responsável pela condução da Oficina Prática, coletando grande parte dos dados utilizados na elaboração deste relatório.

2 Sobre a história da LGPD, ver o documentário "Memória da LGPD" disponível no Observatório da Privacidade da Associação Data Privacy Brasil de Pesquisa. Disponível em: <https://www.observatorioprivacidade.com.br/memorias/>.

Em seguida, em parceria com o Condege, foram disponibilizados acessos ao curso EAD do Data Privacy Brasil, para diversas Defensorias Públicas ao redor do Brasil. O curso EAD foi finalizado em abril de 2021 e disponibilizou o total de 121 vagas. Posteriormente, existe a expectativa de realização de alguns seminários sobre temas importantes para destravar a adequação da instituição à LGPD.

É importante ressaltar que, antes da formulação do programa desses cursos, foram realizadas uma série de entrevistas para compreender que tipo de conteúdo poderia ser interessante de apresentar aos integrantes das defensorias, diante das especificidades das atividades de tratamento de dados dentro dessas instituições.

Já a segunda frente, de Governança, é voltada ao acompanhamento das reuniões dos comitês de proteção de dados que se formaram no Rio de Janeiro e em São Paulo. Nessa segunda parte do projeto, o Data Privacy Brasil participou como ouvinte de cinco reuniões com a Defensoria Pública de São Paulo e três reuniões com a Defensoria Pública do Rio de Janeiro no intuito de compreender o que tem sido feito para promover a conformidade das Defensorias Públicas Estaduais à LGPD, bem como quais são os principais desafios enfrentados pela instituição.

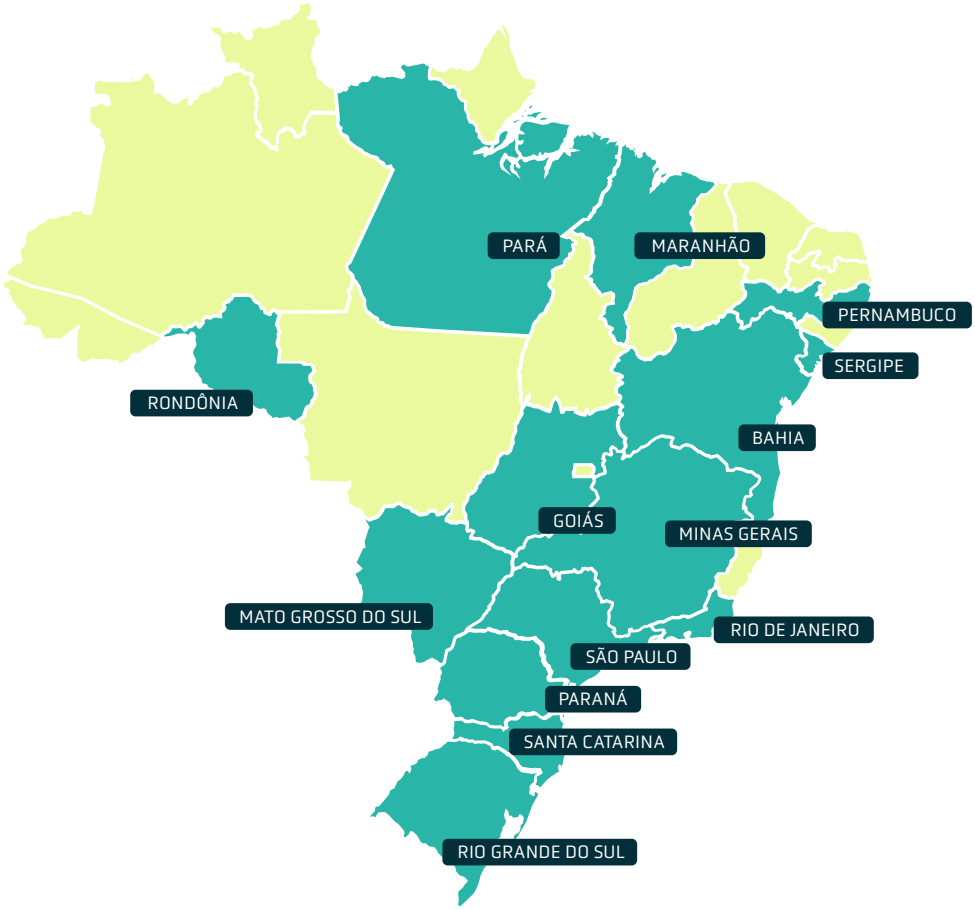
Devido à compreensão derivada da presença nesses espaços, foram produzidos um Guia de Adequação para essas instituições e outros materiais que poderão auxiliar a destravar o processo de adequação, como, por exemplo, templates de formulários que poderão ser mobilizados para o mapeamento e, depois, para a compreensão contínua do nível de adequação atingido pelas Defensorias, além de um roadmap de adequação para essas instituições.

As duas frentes estão relacionadas com o caráter cíclico que se deseja dar ao projeto defensorias, ou seja, ao mesmo tempo em que buscamos formar as pessoas que trabalham na instituição, também buscamos compreender quais são as potencialidades e desafios desse processo, a fim de produzir materiais que possam facilitar a tarefa de estar em conformidade com a LGPD. Isso porque, entendemos que um projeto de adequação de uma instituição como a Defensoria Pública é permeado por particularidades que não são contempladas pela metodologia usualmente utilizada para a adequação em organizações privadas.

Nesse sentido, muito do trabalho nesta segunda frente do projeto diz respeito ao enfrentamento da necessidade de moldar a metodologia de adequação à LGPD, usualmente utilizada no setor privado, aos desafios e potencialidades expostos pelos defensores nas reuniões dos Comitês de Proteção de Dados no rio de Janeiro e em São Paulo, por meio da nossa participação como ouvintes nesses espaços. Assim, é importante reforçar a atuação passiva do Data Privacy Brasil nesses espaços, onde o que se buscou foi a compreensão dos desafios enfrentados pelas Defensorias e não a resolução de dúvidas ou realização de sugestões práticas para promover a conformidade com a LGPD.

Isso é necessário para que a conformidade com a lei não seja encarada como um processo paralisante, mas, pelo contrário, como um projeto que traz a possibilidade de rever atividades ou fluxos de tratamento que ocorrem de forma ineficiente ou desatualizada.

Assim, o presente relatório consolida as discussões realizadas no bojo da **Oficina Prática** que reuniu representantes de Defensorias de todo o Brasil e contou com a presença de cerca de 60 participantes:



No primeiro dia de oficina, 05 de julho, discutiu-se aspectos da proteção de dados em sistemas integrados de cadastramento e a realização do atendimento por vias remotas. No segundo dia, a discussão girou em torno dos convênios e contratos que envolvem o compartilhamento de dados e das estratégias e pontos sensíveis da estruturação e implementação de um programa de adequação à LGPD.

No terceiro dia, a discussão se baseou nos enunciados elaborados pelos participantes. Os enunciados partem dos tópicos de discussão dos primeiros dois dias de Oficina e indicam a interpretação do grupo acerca de um dispositivo da LGPD. Alguns grupos não desenvolveram os enunciados, porém isso não inviabilizou o debate acerca dos temas propostos pela equipe do Data Privacy Brasil.

Para conferir a programação e os casos práticos trabalhados na Oficina, basta conferir o Anexo (Dossiê Oficina Prática).

2. Organização do evento

2.1. OBJETIVO PEDAGÓGICO

O principal objetivo da Oficina foi promover o intercâmbio de experiências horizontais entre Defensorias Públicas, dando maior protagonismo aos Defensores para debater os desafios da adequação do ente à LGPD e à implementação de programas de governança de dados. Nesse sentido, o evento reuniu integrantes de diferentes Defensorias brasileiras, as quais se encontram em estágios distintos de processos de adequação e apresentam inúmeras particularidades que afetam a implementação de seus programas. A pluralidade e as diferentes perspectivas sobre o tema foram fundamentais para a construção deste relatório que sintetiza esse rico debate entre os membros da instituição

Assim, o evento se propôs a: (i) estabelecer uma rede de contatos entre integrantes de diferentes Defensorias Públicas engajados no processo de adequação; (ii) colaborar com a identificação de desafios particulares da instituição no tocante à implementação de um programa de governança de dados; (iii) colaborar com possíveis saídas de enfrentamento para os problemas identificados; (iv) identificar aspectos positivos de um programa de adequação que vão além da conformação legal e que contribuam com a missão institucional das Defensorias e; (iv) gerar materiais de pesquisa para a construção de documentos de suporte que poderão servir de apoio a todas as Defensorias do país e outros entes públicos.

2.2. METODOLOGIA

Todos os temas abordados na Oficina são casos concretos compartilhados por diferentes Defensorias Públicas ao redor do Brasil. Foram constituídos dois comitês: um Comitê de Defensores formado por representantes das Defensorias envolvidos nos programas de adequação do ente à LGPD e um Comitê Executivo formado pelos pesquisadores da Associação Data Privacy Brasil de Pesquisa.

O Comitê de Defensores enviou à equipe do Data Privacy Brasil relatos sobre as experiências de seus respectivos órgãos durante o processo de adequação à LGPD. A partir da coleta e análise de experiências, os casos foram divididos em **três eixos temáticos**:

1. Estruturação do comitê de proteção de dados, desafios organizacionais, divisão de tarefas, nomeação de encarregado, programa de conscientização interna;

2. Atividade-meio, desafios relacionados ao tratamento de dados envolvidos nas atividades administrativas e gerenciais da Defensoria, incluindo registros de relatórios, tratamento de dados de defensores e servidores, segurança de sistemas informáticos, contratos e parcerias;

3. Atividade-fim, desafios relacionados ao tratamento de dados envolvidos nas atividades finais das Defensoria, incluindo triagem, registro em sistemas integrados, trocas de documentos e informações por aplicativos, etc.

A equipe do Data Privacy Brasil identificou dentro de cada eixo questões recorrentes e pontos sensíveis, os quais foram apresentados, como ponto de partida para as discussões e trocas de saberes entre os participantes. Todo o processo de seleção de temas e tópicos se originou de trabalho conjunto entre o Comitê de Defensores e a Data Privacy, por meio de trocas de mensagens e reuniões ao vivo.

2.3. DINÂMICA DO EVENTO

A Oficina contou com a presença de cerca de 60 participantes, número estabelecido a fim de comportar uma média de ao menos dois representantes por cada Defensoria Estadual brasileira. Em virtude da pandemia e, também, pensando na inclusão de integrantes de diversas regiões, o evento teve duas horas de duração em cada dia e foi realizado remotamente através da plataforma Zoom.

Nos dois primeiros dias foram discutidos dois grandes tópicos, sendo que cada encontro foi estruturado em quatro partes:

1. **Primeira parte:** Apresentação dos tópicos identificados a partir do compartilhamento de casos.

2. **Segunda parte:** Apresentação de algumas das experiências relacionadas ao tópico e observadas pelos integrantes do comitê de Defensores.

3. **Terceira parte:** Discussão em grupos menores sobre alguns aspectos específicos a respeito de determinado tópico (apresentados em formato de casos), aqui ainda foi reservado um espaço para apresentações e feedbacks dos demais participantes.

4. **Quarta parte:** Considerações finais da equipe da Data Privacy sobre os pontos apresentados e discutidos.

No último dia de Oficina, os participantes discutiram de forma mais livre sobre os tópicos trabalhados anteriormente a partir dos enunciados elaborados de forma assíncrona.

O texto que segue abaixo representa um esforço de sistematização das discussões e experiências compartilhadas na Oficina, buscando sintetizar, no formato de enunciados, os principais entendimentos sobre os desafios e potencialidades da adequação à LGPD das Defensorias Públicas brasileiras. Cumpre destacar que o presente relatório expressa as diferentes visões e percepções dos participantes, porém, não reflete necessariamente a posição do Data Privacy Brasil.

3. Síntese das discussões

Ao longo dos três dias de Oficina, as principais **reflexões** e **desafios** identificados foram:

- Restrição de acesso ao sistema integrado e as implicações na rotina de trabalho do defensor;
- Padronização do cadastramento de informações em um sistema integrado e o potencial comprometimento da autonomia funcional dos defensores;
- Institucionalização do uso do WhatsApp e possíveis alternativas ao aplicativo para agendamento e atendimento remoto;
- Existência de duas categorias de dados pessoais (essenciais para o peticionamento x utilizados para fins de políticas públicas) e a atribuição de bases legais para tratamento (art. 7º e art. 11 da LGPD);
- Riscos do compartilhamento, com outros entes privados e públicos, de dados por meio de contratos e convênios e, portanto risco de violação aos princípios da finalidade e da transparência;
- Identificação do controlador x operador nas relações contratuais;
- Dificuldade de exercer o controle sobre o que é realizado com os dados compartilhados para fins de pesquisa;
- Definição das atribuições do Encarregado[2] e o papel do Comitê de Proteção de Dados no curso do processo de adequação;

3.1. DINÂMICA DO EVENTO

Os sistemas integrados são ambientes digitais que concentram todas as informações necessárias à efetivação das atividades fim das Defensorias, ou seja, a atividade de atendimento e de ingresso com ações em nome dos assistidos. Esses sistemas, concentram dados cadastrais, dados da triagem e dados referentes aos casos, por exemplo documentos probatórios utilizados para ingressar com a ação.

3 O encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

As Defensorias Públicas brasileiras utilizam sistemas integrados de armazenamento e cadastro de dados pessoais dos usuários, por exemplo, o sistema Solar (Solução Avançada em Atendimento de Referência)[4]. Desenvolvido pela Defensoria Pública do Estado do Tocantins (DPE-TO), o Solar se tornou referência nacional, sendo amplamente utilizado pelas Defensorias de todo o país. Por sua vez, a Defensoria Pública do Estado do Rio de Janeiro utiliza o sistema Verde[5], enquanto a Defensoria de São Paulo trabalha com o sistema DOL[6].

Esses sistemas trouxeram mudanças significativas para a rotina de trabalho dos defensores uma vez que permitem a centralização das informações, otimizando as atividades empenhadas. Tendo em vista que a unidade é um princípio institucional, é fundamental que todas as informações sejam registradas e possam ser acessadas por todos.

Um único repositório de informações garante maior governabilidade, reduzindo as chances de eventuais duplicidades e inconsistências do cadastro de modo que o princípio da qualidade dos dados pessoais seja respeitado. Ao mesmo tempo, entende-se que há um risco atrelado a esse benefício, qual seja o de garantir o controle de acesso às informações inseridas nesses sistemas. Uma solução para esta falha é estabelecer um gerenciamento de identidade para acesso ao sistema.

4 O Solar compila informações desde o primeiro atendimento, registrando todo o histórico processual. Além disso, o sistema permite a checagem das informações do assistido por meio da realização de cadastro, bem como o acesso a documentos, à matéria do caso, e a peças processuais. Existe ainda a possibilidade da criação de agendas dos atendimentos, com a inserção de datas e prazos, a produção de relatórios e obtenção de dados estatísticos, como número total de atendimentos, ou número de atendimentos de determinada natureza, por exemplo. Fonte: <https://www.defensoria.ro.def.br/site/index.php/component/content/article/1-ultimas-noticias/1754-2018-07-23-19-52-01>.

5 O Sistema Verde foi criado por técnicos da Coope/UFRJ com a finalidade de oferecer à Defensoria do Rio ferramentas de informática capazes de integrar rotinas e procedimentos de todos os órgãos de atuação. O sistema tem como objetivo automatizar tarefas repetitivas e registrar e organizar informações que os defensores públicos recebam e produzam, além de tornar possível a formulação de estatísticas, importação de dados de outros sistemas e, consequentemente, dispensa de buscas e pesquisas de dados em outros ambientes. Fonte: <https://defensoria.rj.def.br/noticia/detalhes/3883-Sistema-Verde-e-apresentado-aosdefensores-de-primeiro-atendimento>.

6 O sistema DOL é um conjunto de módulos de sistemas computacionais com finalidade de organizar e armazenar dados cadastrais e processuais, oficiais e de mero expediente, referentes aos usuários, Unidades e Regionais da Defensoria Pública. O DOL foi desenvolvido a partir de três premissas: usabilidade, otimização das informações e produção de dados estratégicos e foi estruturado em três grandes áreas: (1) atendimentos; (2) acompanhamento de processos e seus respectivos atendimentos e (3) atividades administrativas relacionadas diretamente à atividade fim. Fonte: <https://www.defensoria.sp.def.br/dpesp/Repositorio/0/Documentos/Manual%20Defensoria%20Online%20-%20fev2014.pdf>.

Nesse contexto, as Defensorias enfrentam no seu dia-a-dia alguns desafios quanto ao acesso ao sistema, bem como quanto à padronização e centralização do cadastramento.

Principais preocupações e riscos identificados

- Possibilidade da Defensoria atender partes distintas de um mesmo processo, o que em determinadas circunstâncias gera receio dos defensores de inserir certas informações em sistemas integrados e abertos a outros membros da instituição;
- Receio de que as informações confiadas pelo usuário dos serviços da Defensorias possam ser utilizadas em seu desfavor pela própria instituição.
    - **Exemplo 1:** Em processo de alimentos, ambas as partes são representadas por membros da Defensoria. Um defensor acessa o sistema e obtém os dados da parte adversa sobre a renda.
    - **Exemplo 2:** Em uma situação que os dados de residência de um atendimento sejam utilizados para realizar a citação do próprio usuário em outro processo ou dados de vínculo empregatício sejam utilizados para indicar a possível penhora de verbas.
- A padronização de cadastramento de informações, dificuldade de estabelecer o mínimo de informações que deve ser coletado, bem como o acesso ao sistema integrado pode afetar a autonomia funcional dos defensores. Em muitas Defensorias, cada Defensor dispõe de liberdade para determinar se um caso deveria ter acesso mais restrito ou não, tratando-se de uma escolha notadamente individual.
- Fomento ao uso dos sistemas criados para integrar o tratamento de dados. Muitos defensores ou pessoas em cargos administrativos, podem utilizar programas próprios, com os quais já existe familiaridade como o Pacote Office, para tratar os dados pessoais e existe resistência à mudança dessa cultura de "autonomia".
- Dificuldade de mobilizar os defensores para responder a outros dados pessoais que podem gerar a produção de políticas públicas, e que não necessariamente são utilizados para o atendimento do usuário
- Perigo de desumanização do atendimento quando há a opção pelo Chatbot para o atendimento;
- Servidores de aplicativos de mensagens como o Whatsapp;
- Autenticação do titular de dados que está pedindo informações às Defensorias. Existem hipótese nas quais o usuário da Defensoria se encontra impedido de solicitar informações diretamente à instituição de modo que seus familiares ou demais interessados no caso fazem as solicitações em nome do usuário. Nesses casos, existe o desafio de autenticar a titularidade dos dados pessoais, bem como do vínculo entre o solicitante e o usuário.

Medidas de mitigação de risco sugeridas

- Criação de restrições conforme a área e nível de atuação, estabelecendo critérios granulares (Ex: diferenciar acesso de quem está alocado na área civil e criminal ou diferenciar estagiário, servidor e defensor);
- Construção de Perfis de Acesso;
- Imposição de sigilo em determinados procedimentos, para que somente o defensor ou acessor daquela área específica pode acessar o procedimento;

- Utilização de ferramentas como logs de acesso que tornam possível identificar quem acessou determinado procedimento.
- Buscar acordos institucionais entre a empresa e a Defensoria.
    - **Exemplo:** Estabelecer um acordo institucional entre a Defensoria Pública e o Whatsapp para a garantia do direito à proteção de dados dos cidadãos.

Observação: Destacou-se que não necessariamente deve-se replicar o mesmo procedimento de sigilo adotado pelos tribunais de justiça.

Tendo em mente os desafios em questão, os participantes elaboraram o enunciado abaixo:

ENUNCIADO

Art 6º, *caput* e incisos: *Os usuários de um sistema integrado da Defensoria Pública precisam ter perfis de acesso limitados aos casos vinculados às respectivas atribuições do cargo, a fim de que sejam respeitados os princípios da prevenção e da segurança no tratamento de dados pela Defensoria. Os times de segurança da informação devem implementar respectivos controles e sistemas de gerenciamento de identidades.*

3.2. ATENDIMENTO REMOTO

Afora a quantidade massiva de atendimentos e, consequentemente, de dados pessoais tratados, ainda deve-se somar o processo de digitalização da sociedade. Acelerado pela crise do COVID 19, esse processo acentua uma série de desigualdades e torna extremamente desafiador o trabalho das Defensorias Públicas, no Brasil, sendo uma das consequências imediatas do isolamento social a necessidade de digitalização de seu atendimento.

A instituição, sem uma grande disponibilidade de ferramentas tecnológicas próprias para tanto, se viu obrigada a encontrar soluções alternativas disponíveis no mercado, as quais eram, muitas vezes, financeiramente bancadas pelos próprios defensores[7]. Nesse contexto, a principal ferramenta utilizada foi o *WhatsApp*, que funciona como um portal de acesso à instituição. Por meio da ferramenta, os usuários entram em contato com a Defensoria Pública, agendam atendimento, esclarecem dúvidas e enviam documentos e demais informações pessoais.

7 ZANATTA, Rafael; KITAYAMA, Marina. O desafio da LGPD para as Defensorias Públicas no Brasil. In. *Lei Geral de Proteção de Dados e o Poder Público*. Organizadores: Daniela Copetti Cravo, Daniela Zago Gonçalves da Cunda e Rafael Ramos. Tribunal de Contas do Estado do RS. Prefeitura de Porto Alegre Porto Alegre. 2021. p. 171 - 183.

Assim, a utilização do *WhatsApp* tem sido uma das grandes aflições desde a entrada em vigor da LGPD na medida em que alguns defensores não conseguem visualizar um cenário em que não se utilize a ferramenta. As Defensorias Públicas brasileiras vivem o seguinte dilema: Considerando que o *WhatsApp* é uma ferramenta acessível e democrática, o que facilita o acesso à Justiça, caberia às Defensorias Públicas abandonarem o atendimento e agendamento via *WhatsApp*?

Pensando em enfrentar tal desafio, os participantes elaboraram o seguinte enunciado:

ENUNCIADO

Art 6º, *caput* e incisos: *O uso de aplicativos de comunicação para contato com usuários da Defensoria Pública deve ser realizado com observância aos princípios da segurança e prevenção (art. 6º, incisos VII e VIII da LGPD).*

A utilização de tais aplicativos deve ser regulamentada pela instituição, a fim de que sejam adotadas boas práticas para prevenir incidentes, como a utilização de autenticação de dois fatores e a exclusão periódica de documentos e informações pessoais armazenadas em nuvem.

PARA REFLETIR...

- Seria possível criar uma política de uso para utilização do *WhatsApp*? Ex. Nenhum número de *WhatsApp* pessoal seria utilizado, somente o número institucional;
- Quem seria responsável pela regulamentação do uso de aplicativos de mensageria? O encarregado ou a própria Defensoria Pública por meio de resolução?
- A regulamentação também seria aplicável para a comunicação entre defensores e não somente entre defensor e usuário?
- Considerando o compartilhamento de dados entre o *WhatsApp* e o *Facebook*, caberia à Defensoria Pública avisar o usuário sobre o compartilhamento, já que utiliza a ferramenta como principal meio de comunicação?
- Tem se observado uma tendência de desenvolvimento de aplicativos próprios pelas Defensorias Públicas com eventual integração com o *WhatsApp*;
- Ainda haveria a necessidade de se utilizar o *WhatsApp* se fosse desenvolvido um aplicativo de fácil navegabilidade e compreensão pelas Defensorias?

TROCANDO EXPERIÊNCIAS

Como uma alternativa ao *WhatsApp*, a Defensoria Pública do Estado de São Paulo adotou a ferramenta de chatbot (LiveChat) na página inicial da Defensoria. A ferramenta, lançada em agosto de 2020, busca agilizar e garantir um atendimento mais célere e dinâmico, diminuindo também a necessidade de deslocamentos físicos a prédios da Defensoria, que, em razão da pandemia de Covid-19, recebem apenas atendimentos agendados e em número reduzido. O assistente virtual "DEFI" é um sistema de conversa online (chat) com respostas automatizadas por meio de inteligência artificial, criado para receber informações básicas dos usuários da Defensoria (ex: nome, CPF e renda familiar), compreender a demanda e encaminhar à unidade competente para atendimento. Por meio desse sistema, os usuários podem optar por um dentre os horários e datas disponíveis na agenda da unidade e marcar seu atendimento. Feito o agendamento, a pessoa recebe uma senha para acesso a um chat com a equipe de atendentes da Defensoria na data e no horário marcados, por meio do qual é possível também enviar e receber documentos[8].

A Defensoria Pública de Mato Grosso do Sul, por outro lado, buscou desenvolver uma plataforma para buscar desencorajar o uso do *WhatsApp*, mas enfrentou um grande problema de analfabetismo digital. O sistema funcionaria a partir do cadastro do assistido no site da defensoria, e, precisaria validar os dados por e-mail, o que é uma raridade entre os assistidos As pessoas até chegaram a criar e-mails, apesar da dificuldade mas, depois começaram a esquecer as senhas inseridas no cadastro no site da Defensoria para o envio dos documentos. Isso acabou por gerar um grande número de requerimentos de reformulação do acesso e isso ocupou o setor de tecnologia da informação dessa unidade da defensoria durante dias.

É importante destacar que a utilização do *WhatsApp* envolve uma discussão eminentemente estrutural e de monopólio de grandes empresas de tecnologia. Assim, uma regulamentação e diretiva de boas práticas precisam ser encaixadas numa discussão mais ampla do que significa utilizar *WhatsApp* para prestação de serviços públicos. No entanto, isso não significa abolir completamente a utilização da ferramenta uma vez que existem outros fatores em jogo quando se fala de acesso à justiça.

8 Disponível em: <https://www.defensoria.sp.def.br/dpesp/Conteudos/Noticias/NoticiaMostra.aspx?idItem=92057&idPagina=1&flaDestaque=V>. Acessado em 16 de setembro de 2021.

Bases legais para o atendimento ao usuário

Um dos maiores desafios em qualquer processo de adequação à LGPD é a atribuição das bases legais - e não seria diferente para as Defensorias Públicas.

As bases legais são *"pré-condições jurídicas que precisam ser cumpridas para que o controlador possa tratar os dados de forma lícita"*[9] e se encontram no rol específico dos arts. 7º e 11 da Lei. Portanto, a LGPD impôs um modelo de regulação *ex ante*, ou seja, o controlador precisa identificar e documentar a base legal para então realizar o tratamento de dados licitamente.

Nesse ponto, é importante destacar que não há hierarquização ou priorização entre as bases legais. Por exemplo, o consentimento é uma base legal bastante conhecida, mas, em muitos casos, não é a mais adequada.

No caso particular das Defensorias Públicas, no qual o usuário se encontra em uma situação de maior vulnerabilidade socioeconômica, dificilmente o consentimento será livre, informado e inequívoco, conforme exigido na LGPD. Portanto, no contexto das Defensorias Públicas, a base legal do consentimento apresenta três principais desafios que devem ser levados em conta[10]:

1. As desigualdades sociais existentes no Brasil implicam a ausência de letramento da população sobre o tratamento de dados pessoais. A complexidade das informações disponibilizadas, bem como a utilização de conceitos técnico-jurídicos muito específicos dificultam a plena compreensão dos usuários das Defensorias e, consequentemente, a obtenção do consentimento de acordo com os termos da Lei.;
2. A quantidade e a velocidade de informações trafegadas inviabilizam a tomada de decisão plenamente consciente;
3. A etapa de obtenção do consentimento inequívoco e informado para cada cidadão atendido implicaria uma demora sem sentido no fluxo de demandas urgentes.

Nessa linha, Rodrigo Pacheco, Defensor Público-Geral do Estado do Rio de Janeiro, sustenta que *"o consentimento do usuário é dispensável na atividade da Defensoria quando do atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público."*

9 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.

10 Ibid.

Tendo isso em vista, os participantes da Oficina elaboraram o seguinte enunciado:

ENUNCIADO

Arts. 7º e 11: *O consentimento é uma base legal mais arriscada para legitimar o tratamento de dados necessários ao início ou prosseguimento de atendimento. Em vista da condição de vulnerabilidade e assimetria do usuário frente às Defensorias, dificilmente seu consentimento seria livre e, por conseguinte, válido.*

3.3. CONVÊNIOS E CONTRATOS

Comumente as Defensorias firmam uma série de parcerias, contratos e convênios, com cartórios, órgãos do governo em diferentes níveis da federação, universidades e centros de pesquisa, empresas e entidades de terceiro setor. Naturalmente cada caso deve ser analisado cuidadosamente na medida em que o volume, a natureza dos dados envolvidos, bem como a finalidade de cada parceria varia e, com isso, as medidas a serem adotadas também irão variar.

No caso de algumas defensorias, foi mencionada a existência de comitês específicos de pesquisa e, quando isso ocorre, seria importante estabelecer padrões comuns de como esse grupo poderia lidar com os pedidos de compartilhamento de dados que são viabilizados pelo comitê.

Durante os encontros foi mencionada a inserção dos terceiros na posição de operador, e não de co-controlador ou controlador independente, para que esses terceiros fiquem inteiramente vinculados às diretrizes da defensoria pública. Além disso, foi mencionada a boa prática de enviar a s bases de dados já anonimizadas.

Ao longo da Oficina, foram identificadas duas principais questões que envolvem o tema de convênios e contratos:

- **Finalidade**: O compartilhamento de dados das Defensorias com terceiros envolve desafios técnicos e administrativos no tocante ao controle sobre a utilização dos dados e finalidade do tratamento. Em outras palavras, fiscalizar se o terceiro está cumprindo com os termos do contrato ou convênio não é uma tarefa simples.
- **Revisão de cláusulas contratuais**: É necessário rever todas as cláusulas dos contratos e convênios já firmados a fim de fazer os ajustes necessários à nova realidade de proteção de dados. Além disso, a revisão contratual é fundamental para determinação das finalidades de uso dos dados acessados, responsabilidades e deveres das partes envolvidas, bem como para a identificação dos agentes de tratamento como operador, controlador e co-controlador.

- **Responsabilidade**: para além da definição de controlador, operador e etc. Notou-se a importância de definir como fica a responsabilização no caso de um incidente de segurança ou outras situações de ilicitude ou desconformidade provocadas pelo uso dos dados por esses terceiros. Mais do que isso, estipular deveres de notificação, bem como planos de gestão de incidentes de segurança a cargo de cada um dos agentes que fazem parte da cadeia de tratamento de dados.

Assim, recomenda-se que no momento de elaborar as **políticas de convênios** deve-se levar em conta: (i) quais os dados são compartilhados, (ii) o fluxo de dados, (iii) quais as finalidades e (iv) quais as bases legais que sustentam esse compartilhamento.

Principais preocupações e riscos identificados

- Possibilidade de vazamento dos dados;
- Desvio de finalidade;
- Duplicação da base de dados para posterior utilização para outros propósitos;
- Dificuldade de exercer controle sobre o acesso e restrição ao banco de dados, diante do fornecimento de um único acesso compartilhado entre os terceiros;
- Ausência de transparência a respeito da transferência dos dados para outros atores;
- Ausência de consentimento dos assistidos para realização do compartilhamento. Ex. Quando o compartilhamento se dá entre entes que têm uma atribuição funcional oposta a da defensoria, como órgão de segurança pública.
- Ausência de regulação da transferência de dados pessoais públicos para entes privados;

Medidas de mitigação de risco sugeridas

- Incluir cláusula de delimitação de responsabilidades e indicação detalhada das finalidades do tratamento de dados;
- Prever cláusulas de responsabilidade exclusiva do agente caso ele descumpra com aquilo determinado contratualmente;

- Na revisão contratual, deve-se levar em conta, para fins de priorização, o volume e a sensibilidade dos dados objeto do compartilhamento (priorizar contratos nos quais há o compartilhamento de dados sensíveis);
- Na hipótese de compartilhamento com instituições de pesquisa é fundamental que se preste informações sobre a natureza da pesquisa, financiamento, metodologia e os objetivos pretendidos, principalmente no sentido de garantir a confiabilidade da pesquisa e dessa instituição/pesquisador para os quais os dados são transferidos;
- Sempre que possível deve-se proceder à anonimização de modo que somente dados como números e percentuais sejam repassados[10];
- Expor o tipo de tratamento de compartilhamento para pesquisa, por exemplo, nas Políticas de Privacidade das Defensorias ou no próprio termo de hipossuficiência como forma de dar transparência ao tratamento.

PARA REFLETIR...

- As Defensorias recebem e tratam muitos dados vindos de terceiros estranhos à organização. Por exemplo, a instituição tem acesso à base de dados do SUS e de concessionárias de água e energia. No entanto, ultimamente os defensores têm recebido notificações no sentido de que não terão mais acesso aos dados em razão da LGPD. Como isso afeta o trabalho das Defensorias em garantir assistência aos mais vulneráveis?
- Para realizar empréstimo consignado, a Defensoria compartilha dados dos defensores com ferramentas de consignação. A Defensoria faz um termo de consignação com uma instituição privada que operacionaliza o processo, fazendo a ponte entre o servidor e o órgão público. Isto é, existe um convênio feito entre a administração superior e a empresa que oferece o software, permitindo que os dados dos defensores sejam coletados e compartilhados com as instituições financeiras. Tendo em vista que essa prática ocorre sem o consentimento do servidor, haveria violação à LGPD?

Caracterização do controlador, operador e co-controlador

A identificação dos papéis de controlador e operador é uma etapa fundamental quando falamos de contratos e convênios. Determinar "quem é quem" na relação contratual é imprescindível para a atribuição dos deveres e responsabilidades dos agentes de tratamento.

11 Em razão da falta de recursos humano e financeiro, os participantes destacaram que ainda existem desafios técnicos e práticos para a implementação de medidas de anonimização de forma segura e eficiente. Contudo, recomenda-se prosseguir com a anonimização sempre que possível.

De acordo com a LGPD, o controlador, pessoa natural ou jurídica, é o sujeito a quem compete a tomada de decisões referentes ao tratamento: finalidades, condições e meios de processamento de dados pessoais[12].

Já o operador, pessoa natural ou jurídica, de direito público ou privado, é responsável por executar tarefas específicas com o objetivo de atingir metas previamente definidas pelo controlador[13]. Falta ao controlador autonomia para alterar os meios e finalidade do tratamento de modo que este se coloca em uma posição de subordinação[14]. Seria o caso, por exemplo, de um convênio por força do qual a defensoria pública utiliza dados pessoais para uma finalidade definida por um terceiro com quem tem convênio. Nesse caso, se houver uma finalidade própria da defensoria, que extrapola o convênio, ela se tornaria controladora dos dados pessoais.

Pensando nisso, os participantes fizeram os seguintes comentários:

> Na grande maioria dos convênios, a Defensoria seria a controladora. A única hipótese para co-controladoria seria a de convênios entre duas Defensorias dentro do escopo de um projeto conjunto;
>
> Em se tratando de compartilhamento de dados para fins de pesquisa, sugere-se a utilização de cláusulas "guarda-chuva" de maneira que nos contratos de convênio a Defensoria e o conveniado figurem como co-controladores;
>
> De toda forma, foi feita a ressalva de que se deve analisar caso a caso. A análise individualizada dos casos concretos permite identificar se as entidades públicas e privadas envolvidas no contrato também podem tomar decisões acerca do tratamento de dados, caso no qual devem ser consideradas co-controladoras.
>
> Esse arranjo beneficia as Defensorias Públicas e, em última análise, o próprio cidadão uma vez que divide e aloca a responsabilidade de acordo com o poder de cada agente envolvido na operação.

12 KREMER, Bianca. Os agentes de tratamento de dados pessoais. In: *A LGPD e o Novo Marco Normativo no Brasil*. Org. Caitlin Mulholland. Porto Alegre: Arquipélago, 2020. p. 290.

13 Ibid. p. 305.

14 Sobre os métodos para identificar o poder de influência nas atividades de tratamento de dados, consultar o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado" da Autoridade Nacional de Proteção de Dados Pessoais.

3.4. PROGRAMA DE ADEQUAÇÃO

A adequação à LGPD deve ser encarada não somente como uma obrigação legal, mas também como uma janela de oportunidade[15]. Assim, a conformidade à LGPD força as instituições a se organizarem, a reverem processos, a verificarem o fluxo de dados e as razões do tratamento. Essa visão ampla fornecida pelo processo de adequação pode influenciar diretamente na rapidez da resposta a situações de incidente de segurança, mau uso dos dados pessoais e/ou alocação de recursos de tecnologia da informação, ou seja, o programa de adequação tem muito a contribuir com o processo de gestão administrativa da organização.

A Defensoria Pública, como instituição permanente e essencial à função jurisdicional do Estado, apresenta suas particularidades e, portanto, seus programas de governança de dados não podem ser construídos a partir de modelos, templates, tabelas prontas e documentos ao estilo "copia e cola" produzidos pelo setor privado[16]. Em outras palavras, não se trata de simplesmente adaptar o método observado na iniciativa privada, mas sim de uma indispensável customização dos projetos de adequação à Lei Geral de Proteção de Dados Pessoais, levando em considerando as especificidades das Defensorias e a importância dos dados pessoais para atividades-meio e atividades-fim[17].

Considerando tais desafios, os participantes elencaram as duas principais prioridades do processo de adequação:

1. Criar um comitê ou indicar o encarregado para então...
2. Realizar o mapeamento mais aprofundado sobre os fluxo de dados da instituição

Criação de comitê de proteção de dados e indicação de encarregado

A complexidade institucional das Defensorias Públicas, bem como a quantidade massiva de dados tratados denuncia a necessidade da instituição indicar um Encarregado, aquele responsável pelo tratamento das informações do controlador. A complexidade das funções atribuídas ao encarregado de proteção de dados, face ao volume de atividades que os defensores públicos realizam no seu dia a dia,

15 BIONI, Bruno. *A Era dos Dados: Inovar pela Lei*. GV - Executivo. Vol. 18. nº 4. Julho/Agosto 2019 Disponível em: <https://brunobioni.com.br/home/wp-content/uploads/2019/08/gv_0184ce5.pdf>.

16 ZANATTA, Rafael; KITAYAMA, Marina. O desafio da LGPD para as Defensorias Públicas no Brasil. In. Lei Geral de Proteção de Dados e o Poder Público. Organizadores: Daniela Copetti Cravo, Daniela Zago Gonçalves da Cunda e Rafael Ramos. Tribunal de Contas do Estado do RS. Prefeitura de Porto Alegre Porto Alegre. Disponível em: <https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf>.

17 Ibid. p. 181.

destravou, em São Paulo, a criação de um órgão colegiado para endereçar a função. Nesse caso, é o próprio comitê, que de forma conjunta, endereça as atribuições de um encarregado de proteção de dados.

Entretanto, mesmo que o comitê não tenha sido criado, inicialmente, para endereçar essa função, a complexidade do projeto de adequação de uma defensoria sugere também a importância de instituição deste grupo de proteção de dados, o que permitiria uma atuação mais capilarizada do programa sobre as diferentes frentes de trabalho das Defensorias.

A LGPD traz a obrigatoriedade de indicação de um Encarregado, mas não de um comitê nos termos mencionados, mas, destacamos a relevância desse órgão interno[18], por ser esta uma boa solução para iniciar um projeto de governança e uma boa prática, nos termos do artigo 50 da LGPD.

A função do comitê é a de gerir o programa de adequação: o grupo será responsável pela verificação das obrigações legais e regulatórias do ente, por 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[19]. É importante mencionar, que durante os exercícios práticos identificou-se a necessidade de um comitê para o momento inicial da adequação e outro comitê para destravar o monitoramento contínuo e atualização da estrutura de governança de dados criada inicialmente (esse segundo comitê seria aquele que mais tem a ver com as funções de encarregado).

Eventualmente, esse comitê ou parte dele, pode endereçar conjuntamente as funções do encarregado de proteção de dados, conforme exposto anteriormente. Contudo, é importante destacar que

18 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.

19 BIONI, Bruno; ZANATTA, Rafael; KITAYAMA, Marina. *Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2021/06/guia_adequacao_defensorias_vf.pdf>.

algumas defensorias não enxergam essa possibilidade de colegiado diante da redação da lei, que lhes parece individualizar o cargo de encarregado de proteção de dados.

Ainda, foi mencionada a dificuldade de se criar um novo cargo ou órgão diante do estrangulamento orçamentário vivenciado por algumas unidades da defensoria pública no cenário atual, como foi o caso da Defensoria de Pernambuco. Além disso, menciona-se a falta de diretiva interna e normativas para orientar a criação do comitê, de utilizar aplicativos de comunicação ou de criação de um comitê para promover a adequação. No caso da nomeação do encarregado, durante a resolução dos exercícios práticos, no dia 07 de julho, foi mencionada a possibilidade de que o Defensor Público-Geral ou o Conselho Superior realizasse essa nomeação.

PARA REFLETIR...

- A criação de políticas não é responsabilidade exclusiva do Encarregado. Existe um processo de adequação propriamente dito e outro de manutenção e atualização das políticas de governança (este último caberia ao Encarregado).
- As Defensorias Públicas podem criar órgãos para serem encarregados, sendo fundamental que os comitês sejam diversificados.
- Deve haver uma relação de proximidade entre o Encarregado e a estrutura da Ouvidoria, tendo em vista que é o encarregado responsável por responder as requisições de direitos dos titulares.
- Quanto às atribuições do Comitê de Proteção de Dados, este deve atuar como protetor de dados da instituição, ouvindo e fiscalizando internamente a instituição.
- Comitê de implementação da LGPD x Comitê de monitoramento: Há uma distinção entre o comitê responsável pela adequação e o comitê que atua continuamente atualizando e supervisionando a aplicação das políticas de governança. O comitê de implementação da LGPD atua ao longo do processo de adequação, já o outro comitê realiza o monitoramento das atividades de tratamento de dados da instituição.

Criação de comitê de proteção de dados e indicação de encarregado

Quanto ao mapeamento, os participantes entenderam ser fundamental responder às seguintes perguntas de acordo com as etapas do mapeamento:

1. Quais canais serão utilizados para a coleta de dados?
2. Qual é o local de tratamento do dado para a partir disso pensar no fluxo?
3. Qual é o local de armazenamento?
4. Qual a finalidade de determinada operação de tratamento?

PARA REFLETIR...

- Destacou-se a existência de duas categorias de dados:
  1. Aqueles essenciais para o peticionamento;
  2. Aqueles utilizados para fins de políticas públicas.
- Os dados utilizados para fins de políticas públicas também podem ser utilizados posteriormente para defesa da tutela coletiva.
- A melhor forma de obter informações acerca dos processos de cada área é através de entrevistas com os respectivos responsáveis.

4. Considerações finais

A adequação à proteção de dados pessoais no sistema de justiça encontra especificidades que são próprias do poder público em uma dimensão republicana. Conforme nos ensina Miriam Wimmer, "*no setor público, o tratamento de dados pessoais não se inicia, em geral, a partir de uma decisão voluntária do titular, mas como decorrência das exigências do próprio pacto social*[20]". Não à toa, a Constituição Federal atribuiu às Defensorias Públicas o papel primordial de defesa de direitos e garantias fundamentais, o que naturalmente inclui aqueles relacionados à proteção de dados.

Com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais, algumas Defensorias Públicas iniciaram um pioneiro processo de internalização dos valores da proteção de dados pessoais em viés estratégico. Em 2021, diversos processos ocorreram paralelamente, como (i) criação de comitês de adequação dentro das Defensorias Públicas, (ii) publicação de Guias de Adequação para Defensorias Públicas, (iii) publicação de livros específicos sobre LGPD no Poder Público, (iv) realização de seminários de formação com Defensores Públicos e (v) intercâmbio e trocas de experiências entre Defensores sobre aspectos práticos da LGPD.

As Oficinas realizadas entre julho e agosto de 2021 revelaram a centralidade da proteção de dados pessoais como aspecto de justiça e efetivação de direitos na relação entre Defensorias e cidadãos. A instituição guarda uma quantidade expressiva de dados pessoais, muitos dos quais sensíveis. Considerando o perfil dos usuários das Defensorias, os dados tratados pela instituição merecem um cuidado especial dado seu potencial discriminatório. As pessoas atendidas pelo órgão são socioeconomicamente vulneráveis o que torna elas ainda mais suscetíveis de sofrer pelo uso abusivo de dados pessoais, seja em virtude de processos de tomada de decisões automatizadas discriminatórias, seja em virtude do assédio de empresas que colocam a privacidade de seus consumidores em detrimento do acesso "gratuito" de serviços.

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

Nesse sentido, a instituição possui duas missões no tocante à proteção de dados pessoais: a primeira, relaciona-se com a adequação do órgão às exigências legais; já a segunda, refere-se à proteção dos cidadãos por meio da tutela coletiva e da atuação direta em novos casos individuais que envolvam proteção de dados pessoais.

Este documento apresentou nossos esforços de sistematização das discussões travadas ao longo dos três encontros. A Oficina foi um espaço de aprendizagem horizontal que permitiu aos Defensores e servidores compartilharem suas experiências e percepções sobre os desafios impostos pela LGPD. Acreditamos que a construção conjunta é a chave para pavimentar o caminho rumo à disseminação da cultura de proteção de dados dentro e fora da instituição.

As Oficinas trouxeram à tona a necessidade de (i) construir mecanismos e ferramentas de trocas constantes de experiências práticas entre Defensores na adequação à LGPD, (ii) dar visibilidade a ideias inovadoras e experimentações conduzidas pelos Defensores Públicos no processo de adequação à LGPD e (iii) produzir documentações e estudos, em formato aberto e de forma transparente, sobre rotinas, processos e projetos formulados em contextos específicos e as dificuldades de adaptação de arranjos organizacionais em Defensorias que operam em territórios distintos e com condições institucionais e de recursos humanos variantes.

5. Bibliografia recomendada

BIONI, Bruno; JÚNIOR, Florisvaldo Fiorentino; KITAYAMA, Marina; PACHECO, Rodrigo Baptista; ZANATTA, Rafael. **LGPD e sistema de Justiça: a voz e a vez das Defensorias Públicas**. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-e-sistema-de-justica-a-voz-e-a-vez-das-defensorias-publicas-09062021>.

BIONI, Bruno; ZANATTA, Rafael; KITAYAMA, Marina. **Guia de Primeiros Passos para a Adequação das Defensorias Públicas à LGPD**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2021/06/guia_adequacao_defensorias_vf.pdf>.

BIONI, Bruno Ricardo. **Inovar pela lei**. GV EXECUTIVO, v. 18, n. 4, p. 30-33, 2019. Disponível em: <https://rae.fgv.br/sites/rae.fgv.br/files/gv_0184ce5.pdf>.

CERIONI, Clara. **Assistentes virtuais aceleram modernização tecnológica nas Defensorias Públicas**. Disponível em: <https://www.jota.info/coberturas-especiais/inova-e-acao/assistentes-virtuais-modernizacao-defensorias-publicas-05012021>.

GOMES, Rodrigo Dias de Pinho; ZANATTA, Rafael. **Carregando o piano? Notas sobre o encarregado de dados no setor público**. 22 de julho de 2021. Disponível em: <https://www.migalhas.com.br/depeso/348961/notas-sobre-o-encarregado-de-dados-no-setor-publico>.

PACHECO, Rodrigo Baptista. LGPD e **Defensoria Pública: uma análise da necessidade do consentimento**. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-defensoria-publica-uma-analise-da-necessidade-do-consentimento-14042021>.

WIMMER, Miriam. **Proteção de dados pessoais no poder público: incidência, bases legais e especificidades**. Revista dos Advogados da AASP, n. 144, nov., 2019, p. 127. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>.

ZANATTA, Rafael; KITAYAMA. **Os desafios da LGPD para as Defensorias Públicas no Brasil**, in: CRAVO, Daniela et al. A LGPD no setor público. Porto Alegre: Centro de Estudos Municipais, 2021, p. 172-185.Disponível em: <https://t.co/Oa0C5iwqRp?amp=1>.

ZANATTA, Rafael. **Tutela coletiva e coletivização da proteção de dados**, in: PALHARES, Felipe (org.). Temas Atuais de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2020, p. 345-374. Disponível em: <https://www.researchgate.net/profile/Rafael-Zanatta/publication/350852661_Tutela_coleti-va_e_coletivizacao_da_protecao_de_dados_pessoais/links/60764caf92851cb4a9dc18e6/Tutela-coletiva--e-coletivizacao-da-protecao-de-dados-pessoais.pdf>.

6. Anexos

- Dossiê Oficina Prática