RENOUV

Guia de Boas Práticas na Aplicação da Lei Geral de Proteção de Dados Pessoais nas Ouvidorias Públicas

SUMÁRIO

EXPEDIENTE

REDE NACIONAL DE OUVIDORIAS:

VALMIR DIAS
Coordenador-Geral

Ouvidoria-Geral do Distrito Federal

Ouvidoria-Geral do Estado de Minas Gerais

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

Tribunal Regional Eleitoral do Ceará

Empresa de Tecnologia e Informações da Previdência

Instituto Federal de Educação, Ciência e Tecnologia do Paraná
Membros do Conselho Diretivo

GRUPO DE TRABALHO LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NAS OUVIDORIAS:

MARCONI MUZZIO
Coordenador

ELABORAÇÃO:

ABELARDO LOPES
Controladoria-Geral da União

ALEXANDRE SANCHES VICENTE
Ouvidoria-Geral do Município de Londrina

BRUNEI DE OLIVEIRA MAIOCHI MALFATTI
Ouvidoria do Instituto Federal Catarinense

CECÍLIA SOUZA DA FONSECA
Ouvidoria-Geral do Distrito Federal

DIEGO MENEGAZZI
Setor de dados da Ouvidoria do Instituto Federal Catarinense

JANAÍNA ANCHIETA COSTA
Ouvidoria da Universidade Federal de São Paulo

MARIANA ACCIOLY
Controladoria-Geral da União

MARIA ELISA ANDRADE
Ouvidoria-Geral do Estado de Pernambuco

PAULO SÉRGIO ALMEIDA SANTOS
Ouvidoria-Geral da Universidade Federal de Mato Grosso

ROBERSON BRUNO LOBO OLIVIERI
Ouvidoria-Geral do Distrito Federal

REVISÃO:

Secretaria-Executiva da Rede Nacional de Ouvidorias

Coordenadoria de Proteção de Dados Pessoais da Secretaria da Controladoria-Geral do Estado de Pernambuco

Data Privacy Brasil

Open Knownledge Brasil

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
30/03/2022	1.0	Primeira versão do Guia de Boas Práticas na Aplicação da Lei Geral de Proteção de Dados Pessoais nas Ouvidorias Públicas	Membros do Grupo de Trabalho Lei Geral de Proteção de Dados Pessoais nas Ouvidorias

1. CONTEXTUALIZAÇÃO DAS OUVIDORIAS PÚBLICAS E A LGPD

A Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709, de 14 de agosto de 2018 -, atribuiu direitos aos titulares de dados pessoais, que lhes deverão ser garantidos pelos órgãos públicos, nos prazos e procedimentos dispostos em legislação específica, em especial nas disposições constantes da Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, também conhecida como Lei de Acesso à Informação ou LAI e, conforme entendimento, da Lei nº 13.460, de 26 de junho de 2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública, também conhecida como Código de Defesa dos Usuários de Serviços Públicos.

De outra forma, alguns destes direitos serão garantidos com a implementação das medidas de conformidade com a própria Lei, a exemplo das boas práticas que estão dispostas neste Guia.

Este documento tem o objetivo de fornecer conceitos, interpretações de normativos vigentes e orientações de boas práticas às Ouvidorias integrantes da Rede Nacional de Ouvidorias (Renouv) para adequação de suas ações, processos e documentos às diretrizes da LGPD, a partir de debates do grupo de trabalho “Lei Geral de Proteção de Dados Pessoais nas Ouvidorias”.

A Declaração Universal dos Direitos Humanos proclamada pela Assembleia Geral das Nações Unidas (Resolução 217 A III), em 10 de dezembro de 1948, representa marco fundamental para a disseminação da função de Ombudsman em diversos países, como um defensor dos direitos dos cidadãos.

No Brasil, a regulamentação das Ouvidorias começa a surgir com a emenda Constitucional n.º 19, de 1998, que incorporou ao artigo 37

o princípio da eficiência juntamente com os princípios da legalidade, impessoalidade, moralidade e publicidade e determinou, no §3º, que lei disciplinaria as formas de participação do usuário na administração pública, regulando as reclamações relativas à prestação dos serviços públicos em geral, do acesso a registros e informações sobre atos do governo, observado o disposto no art. 5º, X e XXXIII e da representação contra o exercício negligente ou abusivo de cargo, emprego ou função na administração pública.

O disciplinamento das *"reclamações relativas à prestação dos serviços públicos em geral"*, de que trata inciso I, §3º, art. 37 da Constituição Federal, deu-se com a edição da Lei nº 13.460, de 26 de junho de 2017 - Código de Defesa dos Usuários de Serviços Públicos -, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

O Código de Defesa dos Usuários de Serviços Públicos também especifica outros direitos previstos no §3º, art. 37 da Constituição Federal, regulamentando não apenas a apresentação de reclamações, mas também de manifestações na forma de *"... denúncias, sugestões, elogios e demais pronunciamentos de usuários que tenham como objeto a prestação de serviços públicos e a conduta de agentes públicos na prestação e fiscalização de tais serviços"* (art. 2º, inciso V, da Lei nº 13.460/2017). E dispõe ainda que a manifestação deverá ser dirigida para a Ouvidoria do órgão ou entidade responsável.

Com a previsão expressa da Ouvidoria como a unidade competente pelo recebimento das manifestações, a Lei atribui a ela a força normativa necessária para a sua instituição, onde ainda não implantada, e sua consolidação, onde já tiver havido a efetiva implantação.

Todavia, antes mesmo da edição do Código de Defesa dos Usuários de Serviços Públicos e a consolidação da Ouvidoria como instância de defesa dos direitos dos usuários dos serviços públicos, diversos entes da federação já haviam implementado e normatizado as Ouvidorias públicas em suas respectivas esferas de poder. Ademais, com o advento da Lei de Acesso à Informação (LAI) e a criação do Serviço de Informação ao Cidadão (SIC), Ouvidorias de vários poderes e esferas da federação agregaram esse serviço, aproveitando recursos físicos e humanos já estruturados para sua

oferta.

Mais recentemente, em 16 de dezembro de 2020, a Organização das Nações Unidas (ONU) aprovou a Resolução 75/186, que reforça o papel da Ouvidoria no contexto da governança da pasta em que atua, operando como instituto de promoção e proteção dos direitos humanos, bem como das liberdades fundamentais e respeito pelo Estado de Direito. Essa Resolução ressalta também, a necessidade de compartilhamento de informações relacionadas às melhores práticas em relação ao trabalho e funcionamento das instituições de Ouvidoria.

Na atuação da Ouvidoria Pública, a proteção de dados pessoais sempre foi uma preocupação latente. Além do disposto nos artigos 6º e 31 da LAI, que trata do tema, diversos entes da federação, inclusive a União, já buscavam oferecer salvaguardas para proteger os dados pessoais do cidadão, em especial do denunciante, por meio de normativos específicos como, em âmbito federal, os Decretos nº 9.492, de 5 de setembro de 2018, e nº 10.153, de 3 de dezembro de 2019, alterados pelo Nº 10.890, de 9 de dezembro de 2021, que dispõem sobre a proteção ao denunciante de ilícitos e de irregularidades praticadas contra a administração pública federal direta e indireta.

Por outro lado, as normas de proteção de dados pessoais da União Europeia há muito são consideradas um padrão-ouro em todo o mundo. Nos últimos 25 anos, a tecnologia transformou as vidas dos cidadãos de maneira inimaginável, de forma que foi necessária uma revisão das regras. Assim, em maio de 2018, entrou em vigor na União Europeia (EU) o regulamento denominado *General Data Protection Regulation* (GDPR), uma versão atualizada de outra norma de privacidade de dados chamada *Data Protection Directive* (95/46/EC), com a finalidade de proteger a privacidade dos dados pessoais dos cidadãos europeus e evitar o vazamento de informações.

Ao contrário da Diretiva de Proteção de Dados Pessoais de 1995 (95/46/CE), revogada pelo GDPR, que permitia que cada um dos vinte e oito membros da UE a adotasse e personalizasse as regras, de acordo com as necessidades dos seus cidadãos, o GDPR, enquanto regulamento, exige a sua plena adoção pelos vinte e oito países que compõem a UE.

No contexto brasileiro, em agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados (LGPD), tendo a maior parcela de seus dispositivos entrado em vigor em setembro de 2020, que tem como principal referência o GDPR. O objetivo da LGPD é regulamentar a utilização de dados pessoais, trazendo maior segurança e privacidade para as pessoas, prevendo que esses dados possam ser tratados com autorização do seu titular ou no caso de existir uma base legal que autorize.

E para além da Lei, em 10 de fevereiro de 2022, a proteção de dados pessoais foi expressamente incorporada à Constituição Federal como um direito e garantia fundamental, na forma do inciso LXXIX do Art. 5º. Fato esse que fortaleceu, sobremaneira, a aplicação desse direito para o cidadão brasileiro, que agora se vê resguardado de forma permanente, tendo em vista que tal alteração configurou uma cláusula pétrea, ou seja, não pode ser alterada.

2. OUVIDORIAS PÚBLICAS NO CONTEXTO DIGITAL

Em um mundo cada vez mais guiado por dados, identifica-se, a todo tempo, o uso abusivo de dados pessoais, a exemplo da sua comercialização ilegal. E, para coibir tais situações, ações voltadas à proteção do titular do dado são realizadas, como a promulgação de legislações garantidoras dos direitos do indivíduo relacionados à privacidade e a criação de autoridades independentes fiscalizadoras.

A regulamentação da proteção de dados pessoais impõe restrições ao uso indiscriminado dos dados de pessoas naturais não apenas pela iniciativa privada, como também, às instituições públicas, instituindo direitos aos titulares de dados pessoais, ao mesmo tempo em que alinha as necessidades econômicas do país à modernidade virtual, já experimentada em diversos países do mundo.

As Ouvidorias, enquanto instância de defesa dos direitos dos usuários de serviços públicos e integrada à governança de serviços,

possuem importante papel na implementação da LGPD e na adequação dos serviços públicos à evolução digital vivenciada na sociedade atual.

Ademais, reflexo desta constante evolução, o canal de atendimento eletrônico da Ouvidoria, por meio da *internet*, vem crescendo ao longo dos anos. Isso demonstra que o próprio cidadão tem feito a escolha de se relacionar com o Governo pelo mundo digital.

E nesse sentido, o Estado vem se organizando para oferecer um ambiente mais seguro, simplificado e sistematizado à população, inclusive com a publicação de decretos federais, como o de nº 9.094, de 17 de julho de 2017, alterado pelo de nº 9.723, de 11 de março de 2019, que dispõe sobre a simplificação do atendimento prestado aos usuários dos serviços públicos e institui o Cadastro de Pessoas Físicas (CPF) como instrumento suficiente e substitutivo da apresentação de outros documentos, bem como a Lei nº 14.129, de 29 de março de 2021, que trata sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, especialmente por meio da simplificação, da inovação, da transformação digital e da participação do cidadão.

A referida Lei determina em seu art. 18, como componentes essenciais para a prestação digital dos serviços públicos a Base Nacional de Serviços Públicos, as Cartas de Serviços ao Usuário, de que trata a Lei nº 13.460/2017 e as Plataformas de Governo Digital.

Em seguida, no art. 21, inciso XI, dispõe que a ferramenta digital de atendimento e de acompanhamento da entrega dos serviços públicos das Plataformas de Governo Digital deve apresentar, entre suas características e funcionalidades mínimas, a implementação de sistema de ouvidoria, nos termos da 13.460/2017. E estabelece, no art. 23, I, que Poder Executivo federal poderá estabelecer padrões nacionais para os componentes essenciais do Governo Digital, de que trata o art. 18.

Nesse contexto de digitalização de serviços, as Ouvidorias necessitam buscar a consolidação e a organização dos seus fluxos nos ambientes digitais e, ao mesmo tempo, garantir a proteção dos dados pessoais ao cidadão.

Assim, neste Guia buscou-se trazer boas práticas de aplicação da

LGPD nas Ouvidorias também no ambiente físico, tendo em vista que esse processo de digitalização do serviço de Ouvidoria se encontra, ainda, em desenvolvimento.

E, por fim, é importante esclarecer, também, que mesmo quando houver maior avanço no processo de digitalização, ela não será completa, ou seja, sempre haverá pastas físicas e papéis e o tratamento de dados pessoais continuará ocorrendo nesse ambiente físico, devendo ser observada a LGPD.

3. CONCEITOS

Nesta seção, apresentam-se conceitos importantes para as Ouvidorias na compreensão da Lei e dos seus desdobramentos a partir da própria LGPD e de referências a publicações e a outros documentos técnicos já existentes, em especial, o Guia de Boas Práticas da Lei Geral de Proteção de Dados, publicado pelo Comitê Central de Governança de Dados do Poder Executivo Federal.

- **Agentes de Tratamento:** são os responsáveis pelo tratamento dos dados pessoais, sujeitos às regras da LGPD e à fiscalização da ANPD. O controlador é a instituição que toma as decisões referentes ao tratamento de dados pessoais e o operador, a instituição que realiza o tratamento de dados pessoais em nome do controlador. Vale mencionar que a depender da atividade/tratamento exercido, uma instituição pode figurar simultaneamente como controladora e operadora. Isso é especialmente relevante no caso de compartilhamento de dados entre ouvidorias ou diferentes órgãos públicos. Não obstante, essa distinção não ser abordada detalhadamente neste Guia, essa situação demonstra que a classificação dos agentes de tratamento precisa ser analisada com cautela, uma vez que irá refletir diretamente nas responsabilidades de cada agente. Ainda, cabe conhecer a existência de configurações possíveis de agentes de tratamentos, além do controlador e do operador, que são a controladoria conjunta e o suboperador, cujas diferenças são dispostas em detalhes no Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público da ANPD.

• **Autoridade Nacional de Proteção de Dados Pessoais (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. De maneira objetiva, o Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, publicado pela Autoridade em janeiro de 2022, dispõe que a ANPD é o *"...órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua implementação, no que se inclui a deliberação administrativa, em caráter terminativo, sobre a interpretação da lei e sobre as suas próprias competências e casos omissos (art. 55-K, parágrafo único; art. 55-J, XX). Além disso, a autoridade nacional detém competência exclusiva para aplicar as sanções administrativas previstas na LGPD, com prevalência de suas competências sobre outras correlatas de entidades e órgãos da administração pública no que se refere à proteção de dados pessoais (art. 55-K)."*

• **Bases de dados ou banco de dados:** A LGPD conceitua banco de dados como "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico" (art. 5º, IV). Em outras palavras, são coleções organizadas de dados que se relacionam de forma a criar algum sentido e dar mais eficiência durante uma pesquisa ou estudo científico, independente do formato em que estejam armazenadas (por exemplo, pode ser uma simples planilha no computador de um agente público, ou um grande volume de dados em nuvem ou servidor remoto). Como exemplo de banco de dados físicos, existem os assentamentos funcionais dos servidores públicos, onde constam, além ocorrências da vida funcional do servidor público, seus dados pessoais, como CPF e endereço residencial, que podem vir a ser armazenamos em armários ou prateleiras. E, um exemplo de banco de dados eletrônico, é o da Plataforma Fala.BR que reúne os dados das manifestações de ouvidoria registradas.

• **Base legal ou Hipóteses de Tratamento de Dados Pessoais:** A LGPD previu expressamente, em seus artigos 7º e 11, as hipóteses que autorizam o tratamento de dados pessoais, que podem ser, também, chamadas de bases legais de tratamento de dados pessoais. A Tabela 3 do Guia de Boas Práticas da Lei Geral de Proteção de Dados, publicado pelo Comitê Central de Governança de Dados do

Poder Executivo Federal, elenca resumidamente as hipóteses de tratamento autorizadas pela LGPD, com respectivas bases legais referentes ao tratamento de dados pessoais em geral (Art. 7º) e de dados pessoais sensíveis (Art. 11).

• **Controlador:** A definição legal de controlador se encontra no art. 5º, VI, da LGPD, qual seja, *"pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"*. O Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado, publicado pela ANPD, dispõe que no contexto de pessoas jurídicas, o controlador é a organização e não as pessoas naturais que atuam como profissionais subordinados ou como membros dos órgãos. Trata, ainda, especificamente das pessoas jurídicas de direito público, cujas competências decisórias são distribuídas internamente entre diferentes órgãos públicos. Nesses casos, utilizando-se do exemplo da União, a ANPD orienta observar os seguintes aspectos: (a) o controlador é pessoa jurídica de direito público, que no caso é a União e, portanto, responde pelas obrigações previstas na Lei, pelos instrumentos contratuais e atos ilícitos praticados pelos seus órgãos e servidores e (b) por outro lado, pelo princípio da desconcentração administrativa, a LGPD atribuiu aos órgãos públicos obrigações típicas de controlador, o que não obstante a União seja a controladora, as atribuições de controlador, são exercidas pelos órgãos públicos que desempenham essas funções em nome da pessoa jurídica da qual fazem parte. Contudo, a ANPD faz a ressalva de que esta análise refere-se apenas à Administração Pública direta, uma vez que a indireta segue o regramento de pessoa jurídica estabelecido pela LGPD. Exemplos das obrigações atribuídas ao controlador pela LGPD são elaborar relatório de impacto à proteção de dados pessoais (art. 38), comprovar que o consentimento obtido do titular atende às exigências legais (art. 8º, § 2º) e comunicar à ANPD a ocorrência de incidentes de segurança (art. 48).

• **Dados pessoais:** De acordo com o inciso IV do artigo 4° da LAI, informação pessoal é aquela relacionada à pessoa natural identificada ou identificável entendendo-se por pessoa natural a pessoa física, ou seja, o indivíduo. E a LGPD adotou a mesma referência, em relação ao dado pessoal, o que demonstra que a proteção de dados pessoais

não surgiu com a LGPD, mas já era regulamentada no Brasil por outras normas.

• **Dados pessoais sensíveis:** A LGPD manteve o conceito de dado pessoal trazido pela LAI e evoluiu sobre o conceito de informação sensível para *"dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"* (Art. 5º, II).

• **Direitos do Titular de Dados Pessoais:** A LGPD estabeleceu direitos aos titulares de dados pessoais a serem assegurados pelos controladores de dados, que devem ser garantidos durante toda a existência do tratamento dos dados pessoais do titular realizado pelo órgão ou entidade. Para o exercício desses direitos, no âmbito público, a Lei provoca um aprofundamento de obrigações de transparência ativa e passiva e de defesa dos usuários de serviços. Essas obrigações são apresentadas no Guia de Boas Práticas da Lei Geral de Proteção de Dados, publicado pelo Comitê Central de Governança de Dados do Poder Executivo Federal documento: (a) obrigações de transparência ativa; (b) meios de acesso à informação em transparência passiva; e (c) meios de petição e manifestação à administração pública. Estes direitos serão abordados mais detalhadamente em capítulo específico deste Guia.

• **Encarregado:** O controlador de dados deverá indicar um encarregado pelo tratamento de dados pessoais, que será o indivíduo responsável por garantir a conformidade da instituição à LGPD. Considerando as boas práticas internacionais, conforme orienta a ANPD, (a) o encarregado poderá ser um funcionário da instituição ou um agente externo, de natureza física ou jurídica; (b) indicado por um ato formal ou administrativo; (c) com liberdade na realização de suas atribuições; (d) com conhecimentos de proteção de dados e segurança da informação em nível que atenda às necessidades da instituição; e (e) que tenha recursos adequados para realizar suas atividades (prazos apropriados, finanças e infraestrutura) e apoio de uma equipe de proteção de dados. Importante, também, o reforço da ANPD em relação ao papel do encarregado no fomento e disseminação da cultura de proteção de dados pessoais na organização. A LGPD

define como atribuições do encarregado, no § 2º do art. 41, (I) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; (II) receber comunicações da autoridade nacional e adotar providências; (III) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e (VI) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. E, por fim, no §1º desse mesmo dispositivo, determina, como requisito de transparência, que *"a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador"*.

• **Gestão de Riscos:** Conforme a ABNT, a gestão de riscos, consiste em *"atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos"* (ABNT NBR ISO/IEC 31000:2018).

• **Operador:** A definição legal desse agente de tratamento se encontra no art. 5º, inciso X da LGPD, que corresponde à *"pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"*. A Lei reforça esse conceito no artigo 39, a seguir: *"o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria"*. Em breve síntese, nas palavras do Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado, publicado pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD), o *"operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada"*. No mesmo material, a ANPD destaca as seguintes obrigações do operador: *"(i) seguir as instruções do controlador; (ii) firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador; (iii) dar ciência ao controlador em caso de contrato com suboperador"*. Por fim, esse Guia da ANPD discorre, ainda, sobre o conceito de suboperador. Para conhecimento mais aprofundado sobre o tema, recomenda-se a leitura do documento.

• **Ouvidor:** titular da Ouvidoria, que corresponde à instância competente para recepcionar as manifestações dos usuários dos

serviços públicos, conforme estabelecido no art. 10 do Código de Defesa dos Usuários de Serviços Públicos. E, em alguns casos, é também o responsável pela gestão do Serviço de Informação ao Cidadão (SIC), de que trata o art. 9º, I, da LAI, quando o referido serviço é incorporado à Ouvidoria.

• **Pseudonimização de dados ou dados pseudonimizados:** Pseudonimização é a técnica de tratar dados pessoais de forma em que os dados somente possam ser atribuídos a um titular de dados mediante a utilização de informações adicionais, não disponíveis a todos e mantidas em ambiente separado, controlado e seguro. Para distingui-lo do processo de anonimização, deve-se compreender que se observada a possibilidade de reversão do processo que obteve a anonimização, permitindo a reidentificação do titular de dados, não se está diante de um dado verdadeiramente anonimizado, mas de um dado potencialmente pseudonimizado. A título ilustrativo, criptografia é um método de pseudonimização, quando os dados somente podem ser atribuídos a um titular mediante o conhecimento da chave criptográfica. Sem conhecer a chave, os dados são ininteligíveis. De acordo com a LGPD, o processo pseudonimização, bem como de anonimização, devem ser utilizados, sempre que possível, por meio da aplicação de meios técnicos razoáveis e disponíveis, na ocasião do tratamento dos dados (Guia de Boas Práticas da Lei Geral de Proteção de Dados, Comitê Central de Governança de Dados do Poder Executivo Federal, Agosto 2020).

• **Relatório de Impacto à Proteção de Dados:** conforme a LGPD, o Relatório de Impacto à Proteção de Dados (RIPD) é uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais e dados pessoais sensíveis que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

• **Titular de Dados Pessoais:** art. 5º, V da LGPD conceitua titular de dados pessoais como a *"pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"*. Em outras palavras, os dados, quando atrelados a um indivíduo são uma projeção, extensão ou dimensão de seus titular que, pelo princípio da autodeterminação, tem o direito de decidir sobre o uso dos seus dados. Em decisão

liminar que suspendeu a eficácia da Medida Provisória (MP) 954/2020, que previa o compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE), o Supremo Tribunal Federal fundamenta que a proteção de dados pessoais advém dos direitos da personalidade, que pelo Código Civil, não são recursos alienáveis.

- **Tratamento de Dados Pessoais:** toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, nos termos do inciso X do art. 5º da LGPD. A Figura 1 extraída do Guia de Boas Práticas da Lei Geral de Proteção de Dados do Comitê Central de Governança de Dados do Poder Executivo Federal, apresenta a conceituação de cada operação de tratamento de que trata a LGPD:

Figura 1: Conceitos das operações de tratamento de dados pessoais (LGPD, art. 5º, X).

As operações de tratamento são destacadas a seguir:

ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

ARMAZENAMENTO - ação ou resultado de manter ou conservar em repositório um dado;

ARQUIVAMENTO - ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;

AVALIAÇÃO - analisar o dado com o objetivo de produzir informação;

CLASSIFICAÇÃO - maneira de ordenar os dados conforme algum critério estabelecido;

COLETA - recolhimento de dados com finalidade específica;

COMUNICAÇÃO - transmitir informações pertinentes a políticas de ação sobre os dados;

CONTROLE - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;

DIFUSÃO - ato ou efeito de divulgação, propagação, multiplicação dos dados;

DISTRIBUIÇÃO - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;

ELIMINAÇÃO - ato ou efeito de excluir ou destruir dado do repositório;

EXTRAÇÃO - ato de copiar ou retirar dados do repositório em que se encontrava;

MODIFICAÇÃO - ato ou efeito de alteração do dado;

PROCESSAMENTO - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;

PRODUÇÃO - criação de bens e de serviços a partir do tratamento de dados;

RECEPÇÃO - ato de receber os dados ao final da transmissão;

REPRODUÇÃO - cópia de dado preexistente obtido por meio de qualquer processo;

TRANSFERÊNCIA - mudança de dados de uma área de armazenamento para outra, ou para terceiro;

TRANSMISSÃO - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;

UTILIZAÇÃO - ato ou efeito do aproveitamento dos dados.

Fonte: Guia de Boas Práticas da Lei Geral de Proteção de Dados do Comitê Central de Governança de Dados do Poder Executivo Federal , Brasil.

4. IMPLICAÇÕES DA LGPD SOBRE AS OUVIDORIAS PÚBLICAS

Com o advento da LGPD, recai sob as instituições públicas de todos os poderes e esferas da federação o dever de adequar suas ações, processos, documentos físicos e eletrônicos e sistemas informatizados de forma a atender as diretrizes da Lei e, assim, garantir que o tratamento de dados pessoais seja realizado apenas nas hipóteses legais previstas e com a transparência necessária perante os titulares de dados pessoais e, ainda, garantindo a eles um canal oficial, por meio do qual poderão pleitear o exercício dos direitos instituídos.

Sob a ótica da Ouvidoria, identificam-se 03 (três) implicações distintas da LGPD nas suas atribuições:

a) Intensificar as ações adotadas para a proteção de dados pessoais e adequação das suas ações, processos, documentos e sistemas informatizados para atendimento à LGPD: A primeira implicação identificada recai, obrigatoriamente, sob todas as Ouvidorias, independente do poder e esfera de atuação, e corresponde à intensificação das ações realizadas para garantir a proteção dos dados pessoais. Uma vez que a LAI, em seu art. 31 já estabelece diretrizes de proteção de dados pessoais, já cabia à Ouvidoria essa obrigação. Todavia, com a implantação da LGPD, houve a regulamentação específica de como deve se dar a referida proteção e, por isso, a necessidade da intensificação das ações. Assim, compete à Ouvidoria a realização das adaptações que se farão necessárias nas suas ações, processos, documentos físicos e eletrônicos e sistemas informatizados para garantir essa proteção. Nesse contexto, é importante que se faça um mapeamento dos dados pessoais tratados em cada ação, processo, base de dados e sistemas informatizados utilizados pela Ouvidoria e que seja identificada a finalidade do uso de cada um desses dados, a partir de uma priorização com base em análise de riscos. Caso o uso identificado não obedeça ao princípio da finalidade de que trata a LGPD e que será abordado mais detalhadamente neste Guia, o uso deve ser descontinuado. E, quando o uso do dado obedece a esse princípio, deverão ser implantadas salvaguardas, de forma a proteger os dados do uso em finalidade incompatível.

Deverão, ainda, as Ouvidorias, evoluir os sistemas informatizados utilizados para garantir a observância dos princípios de proteção de dados pessoais. Sob esse ponto é importante atentar que os bancos de dados dos sistemas informatizados de Ouvidoria, pela própria característica do negócio, possuem uma quantidade significativa de dados pessoais e, até mesmo, dados pessoais sensíveis. Então, assim como deverá ocorrer em toda a Administração Pública, as Ouvidorias precisarão adequar seus sistemas a requisitos de segurança da informação e de proteção de dados pessoais definidos no âmbito da esfera e do órgão a que estejam vinculadas. Da mesma forma, precisarão observar os requisitos de segurança aplicados ao manuseio de documentos em papel onde constem dados pessoais, uma vez que arquivos físicos também são regidos pela LGPD;

b) Canal de comunicação com o titular do dado pessoal: Uma segunda implicação à Ouvidoria que se apresenta como possível, a critério de cada instituição pública, é a atribuição de atuar como canal de comunicação entre o titular do dado pessoal e a Administração Pública, no exercício dos seus direitos previstos na LGPD. Essa implicação decorre da compreensão de que os direitos dos titulares perante a Administração Pública serão, geralmente, exercidos nos prazos e procedimentos da Lei de Acesso à Informação, por meio do Serviço de Informação ao Cidadão (SIC) que, em muitos casos, já funcionam vinculados às estruturas de Ouvidoria ou do Código de Defesa dos Usuários de Serviços Públicos, que expressamente atribui à Ouvidoria o papel de recepcionar o usuário dos serviços públicos para registro de suas manifestações e

c) Ouvidor como encarregado de proteção de dados: Por fim, a terceira implicação à Ouvidoria, sendo esta também possível, mas não obrigatória, é a de exercer as competências do encarregado, quando o titular da Ouvidoria, ou seja, o ouvidor, é indicado pelo controlador como encarregado da instituição pública à qual aquela Ouvidoria está vinculada. Como a Lei conceitua encarregado como *"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 (ANPD)"* (art. 5º, VII, da LGPD) e, comumente, na Administração Pública, a Ouvidoria já atua como canal de comunicação com os usuários dos serviços públicos, por força Código de Defesa dos Usuários de Serviços Públicos

(Lei n° 13.460/2017), em algumas instituições públicas, inclusive, na Controladoria-Geral da União (CGU), a função de encarregado recaiu na pessoa do ouvidor. Ainda que o ouvidor não atue como Encarregado, a sua participação na Unidade de Governança para Proteção de Dados Pessoais, se houver, no contexto da Governança de Serviços, faz-se importante e necessária. E, mesmo não havendo a instituição de órgão colegiado para coordenação das ações de proteção de dados no âmbito da esfera a que a Ouvidoria está vinculada, ressalta-se a importância de que a Ouvidoria mantenha relacionamento com o setor responsável, uma vez que recepcionará as demandas dos titulares de dados pessoais.

O presente documento discorre sobre os riscos e as correspondentes boas práticas referentes às implicações "a" e "b", com intuito de subsidiar as Ouvidorias com orientações para adequar suas ações, processos, documentos físicos e eletrônicos e sistemas informatizados às diretrizes da LGPD, protegendo os dados pessoais que são tratados na realização das suas atividades, bem como para o atendimento ao titular dos dados que busca a instituição pública, por meio da Ouvidoria, para pleitear o exercício de seus direitos regulamentados.

5. BASE LEGAL PARA TRATAMENTO DE DADOS PESSOAIS PELAS OUVIDORIAS PÚBLICAS

Base legal ou Hipóteses de Tratamento de Dados Pessoais são as circunstâncias expressamente previstas pela LGPD, no artigo 7°, que autorizam o tratamento de dados pessoais.

A Figura 2, extraída do Guia de Boas Práticas da Lei Geral de Proteção de Dados do Comitê Central de Governança de Dados do Poder Executivo Federal, elenca resumidamente as hipóteses de tratamento autorizadas pela LGPD, com respectivas bases legais referentes ao tratamento de dados pessoais em geral (Art. 7°) e de dados pessoais sensíveis (Art. 11).

Figura 2. Hipóteses de tratamento de dados pessoais previstas no art. 7º, da LGPD.

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art. 11, I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, "a"
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, inciso III	LGPD, art. 11, II, "b"
Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, inciso IV	LGPD, art. 11, II, "c"
Hipótese 5: Para a execução ou preparação de contrato	LGPD, art. 7º, inciso V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, inciso VI	LGPD, art. 11, II, "d"
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, art. 7º, inciso VII	LGPD, art. 11, II, "e"
Hipótese 8: Para a tutela da saúde do titular	LGPD, art. 7º, inciso VIII	LGPD, art. 11, II, "f"
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, inciso IX	Não se aplica
Hipótese 10: Para proteção do crédito	LGPD, art. 7º, inciso X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, art. 11, II, "g"

Fonte: Guia de Boas Práticas da Lei Geral de Proteção de Dados do Comitê Central de Governança de Dados do Poder Executivo Federal , Brasil.

No contexto da Ouvidoria Pública, importante esclarecer que as hipóteses que autorizam o tratamento de dados pessoais e dados pessoais sensíveis são o cumprimento de obrigação legal regulatória, prevista nos artigos 7º, II e 11, II, "a" e a execução de políticas públicas, de que trata artigos 7º, III e 11, II, "b". Desta forma, o consentimento, de que tratam artigos 7º, I e 11, I não deve ser a base legal utilizada para o tratamento dos dados pessoais nos processos típicos de Ouvidoria.

Isso ocorre porque, conforme o Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, o consentimento é a *"manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"*. Ou seja, o consentimento pressupõe uma escolha do titular em autorizar ou não o tratamento de seus dados, que pode, inclusive, solicitar sua revogação a qualquer momento.

Todavia, o Poder Público realiza suas ações em cumprimento a obrigações e atribuições legais, podendo ser necessário, para tanto, o tratamento de dados pessoais. O mencionado Guia da ANPD complementa que, nesse contexto, *"...o órgão ou a entidade exerce prerrogativas estatais típicas, que se impõem sobre os titulares em uma relação de desbalanceamento de forças, na qual o cidadão não possui condições efetivas de se manifestar livremente sobre o uso de seus dados pessoais"*.

Desta forma, as informações pessoais coletadas por meio do registro de manifestações e no ato de cadastro em sistemas informatizados de Ouvidoria são necessárias para as providências dos órgãos em relação ao que fora apresentado pelo usuário na forma de denúncia, reclamação, solicitação, entre outros, em atendimento à obrigação legal regulatória prevista no artigo 12, parágrafo único, da Lei nº 13.460, de 26 de junho de 2017, que impõe à administração pública a efetiva resolução das manifestações apresentadas pelos usuários.

Em adição, uma vez que a resolução das manifestações acerca da prestação de serviços públicos provoca atos e decisões administrativas, podendo, inclusive, motivar melhorias nos processos e serviços, a depender da situação fática, poderá ser enquadrada na hipótese legal de execução de políticas públicas, de que tratam artigos 7º, inciso III e 11, inciso II, "b".

Contudo, é importante destacar que cada tratamento de dados

necessita de uma base legal específica. Além disso, um mesmo tratamento de dados não pode ter duas bases legais.

Ainda acerca da hipótese de execução de políticas públicas, a título exemplificativo, poderá ocorrer a utilização dos dados pessoais coletados pela Ouvidoria, para identificação do perfil socioeconômico dos seus usuários e, a partir disso, definição da sua estratégia de atuação, dando maior efetividade à política pública de Ouvidoria.

E, para afastar definitivamente a hipótese de consentimento no registro de manifestações de Ouvidoria, importante destacar que a Lei nº 13.460, de 26 de junho de 2017, determina que a manifestação perante a administração pública acerca da prestação de serviços públicos deverá ser, obrigatoriamente, identificada. E, ainda, § 1º do art. 10-A, incluído pela Lei nº 14.129/2021, determina que *"os cadastros, os formulários, os sistemas e outros instrumentos exigidos dos usuários para a prestação de serviço público deverão disponibilizar campo para registro do número de inscrição no CPF, de preenchimento obrigatório para cidadãos brasileiros e estrangeiros".*

Por outro lado, vale destacar que essa prerrogativa de não precisar de consentimento do titular para o tratamento de dados só poderá ser aplicada se cumprido o princípio da finalidade, explícito no inciso I do art. 6º da LGPD. Isso porque, conforme Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, elaborado pela ANPD, o tratamento dos dados pessoais deve ser realizado com *"...propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades." Adicionalmente, no âmbito do setor público, o tratamento de dados pessoais deve atender a uma 'finalidade pública', conforme previsto no art. 23 da LGPD".*

Não obstante o consentimento não ser a base legal mais apropriada para o tratamento de dados pessoais pelo Poder Público, conforme orientações do Guia Orientativo da ANPD, e, especificamente, em Ouvidoria, pelos argumentos ora expostos, ele poderá eventualmente ser admitido como base legal para o tratamento de dados pessoais, quando a utilização dos dados não for compulsória e a atuação da Ouvidoria tiver finalidade distinta de sua função típica. Como exemplo, considera-se que uma organização sem fins lucrativos esteja promovendo capacitação

gratuita a cidadãos com intuito de capacitá-los para o exercício do controle social e solicita à Ouvidoria os e-mails dos usuários, entendendo serem eles potenciais interessados na participação no evento. Considerando que, nesse exemplo, a Ouvidoria não está no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais, o compartilhamento do dado solicitado só poderá ocorrer mediante consentimento do titular.

Diante do exposto, é de suma importância que as Ouvidorias apresentem o Termo de Uso de sistema e a respectiva Política de Privacidade ao cidadão na etapa de registro da manifestação e na realização do cadastro no sistema informatizado, se houver, e, ainda, em resposta a e-mails de usuários, quando este for um dos canais de ouvidoria disponibilizados. Para tanto, recomenda-se utilizar como referência o Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos, elaborado pelo Comitê Central de Governança de Dados do Poder Executivo Federal.

6. DIREITOS DOS TITULARES DE DADOS PESSOAIS E SEU EXERCÍCIO

A LAI já havia estabelecido, em seu art. 31, procedimentos e diretrizes básicas para o tratamento de dados pessoais no âmbito público.

Reconhecendo esse legado, a Lei Geral de Proteção de Dados, no art. 23, §3º, determina que os prazos e procedimentos para o exercício dos direitos do titular perante o Poder Público observarão a legislação específica, entre elas, a Lei de Acesso à Informação.

Diante disso, o entendimento é que o exercício dos direitos de titulares de dados pessoais previstos no art. 18, incisos I, II, VII e VIII ou art. 20, § 1º, da LGPD, equivale ao direito fundamental de acesso à informação perante o Estado já previsto na LAI e, por isso, estarão submetidos aos prazos e procedimentos já estabelecidos pela Lei de Acesso à Informação.

Isso significa que, para o exercício desses direitos, o titular de dados

pessoais deverá utilizar o Serviço de Informação ao Cidadão (SIC), de que trata a Lei de Acesso à Informação, e seguir os prazos e procedimentos deste serviço.

A Tabela 1 apresenta os direitos que serão exercidos conforme regramento da LAI:

Direitos que seguirão regramento LAI	
Direitos do titular de dados pessoais	**Dispositivo na LGPD**
Receber confirmação da existência de tratamento de seus dados pessoais	Art. 18, I
Acessar seus dados pessoais	Art. 18, II
Receber informação das entidades públicas e privadas sobre com as quais o controlador realizou uso compartilhado de seus dados pessoais, quando aplicável	Art. 18, VII
Receber informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;	Art. 18, VIII
Receber informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.	Art. 20, §1°

Tabela 1. Direitos que seguirão regramento LAI. Referência LGPD.

Diferentemente, no que tange aos demais direitos garantidos pela LGPD, que não se caracterizam como direito fundamental de acesso à informação, mas sim, essencialmente, decorrem da autodeterminação informativa, como também no caso específico da revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, para o seu exercício, poderá ser adotado o mecanismo estabelecido pelo Código de Defesa dos Usuários de Serviços Públicos - Lei n° 13.460/2017.

Esse mesmo entendimento está disposto no Guia de Boas Práticas

da Lei Geral de Proteção de Dados do Comitê Central de Governança de Dados do Poder Executivo Federal, quando versa sobre exercício dos direitos dos titulares perante a Administração, diferencia-os em meios de acesso à informação em transparência passiva e meios de petição e manifestação à administração pública.

O Guia mencionado explica que essa compreensão decorre do fato que, no âmbito administrativo, a LGPD cita expressamente as Leis nº 12.527/2011 (LAI), nº 9.784/1999 (Lei de Processo Administrativo) e nº 9.507/1997 (Lei do Habeas Data) como referências não exclusivas para o exercício dos direitos dos titulares. Porém, uma vez que a Lei não estabelece a observância exclusiva dos normativos citados e, considerando que o mecanismo estabelecido pelo Código de Defesa dos Usuários de Serviços Públicos - Lei nº 13.460/2017 - é mais célere e, portanto, mais benéfico ao titular para o exercício dos direitos apresentados na Tabela 2, poderia ser adotado como padrão para o recebimento de solicitações de providências e reclamações relativas ao tratamento de dados.

Direitos que seguirão regramento do Código de Defesa dos Usuários de Serviços Públicos	
Direitos do titular de dados pessoais	**Dispositivo na LGPD**
Solicitar correção de dados incompletos, inexatos ou desatualizados	Art. 18, III
Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD	Art. 18, IV
Solicitar a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD (não aplicável em Ouvidoria)	Art. 18, VI
Solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade	Art. 20

Tabela 2. Direitos que seguirão regramento do Código de Defesa dos Usuários de Serviços Públicos. Referência LGPD.

Especificamente acerca do direito de solicitar a eliminação dos dados pessoais tratados com o consentimento do titular, de que trata o art. 18, VI, da LGPD, importante esclarecer que ele não se aplica aos dados coletados pela Ouvidoria. Isso decorre do fato de que, conforme já descrito no item 3 deste Guia, o consentimento não é a base legal adequada para o tratamento de dados pessoais em Ouvidoria, desde que ela esteja atuando no cumprimento de suas obrigações e atribuições legais ou na execução da política pública.

Contudo, importante ressaltar que, art. 18, §2º da LGPD, prevê o direito de oposição, determinando que *"o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei"*.

Além dos direitos dos titulares apresentados nas Tabelas 1 e 2, em observância ao princípio da transparência, o órgão disponibilizará e dará ampla divulgação às informações acerca da identidade e contatos do encarregado, bem como de suas atribuições.

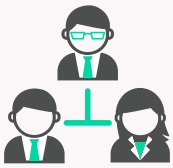
Desta forma, as informações do nome e cargo do encarregado indicado pelo controlador, horários e locais para atendimento do titular, telefone e e-mail para orientações e esclarecimentos de dúvidas, deverão estar disponíveis no sítio institucional do órgão e da Ouvidoria.

De modo complementar, o titular dos dados no exercício de seus direitos previstos na LGPD, deverá manifestar-se diretamente ao controlador responsável pelo tratamento dos dados pessoais do órgão, por meio dos canais oficiais. E, caso entenda que a manifestação não tenha sido atendida pelo controlador, o titular pode apresentar petição à Autoridade Nacional de Proteção de Dados, com a comprovação da ausência de atendimento.

Por fim, compreendida a distinção dos direitos de acesso à informação em transparência passiva e de meios de petição e manifestação à administração pública, importante que sejam definidas as ferramentas e fluxos internos de atendimento ao titular de dados pessoais no âmbito do Serviço de Informação ao Cidadão e Ouvidoria do órgão e estabelecido o relacionamento com o encarregado para atendimento às manifestações relacionadas ao tratamento de dados pessoais.

Em seguida, é necessário que ocorra a devida capacitação da

equipe de Ouvidoria para o acolhimento desses pedidos e manifestações e a ampla divulgação desses canais de atendimento.



7. AGENTES DE TRATAMENTO E DEMAIS ENVOLVIDOS NO EXERCÍCIO DOS DIREITOS DOS TITULARES

Considerando a Ouvidoria como o canal oficial de atendimento ao titular dos dados pessoais, uma vez que ela responde pelo SIC, criado pela LAI, e, ainda, pelo registro e acompanhamento de manifestações, à luz do Código de Defesa dos Usuários, é importante conhecer todos os atores envolvidos no processo. São eles o titular dos dados pessoais, os agentes de tratamento (controlador e operador), o encarregado e o ouvidor. Relevante ainda, nesse contexto, conhecer as atribuições da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), bem como as circunstâncias que podem ensejar a criação de uma Unidade de Governança para Proteção de Dados Pessoais, na forma de comissões, comitês, grupos de trabalho, entre outros.

Nesta seção serão reforçados os conceitos apresentados no item anterior deste Guia, bem como demonstrada a distinção e o relacionamento entre os agentes de tratamento, tendo como base o Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado, publicado pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD), que busca estabelecer diretrizes não vinculantes aos agentes de tratamento e explicar quem pode exercer a função do controlador, do operador e do encarregado, entre outros.

Conforme já mencionado, os agentes de tratamento (controlador e operador) são os responsáveis pelo tratamento dos dados pessoais, sujeitos às regras da LGPD e à fiscalização da ANPD.

Ao controlador compete a tomada de decisões referentes ao tratamento de dados pessoais e ao operador, a realização do tratamento em nome e conforme determinação do controlador.

Figura 3. Agentes de tratamento.

Dos conceitos de controlador e operador é possível identificar que a principal diferença entre eles está no poder de decisão, que recai sob o controlador, e no dever de observância, atribuído ao operador, que só poderá agir conforme as instruções do controlador. Outra distinção importante para compreensão dos conceitos é que o operador deve ser uma entidade distinta do controlador, ou seja, não poderá ser um funcionário do próprio órgão atuando sob a subordinação do controlador. Os funcionários, sob essa condição, não são operadores de dados pessoais.

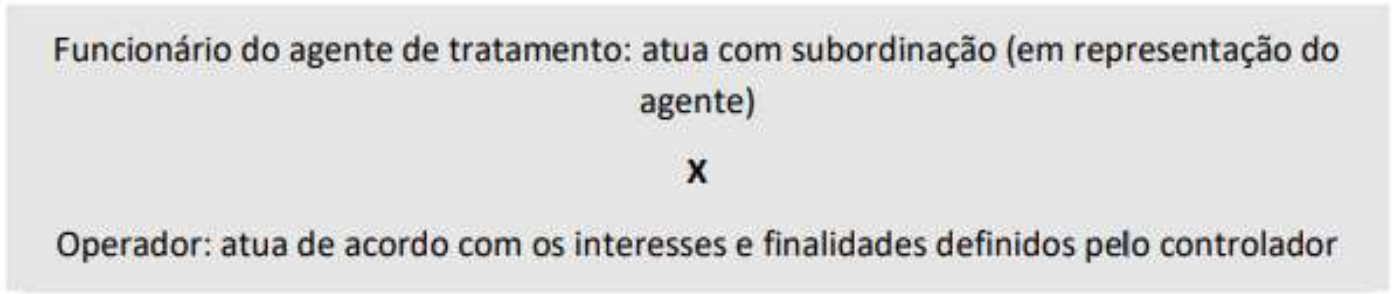
Importante esclarecer que quando se trata de uma pessoa jurídica, a organização é o próprio agente de tratamento para os fins da LGPD, já que é esta que estabelece as regras para o tratamento de dados pessoais a serem executadas por seus representantes ou prepostos. Os funcionários de uma organização não devem ser tidos como "operadores", mas sim como funcionário do agente de tratamento, atuando sob subordinação (em representação do agente), seguindo suas determinações.

Esse conceito é importante porque esclarece que o controlador e o operador podem ser a mesma pessoa, tendo em vista que seria a própria pessoa jurídica (organização), representada por seu dirigente máximo.

No caso das Ouvidorias Públicas, os servidores que nela atuam, bem como os gestores que respondem as manifestações recepcionadas, são tidos como funcionários, e não operadores. E, caso ocorra o compartilhamento da manifestação entre órgãos diferentes com foco na construção da resposta e solução do caso apresentado, o agente de tratamento (controlador e operador) que fará o tratamento do dado pessoal passará a ser, também, o órgão que recebeu a manifestação, representado pelo seu dirigente máximo.

A Figura 2, extraída da 1ª versão do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, da ANPD, destaca essa distinção entre o funcionário do controlador e o operador de dados pessoais:

Figura 2. Distinção entre o funcionário do controlador e o operador de dados pessoais



Fonte: Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. ANPD. Maio, 2021. Página 06

Ainda tratando da distinção entre controlador e operador, o Guia de Boas Práticas da Lei Geral de Proteção de Dados, publicado pelo Comitê Central de Governança de Dados do Poder Executivo Federal, esclarece que a identificação dos controladores dependerá, em cada caso concreto, da existência do poder de decisão sobre os meios e a finalidade dos tratamentos de dados. Como exemplo, apresenta a situação em que serão controladoras as instituições públicas que firmarem contratos de gestão de registro de visitantes às suas dependências, estabelecendo a finalidade do tratamento e exigindo da empresa contratada que, nesse caso, será a

operadora de dados pessoais, a adoção dos meios técnicos necessários para garantir a observância dos princípios especificados no art. 6º da LGPD.

Cabe mencionar novamente que a depender da atividade/tratamento exercido, uma instituição pode figurar simultaneamente como controladora e operadora. Isso é especialmente relevante no caso de compartilhamento de dados entre ouvidorias ou diferentes órgãos públicos. Não obstante, essa distinção não ser abordada detalhadamente neste Guia, importante ficar claro que a classificação dos agentes de tratamento precisa ser analisada com cautela, uma vez que irá refletir diretamente nas responsabilidades de cada agente.

Assim, no exemplo mencionado referente às instituições públicas que firmarem contratos de gestão de registro de visitantes às suas dependências, caso a empresa contratada para prestação do serviço já tenha estabelecido os meios técnicos para sua execução e como pretendem atender às disposições da LGPD ou, ainda, quando terceiriza alguma parte do serviço prestado, elas também, em certa medida, figuram como controladoras.

Além dos agentes de tratamento, a LGPD criou a figura do encarregado pelo tratamento de dados pessoais, que será o indivíduo responsável por executar as ações definidas pelo controlador, com o intuito de garantir a conformidade da instituição à LGPD, com atribuições definidas no § 2º do art. 41, apresentadas no item 5. Conceitos, deste Guia.

É recomendável que o servidor indicado pelo controlador como encarregado de dados pessoais seja subordinado diretamente ao dirigente máximo do órgão, devendo ter experiência em gestão, com assessoria jurídica e tecnológica e autonomia para deliberar sobre questões que afetem os operadores. Ainda, para o fiel cumprimento de suas atribuições, é essencial que o encarregado conte com o apoio do controle interno e da ouvidoria. Ambas as áreas têm papel fundamental no fornecimento ao encarregado de informações necessárias às ações de controle.

Considerando as suas atribuições, o controle interno poderá apoiar o encarregado por meio de técnicas e métodos de gestão de riscos, diagnósticos de vulnerabilidades, planos de adequação aos normativos, prestação de contas, entre outros. E a Ouvidoria, por sua vez, poderá apoiá-lo, por exemplo, no processo de transparência e de atendimento ao

titular do dado pessoal, com informações estatísticas e gerenciais sobre as manifestações recepcionadas que possuem relação com a proteção de dados pessoais.

E, ainda, a depender do volume de dados pessoais tratados no âmbito da instituição ou do nível de maturidade da política de segurança e de privacidade instituídas, ou ainda, da sua inexistência, é recomendável considerar a possibilidade de criação de instância colegiada no âmbito do órgão, como uma Unidade de Governança para Proteção de Dados Pessoais, para coordenar e orientar a implementação das ações necessárias à adequação à LGPD.

No contexto de implementação da LGPD nas instituições públicas, o Ouvidor atua, primordialmente, em sua função típica de acolher o cidadão e, no caso específico, o titular de dados pessoais e, fornecer os meios necessários para ele requerer, perante a Administração Pública, o exercício dos seus direitos. Além desta função, importante se faz que o Ouvidor componha a Unidade de Governança para Proteção de Dados Pessoais, se instituída, considerando os fatores já mencionados, bem como a sua atuação na governança de serviços.

Por fim, importante missão recai sobre a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), órgão criado pela LGPD, com a competência de implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

O Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, publicado pela Autoridade em janeiro de 2022, ressalta que a ANPD é o *"...órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua implementação, no que se inclui a deliberação administrativa, em caráter terminativo, sobre a interpretação da lei e sobre as suas próprias competências e casos omissos (art. 55-K, parágrafo único; art. 55-J, XX). Além disso, a autoridade nacional detém competência exclusiva para aplicar as sanções administrativas previstas na LGPD, com prevalência de suas competências sobre outras correlatas de entidades e órgãos da administração pública no que se refere à proteção de dados pessoais (art. 55-K)."*

8. RELAÇÃO ENTRE A LEI DE ACESSO À INFORMAÇÃO (LAI) E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A LAI já previa, em seu art. 31, procedimentos e diretrizes para o tratamento de informações pessoais no âmbito público, entre eles, o tratamento transparente dos dados, a garantia expressa aos direitos de personalidade e o consentimento do titular para a sua disponibilização a terceiros, atribuindo, inclusive, a regulamento específico, a disposição sobre os procedimentos para tratamento de informação pessoal.

Não existe, portanto, hierarquia entre a LAI e a LGPD. Ambas são leis gerais que regulamentam direitos fundamentais específicos, sendo eles, direitos fundamentais de acesso à informação e de privacidade dos dados pessoais dos indivíduos, respectivamente.

Para melhor compreensão do exercício dos direitos consubstanciados pelas citadas leis, apresenta-se o seguinte exemplo: um cidadão, pai de paciente maior de 18 (dezoito) anos internado em hospital de determinada rede estadual de saúde, ao requisitar acesso às informações referentes ao plantão médico daquele hospital ou de quaisquer outras unidades de saúde daquele Estado, faz uso do seu direito fundamental de acesso à informação, consubstanciado na LAI. Se, por outro lado, esse mesmo pai deseja obter acesso ao prontuário médico de seu filho, estará diante de um dado pessoal cujo acesso é protegido pela Lei Geral de Proteção de Dados Pessoais.

Diferentemente, quanto à publicação ativa de informações na internet, por vezes, para cumprimento do princípio constitucional da publicidade, a administração pública necessita dar transparência a dados pessoais, a exemplo de beneficiários de auxílios financeiros.

No Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, a ANPD se posiciona no sentido de que a divulgação pública de dados pessoais, quando necessária ao atendimento ao princípio da publicidade, também deve ser realizada em conformidade com as

disposições da LGPD. O que significa dizer que, *"em termos práticos, considerando o reforço protetivo trazido pela LGPD ao titular de dados, é necessário realizar uma avaliação sobre os riscos e os impactos para os titulares dos dados pessoais bem como sobre as medidas mais adequadas para mitigar possíveis danos decorrentes do tratamento de dados pessoais",* reforçando, com maior detalhamento, a necessidade já prevista na LAI. Para aprofundamento sobre o tema, recomenda-se a leitura do Guia.

Em decorrência das dúvidas em relação à publicação de informações pessoais no âmbito da administração pública, é possível que ocorra, também, o indeferimento equivocado de pedidos de acesso à informação, nos Serviços de Informação ao Cidadão, sob a alegação de infringir a LGPD.

Um exemplo desta situação são as informações sobre servidores públicos. Acerca dessas informações, em específico, é possível esclarecer que informações de servidores públicos referentes às suas atividades laborais, como escala de trabalho, gozo de férias, realização de viagens a trabalho e recebimento de diárias, geralmente, são informações públicas. Diferentemente, o número do cadastro de pessoa física e a classificação estatística internacional de doenças e problemas relacionados com a saúde (CID) que provocaram afastamentos para tratamento médico de servidores, estas sim, são informações pessoais, pois não decorrem diretamente das atividades laborais do servidor.

Nesse sentido, a Controladoria-Geral da União emitiu o Enunciado nº 04, de 10 de março de 2022, com seguinte teor:

> *Nos pedidos de acesso à informação e respectivo recursos, as decisões que tratam da publicidade de dados de pessoas naturais devem ser fundamentadas nos arts. 3º e 31 da Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI), vez que:*
>
> *A LAI, por ser mais específica, é a norma de regência processual e material a ser aplicada no processamento desta espécie de processo administrativo; e*
>
> *A LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos.*

9. GESTÃO DE RISCOS APLICADA ÀS OUVIDORIAS

Sobre a gestão de riscos enquanto metodologia que auxilia na prevenção do impacto provocado por possíveis intercorrências no processo de trabalho, entende-se como extremamente necessária na implementação de boas práticas para aplicação da LGPD.

A aplicação de salvaguardas com foco na proteção do sigilo dos dados pessoais do manifestante é uma medida que a maioria das Ouvidorias já adota há anos, com o objetivo de resguardar o cidadão. Essas medidas têm o intuito de transmitir segurança e confiabilidade no mecanismo da Ouvidoria. Assim o usuário sente-se protegido para informar seus dados pessoais e prestar informações relevantes para o atendimento da sua demanda.

Como já mencionado, com o advento da LAI e da LGPD, essas salvaguardas foram intensificadas e sistematizadas com adoção de providências mais eficientes. E nesse contexto, a gestão de riscos se torna um importante instrumento que auxilia na detecção de possíveis riscos de vazamento de dados, bem como de erros operacionais intencionais ou não.

A partir dessa premissa, apresenta-se como boa prática o levantamento inicial dos riscos no âmbito das Ouvidorias no contexto de planejamento organizacional, mapeamento de processos e definição de plano de ação para aplicação da LGPD.

É importante destacar que a "Privacidade desde a Concepção" *(privacy by design)* pode ser aplicada ao gerenciamento de riscos. Isso porque esse termo se trata de uma estrutura que tem como proposta central incorporar a privacidade e a proteção de dados pessoais em todos os projetos e processos desenvolvidos por uma organização, desde a sua concepção. Essa metodologia implica adotar uma postura proativa, em vez de reativa, ou seja, o gerenciamento deve se respaldar na prevenção do risco e não na remediação.

Considerando os riscos levantados, teremos mais clareza sobre onde devemos atuar e envidar mais esforços, pois, de acordo com a metodologia, deve-se priorizar a realização de ações mitigadoras nos riscos classificados

como extremos e altos, que apresentam maior probabilidade de acontecer e cujo impacto nos processos de trabalho é mais alto.

Nesse mesmo contexto, após identificados potenciais riscos ou até mesmo riscos materializados, deve-se elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), disposto no §3ª do artigo 4º, da LGPD. Para apoiar os órgãos da administração pública federal, o Comitê Central de Governança de Dados do Poder Executivo Federal disponibilizou Guia e *template* para elaboração do RIPD, que pode ser utilizado como referência, consolidando diversas referências a publicações e a outros documentos técnicos já existentes, que poderá ser utilizado como referencial para análise das demais esferas administrativas, além do Poder Executivo Federal.

Além do mencionado Guia, recomenda-se os seguintes materiais como sugestão de conteúdo sobre como aplicar a Gestão de Riscos:

- Gestão de Riscos – Avaliação da Maturidade – elaborado pelo Tribunal de Contas da União (TCU) - Link: https://portal.tcu.gov.br/data/files/0F/A3/1D/0E/64A1F6107AD96FE6F18818A8/Gestao_riscos_avaliacao_maturidade.pdf

- Metodologia de Gestão de Riscos – elaborada pela Controladoria-Geral da União CGU) – Link: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf

- Guia de Avaliação de Riscos de Segurança e Privacidade - Lei Geral de Proteção de Dados Pessoais (LGPD) – elaborado pelo Comitê Central de Governança de Dados do Poder Executivo Federal – Link: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf

- COSO. Committee of Sponsoring Organizations of the Treadway Commission. Gerenciamento de Riscos Corporativos – Estrutura Integrada. 2017.

- COSO. Committee of Sponsoring Organizations of the Treadway Commission. Risk Assessment in Practice.

10. PASSO A PASSO PARA ADEQUAÇÃO DAS OUVIDORIAS À LGPD

Nesta seção do Guia, serão apresentados os passos necessários para adequação das Ouvidorias à LGPD, com as providências iniciais para sua realização.

São eles: (1) mapear os dados pessoais sob a responsabilidade da ouvidoria; (2) mapear processos e ações da ouvidoria; (3) identificar os riscos relevantes envolvidos em cada um desses processos; (4) analisar quais ações de resposta poderão ser adotadas; (5) revisar os processos e ações relacionadas aos riscos relevantes identificados e (6) adequar os documentos internos e termos de contrato.

Importante esclarecer que a depender da estrutura e organização de cada Ouvidoria, bem como do órgão ao qual está vinculada, se houver, os referidos passos podem ser realizados em ritmo mais acelerado ou mais lento e, ainda, dentro de cada um desses passos, a abrangência da ação pode ser ampliada gradativamente, de maneira incremental, a partir de uma priorização com base numa análise dos riscos mais relevantes.

Passo 1: Mapear os dados pessoais sob a responsabilidade da ouvidoria

Sob a coordenação da Unidade de Governança para Proteção de Dados Pessoais do órgão, é recomendável que seja elaborado o Inventário de Dados Pessoais a partir de uma priorização por meio de uma análise de riscos, documento fundamental para registro do tratamento de dados pessoais realizados pela instituição.

O inventário se faz necessário, dentre outros motivos, para o fiel cumprimento do art. 37 LGPD, que dispõe que o *"controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse"* e consiste, também, uma forma efetiva de levantar quais dados pessoais são tratados, onde e como estão armazenados, quais operações são realizadas com eles e, ainda, com qual finalidade.

É recomendável que esse processo de mapeamento seja articulado com a governança de dados de um ponto de vista mais abrangente na organização. Dessa forma, o inventário elaborado pode ser restrito apenas à identificação dos dados pessoais, mas a todas as operações envolvendo dados na instituição. Isso porque os sistemas podem ser alterados e passar a coletar dados pessoais, devendo observar a LGPD desde a sua concepção.

De acordo com o Guia de Elaboração de Inventário de Dados Pessoais - Lei Geral de Proteção de Dados Pessoais, publicado pelo Comitê Central de Governança de Dados do Poder Executivo Federal, de maneira geral, o Inventário deve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade, tais como:

- atores envolvidos (agentes de tratamento e o encarregado);
- finalidade (o que a instituição faz com o dado pessoal com base em atribuição legal);
- base legal do tratamento (arts. 7º e 11 da LGPD);
- previsão legal (dispositivos legais ou normativos que determinam o tratamento dos dados)
- dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 LGPD);
- medidas de segurança atualmente adotadas.

Importante observar que devem ser identificados os dados pessoais constantes em quaisquer meios, físicos ou eletrônicos. Para tanto, deve-se buscar identificar a existência, por exemplo, de documentação em papel arquivada na Ouvidoria, onde constem dados pessoais do usuário, como formulários de atendimento presencial, de cadastro ou, até mesmo, formulários de manifestações, comumente utilizados em urnas coletoras e em ações itinerantes de Ouvidoria.

Especificamente, no tocante à finalidade, importante mencionar que o mapeamento deve considerar todo o fluxo de dados, isso porque

um mesmo dado pode ser tratado para finalidades diferentes, por setores diferentes, por exemplo, sendo exigida uma base legal para cada finalidade.

Passo 2: Mapear processos e ações da Ouvidoria

O mapeamento do processo é uma técnica que busca identificar falhas e potencialidades, para posterior correção e disseminação, respectivamente, e evitar a utilização de procedimentos isolados que não consideram o processo como um todo, fazendo com que os trabalhos sejam conduzidos de forma mais integrada, proporcionando alcance de resultados com mais eficiência.

Com o advento da LGPD, o mapeamento de processos ganha ainda maior importância, pois a partir da análise detalhada de cada etapa dos processos é possível a identificação da ocorrência de tratamento de dados pessoais, na forma de coleta, produção, acesso ou quaisquer formas de tratamento de que trata o art. 5º, inciso X da Lei.

Uma vez identificados os processos e respectivas etapas em que ocorrem tratamentos de dados pessoais, é necessário avaliar a sua conformidade aos princípios, diretrizes e direitos previstos na Lei Geral de Proteção de Dados Pessoais. Caso estejam em desconformidade, será o caso de prever adequação para tanto.

Inclusive, é recomendável que o Inventário de Dados citado no passo 1 seja realizado em consonância com o mapeamento de processos ou, até mesmo, de forma concomitante.

Passo 3: Identificar os riscos relevantes envolvidos em cada um desses processos

Conforme a ABNT, a gestão de riscos consiste em *"atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos"* (ABNT NBR ISO/IEC 31000:2018).

Em adição, de acordo com o COSO 2017, modelo internacional de referência em gestão de riscos aplicável às instituições públicas, o gerenciamento de riscos corporativos está baseado na manutenção de práticas alinhadas às estratégias e objetivos das organizações, as quais, por sua vez, devem estar adaptadas a ambientes de negócios globais e altamente dependentes de tecnologia. Nesse sentido, o modelo ressalta

a importância de se analisar o risco na definição das estratégias e para o desenvolvimento das organizações.

No que concerne aos sistemas informatizados utilizados pelas Ouvidorias, faz-se essencial a atuação conjunta da Ouvidoria com a área de tecnologia do órgão, para a avaliação dos riscos de segurança e privacidade.

Importante reforçar que nesses sistemas as ouvidorias tramitam não apenas informações pessoais como a identificação dos manifestantes que, nos termos do §7º. art. 10, da Lei nº 13.460, de 26 de junho de 2017, *"é informação pessoal protegida com restrição de acesso nos termos da Lei nº 12.527, de 18 de novembro de 2011",* como também o teor das manifestações apresentadas, cujo acesso só deve ser permitido com a finalidade de apuração ou para tomada de providência acerca do que foi apresentado.

A título exemplificativo, a Lei nº 16.420, de 17 de setembro de 2018, aplicável ao Poder Executivo do Estado de Pernambuco, atribui à Ouvidoria-Geral e às Ouvidorias dos órgãos e entidades estaduais o dever, dentre outros, de *"garantir o sigilo, a discrição e a fidedignidade quanto ao conteúdo e providências das manifestações recebidas".*

De maneira similar, a Norma Modelo para Criação de Unidades de Ouvidoria aprovada pela Resolução Nº 7, de 30 de novembro de 2021, da Coordenação Geral da Rede Nacional de Ouvidorias, trata do sigilo das manifestações quando estabelece a necessidade de estrutura adequada para atendimento ao usuário, com vistas a resguardá-lo, e quando dispõe sobre a possibilidade de utilização de base de dados e sistema informatizado cedidos por órgãos públicos, que deverá obedecer critérios técnicos que garantam a segurança e o sigilo dos dados.

Com o intuito de fornecer aos responsáveis pelo tratamento de dados pessoais do Poder Executivo Federal uma orientação para identificar lacunas de segurança da informação e de privacidade sobre os sistemas, contratos e processos da instituição, o Comitê Central de Governança de Dados do Poder Executivo Federal publicou o Guia de Avaliação de Riscos de Segurança e Privacidade, que poderá ser utilizado como referência nesta avaliação de sistemas, inclusive, os de registro e tramitação de manifestações de ouvidoria.

Passo 4: Analisar quais ações de resposta poderão ser adotadas

A Lei Geral de Proteção de Dados Pessoais, em seu artigo 50, estabelece que os controladores e operadores, no âmbito de suas competências, deverão formular regras de boas práticas e de governança.

Especificamente, a alínea 'g', I, §2º, do mesmo artigo determina que planos de resposta a incidentes e remediação deverão constar nos programas de governança em privacidade que poderão ser instituídos pelos mencionados agentes de tratamento. E, além deste plano, há outros controles aplicáveis na formulação de respostas ao risco, como controle de acesso, desenvolvimento seguro, gestão de continuidade, entre outros.

Neste contexto, elaborado o Inventário de Dados Pessoais da organização e a Avaliação de Riscos de Segurança e Privacidade, ambos tratados nos itens anteriores deste Guia, é necessário planejar as respostas aos riscos relevantes identificados, que se trata de etapa necessária à implementação da gestão de riscos, denominada Plano de Tratamento de Riscos, com foco na adoção de controles preventivos, atenuantes ou de recuperação.

Algumas das respostas aos riscos poderão corresponder a ajustes nos procedimentos de ouvidoria já existentes ou a criação de novos fluxos de comunicação, como exemplo, para garantir que todas as partes interessadas sejam informadas sempre que houver mudanças em atualizações de software e outros componentes das soluções de tecnologia da informação e comunicação. E, nos casos de respostas que ensejem mudanças das soluções de tecnologia da informação e comunicação utilizadas pela Ouvidoria, será necessária, mais uma vez, a análise conjunta com a área de tecnologia da organização.

Passo 5: Revisar os processos e ações relacionadas aos riscos relevantes identificados

Identificados os riscos relevantes dos processos e sistemas de ouvidoria, o próximo passo deverá ser a revisão desses processos, com o intuito de corrigir procedimentos e/ ou implantar controles que visem reduzir os riscos relevantes identificados e, em relação àqueles associados aos sistemas, buscar junto à área de tecnologia formas de mitigá-los.

Essa revisão deverá constar nos planos de resposta a incidentes e remediação, de que dispõe a Lei Geral de Proteção de Dados (LGPD), já abordado neste Guia.

Passo 6: Adequar os documentos internos e termos de contrato

Assim como os processos e ações da ouvidoria precisarão ser revisadas após identificação dos riscos, os documentos e demais registros da área também deverão ser objeto de análise e ajuste, caso necessário.

Exemplos de documentos que poderão necessitar de adequação no âmbito das Ouvidorias são os relatórios produzidos, em especial, relatórios gerenciais e termos de confidencialidade e sigilo. Deve-se observar que relatórios com informações estatísticas, apesar de apresentarem menor risco de conter divulgação indevida de dados pessoais, deverão, também, ser objeto de análise neste momento.

Essa necessidade de revisão aplica-se, também, a roteiros, *scripts* e materiais de orientação que sejam utilizados como referência às atividades de Ouvidoria.

Nesse contexto, é importante que se faça a revisão dos termos dos contratos firmados pela ouvidoria para suporte e desenvolvimento de sistemas de tecnologia da informação e comunicação, bem como para serviços de consultoria e fornecimento de mão de obra.

Independentemente do seu objeto, se para sua execução for necessário o acesso à base de dados de Ouvidoria, deverá ser incluída cláusula de proteção de dados pessoais e confidencialidade das manifestações nos respectivos contratos. Ou seja, nessa formalização devem constar cláusulas que assegurem a adoção das medidas de segurança pertinentes, bem como que vedem o compartilhamento com terceiros. A depender do tratamento dos dados realizado pela empresa contratada, ela pode ser considerada operadora dos dados, tratado no Capítulo 7 deste Guia, tendo responsabilidades sobre o tratamento dos dados pessoais.

A mesma análise deverá ser realizada e as adequações providenciadas, se necessário, em relação a outras formas de parcerias distintas da contratação, como formalização de convênios, termos de

parceria e congêneres.

Por fim, importante mencionar que, em consonância com a LAI e o princípio da transparência previsto na LGPD, esses documentos devem ser publicados, de forma a permitir aos titulares de dados conhecerem as práticas e os agentes de tratamento de seus dados.

11. BOAS PRÁTICAS APLICADAS À OUVIDORIA PARA ATENDIMENTO À LGPD

O Guia da Avaliação de Riscos de Segurança e Privacidade publicado pelo Comitê Central de Governança de Dados do Poder Executivo Federal estabelece um rol de riscos de segurança e privacidade e a indicação dos controles.

Neste capítulo do Guia de Boas Práticas na Aplicação da Lei Geral de Proteção de Dados Pessoais nas Ouvidorias Públicas, serão apresentadas boas práticas ou controles adicionais, sob a ótica do processo de tratamento de manifestações, fruto de debates do grupo de trabalho Lei Geral de Proteção de Dados Pessoais nas Ouvidorias da Rede Nacional de Ouvidorias Públicas (Renouv).

Importante reforçar que se tratam de boas práticas, e não de imposições às Ouvidorias, bem como que o que está aqui disposto é um rol exemplificativo, e não exaustivo, de medidas e ações que podem ser tomadas pelos órgãos e, especificamente, pelas Ouvidorias, para adequação ao disposto na LGPD.

Cabe mencionar, também, que na análise da possibilidade de implementação destas boas práticas, faz-se importante a reflexão sobre a realidade individual de cada Ouvidoria, considerando os recursos humanos, financeiros e tecnológicos disponíveis.

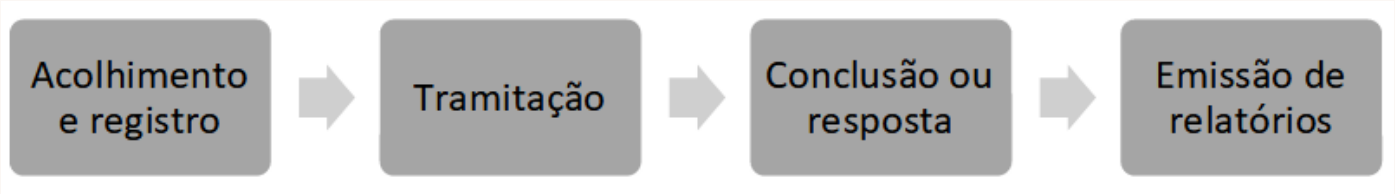
Outro ponto que se sugere considerar é que, mesmo Ouvidorias com uma boa estrutura e nível de maturidade elevado precisarão priorizar algumas boas práticas em detrimento de outras. E, como critério de escolha, para essa priorização, podem ser consideradas as boas práticas que têm

a potencialidade de mitigar mais de um risco ou aquelas que visem a mitigar os riscos mais altos, sendo eles aqueles com maior probabilidade de ocorrer e/ ou que, caso o evento ocorra, causarão consequências mais danosas ao órgão ou à Ouvidoria.

Dito isso, com o intuito de facilitar a compreensão, as boas práticas serão apresentadas em três grupos distintos, sendo o primeiro deles formado por aquelas que visam a mitigar o risco de acesso não autorizado aos sistemas e documentos da Ouvidoria, podendo ocorrer em qualquer etapa do fluxo do processo de tratamento de manifestações e pedidos de acesso à informação.

Em seguida, serão apresentados riscos e boas práticas relacionadas, especificamente, a cada etapa deste fluxo, que contempla (1) acolhimento e registro, (2) tramitação, (3) conclusão ou resposta e (4) emissão de relatórios, conforme Figura 4:

Figura 4. Etapas do fluxo das manifestações de Ouvidoria.



Ao final, serão apresentados riscos e as boas práticas, que não se relacionam, diretamente, com nenhuma das etapas desse fluxo.

11.1. Boas práticas relacionadas ao risco de acesso não autorizado aos sistemas e documentos da Ouvidoria

Pela exigência disposta no Código de Defesa dos Usuários, quanto à obrigatoriedade de identificação na apresentação de manifestações à Ouvidoria, bem como para permitir que as providências necessárias sejam tomadas pelos órgãos em relação a essas manifestações, a Ouvidoria trata dados pessoais e dados pessoais sensíveis em suas atividades.

Diante disto, algumas medidas se fazem necessárias para garantir a proteção desses dados armazenados.

Nesse contexto, as primeiras boas práticas que serão apresentadas

neste Guia são aquelas relacionadas a mitigar o risco de acesso não autorizado desses dados, que podem estar não apenas no sistema informatizado, como também em documentos em papel ou salvos na área de trabalho dos computadores dos servidores, por exemplo.

Risco: Acesso não autorizado ao sistema informatizado de ouvidoria, inclusive, à sua base de dados.

Este risco consiste, de maneira geral, no acesso não autorizado de pessoas ao sistema informatizado em uso pela Ouvidoria, incluindo-se, neste contexto, o acesso diretamente à base de dados de ouvidoria por servidores e colaboradores responsáveis pela manutenção e evolução do sistema.

Será considerado neste risco, também, o acesso ilegal ao sistema por *hackers*.

Boas práticas: Utilizar sistema informatizado com controle efetivo de acesso, e demais requisitos de segurança necessários para mitigar o risco de invasão.

Sabe-se que a Política de Segurança da Informação tem como objetivo limitar a exposição ao risco a níveis aceitáveis e buscar continuamente a disponibilidade, a integridade, a confidencialidade, a autenticidade. Neste contexto, deve-se ater às questões de controle de acesso, garantindo que os usuários tenham acesso apenas aos recursos necessários à execução do seu trabalho e da audibilidade, que consiste na garantia de rastreabilidade de usuários e processos por meio de registro detalhado.

O controle de acesso também é considerado uma medida de segurança que tem como objetivo proteger equipamentos, *softwares,* arquivos de dados, modificação ou divulgação de informações, entre outros e, basicamente, são classificados em controles de acesso físicos ou lógicos.

O controle de acesso físico busca proteger o acesso de pessoas em determinado local e é composto de uma barreira, uma porta, fechaduras, catracas, chaves, entre outros. Já o controle de acesso lógico, tem como objetivo garantir a segurança das informações, além disso, deve garantir que apenas usuários autorizados tenham acesso ao sistema.

Em outras palavras, o controle de acesso é um conjunto de

procedimentos e medidas com o objetivo de proteger as informações de um sistema contra as tentativas de acesso não autorizadas por outras pessoas. É um exemplo de controle, o acesso ao sistema mediante *login* e senha, para validar que essa determinada pessoa possui acesso autorizado ao sistema.

Ainda com relação ao controle de acesso, é importante implantar controles e estar atento para que credenciais de acesso legítimas não sejam obtidas e utilizadas por pessoas não autorizadas. Práticas inseguras como o registro de senhas em arquivos de texto em computadores pessoais ou pastas compartilhadas podem ser causas de vazamento de dados de sistemas. Para evitar que isso aconteça, é recomendável que o órgão mantenha uma política de gestão de senhas e atualização periódica obrigatória.

Nesse contexto, deve constar na Política de Segurança da Informação do órgão e, principalmente, estarem em pleno funcionamento no sistema informatizado, requisitos de segurança disponíveis que impeçam, efetivamente, a invasão à base de dados por ação de *hackers*, como exemplos, a instituição de senha forte de acesso e o ambiente protegido.

Uma senha forte deve conter, por exemplo, um composto de letras maiúsculas e minúsculas, números e símbolos e, deve ainda, formar uma sequência aleatória, ou seja, uma frase que não tenha nenhum sentido lógico. É uma boa prática, também, que essa senha seja alterada, preferencialmente, de 3 em 3 meses.

Boas práticas: Submeter à assinatura de termo de confidencialidade aos colaboradores que realizam ações de suporte e manutenção de tecnologia da informação e comunicação.

A importância do termo de confidencialidade no contexto das Ouvidorias será ressaltada, também, na etapa de acolhimento e registro de manifestações, em relação aos colaboradores que estarão autorizados a realizar este acolhimento e, consequentemente, a coleta de dados pessoais dos usuários do serviço.

No contexto do risco de vazamento, pretende-se ainda incluir a prática de assinatura destes termos por aqueles que acessam o sistema e, até mesmo a sua base de dados diretamente, quando realizam operações de manutenção e evolução do sistema. Aqui estão se tratando daqueles

que dão o suporte e o apoio em tecnologia da informação e comunicação necessários às atividades de Ouvidoria.

Caso esse serviço de suporte seja prestado por meio de uma contratação de empresa especializada, a obrigação de sigilo, inclusive da assinatura do termo de confidencialidade deve ser incluída entre as cláusulas contratuais.

É interessante, ainda, que o próprio sistema informatizado utilizado pela Ouvidoria mostre avisos aos usuários relembrando sobre a Política de Privacidade da instituição e a obrigação de sigilo.

Risco: Acesso não autorizado aos documentos e informações de Ouvidoria armazenados em meios eletrônicos.

Além dos dados pessoais que constem no sistema informatizado, a Ouvidoria deverá proteger, do risco de acesso por pessoa não autorizada, os dados que, porventura, constem em documentos armazenados nas redes internas ou, na área de trabalhos dos computadores dos servidores e colaboradores da ouvidoria.

Boas práticas: Possuir sistema de gestão documental para armazenamento e acesso a documentos de ouvidoria em meio eletrônico.

Para um armazenamento seguro de documentos eletrônicos da Ouvidoria, em especial, aqueles que, porventura, contenham dados pessoais dos manifestantes, é aconselhável que a organização possua um sistema de gestão de documentos.

Desta forma, além de deixá-los armazenados em um único local, é possível controlar o acesso a eles e, ainda, deixar as informações com acesso restrito, para que somente aquelas pessoas autorizadas possam acessá-las.

Ademais, neste sistema também ficam centralizadas as informações de um determinado processo, facilitando, sobremaneira, as tarefas do dia a dia.

Caso a organização não disponibilize de um sistema de gestão documental, pode seguir algumas boas práticas quanto ao armazenamento dos arquivos em rede interna, conforme abaixo:

• Organizar uma pasta para cada processo e dentro organizar subpasta;

• Nomear as pastas;

• Atribuir identificação específica aos documentos eletrônicos e aos escaneados;

• Utilizar caracteres simples;

• Não abreviar;

• Colocar data nos documentos com mais de uma edição;

• Ativar a indexação do seu sistema operacional.

Risco: Acesso não autorizado aos documentos e informações de Ouvidoria reproduzidos em meio distinto ao sistema informatizado de ouvidoria, como impresso em papel ou copiado e encaminhado por correio eletrônico (e-mail).

Não obstante a digitalização do serviço de ouvidoria estar em crescente expansão, não apenas, especificamente, com o sistema informatizado de ouvidoria, como também, com o uso de outros sistemas de tramitação de processos, a exemplo do Sistema Eletrônico de Informação (SEI), é compreensível que as Ouvidorias estejam em níveis distintos de maturidade nesse processo, remanescendo situações em que o registro e a tramitação de manifestações ocorram em meio físico.

E, até mesmo em Ouvidorias que utilizam sistema informatizado, é possível existir situações de indisponibilidade do sistema em uso, o que as leva a utilizar outras formas de registro e tramitação, dentre elas aquelas em meio físico, com documentação impressa em papel.

Outras duas circunstâncias que podem ensejar a produção de documentos de ouvidoria em meio distinto do sistema, é a realização de ação itinerante e a captação de manifestações por meio de urnas coletoras.

Nesse contexto é importante estar claro que arquivos físicos também são regidos pela LGPD. Assim, se a Ouvidoria recebe manifestações em formulários em papel e os coloca em um espaço sem segurança, por exemplo, apoiado em uma mesa em uma sala de acesso público e esses documentos se perdem, trata-se de incidente de segurança tanto quanto uma invasão em sistemas informatizados.

Boa prática: Levantar os fluxos de trabalho e estabelecer procedimentos considerando o eventual uso e armazenamento de documentos onde constem dados pessoais dos manifestantes, em meios físicos.

As Ouvidorias devem buscar implantar mecanismos e o desenvolvimento de uma cultura de proteção dos dados pessoais do cidadão, independente do canal e do suporte utilizado para registro, seja ele físico, lógico ou analógico. Para isto, como já mencionado, é essencial manter uma boa gestão dos documentos eletrônicos armazenados nas redes internas, na área de trabalho dos computadores, encaminhados por e-mail, entre outros.

Especificamente, quanto aos documentos arquivados em meio físico, é importante que eles sejam mantidos em armários fechados e que haja barreiras físicas de proteção, a exemplo de cadeados, com a atenção à guarda das chaves.

Nesse sentido, entende-se como uma boa prática o levantamento dos fluxos de trabalho e estabelecimento de procedimentos adequados considerando o eventual uso e armazenamento de documentos onde constem dados pessoais dos manifestantes, em todos os formatos aplicáveis, como consta no primeiro passo para a adequação das Ouvidorias à LGPD, de que trata capítulo 10 deste Guia.

A adequação ou a criação dos procedimentos deve considerar, além dos aspectos relacionados à LGPD, as normas arquivísticas e de segurança da informação vigentes e aplicáveis em todos os casos e para todas as ferramentas envolvidas na execução. Para isto, seguem algumas dicas:

Dica 1: Quando for indispensável a reprodução de dados em formatos distintos, por exemplo, de papel para documento eletrônico, observar os mecanismos de segurança previstos para os dois suportes.

Dica 2: Quando da utilização de outros meios, diferentes do sistema de Ouvidoria, como e-mail ou Sistema SEI, inserir mecanismos que dificultem a reprodução ou utilização das informações ali presentes, tais como mensagem em formato “imagem” ou inserção de marca d`água.

Dica 3: O sistema de Ouvidoria deve prever, em seus mecanismos de rastreabilidade, o registro dos dados e informações gravadas

e/ou distribuídas em outra ferramenta. Tal procedimento visa à rastreabilidade dos dados pessoais e à mitigação de riscos decorrentes da falha na segurança.

Dica 4: Fomentar a importância e as vantagens de uso do sistema de Ouvidoria para fins de atendimento, evitando a utilização de mecanismos como e-mail e sistemas diversos para cadastro e tramitação de demandas, dando preferência à disposição dos dados coletados e tramitados exclusivamente no sistema informatizado de ouvidoria.

Boa prática: No caso de acolhimento de manifestações em formulários em papel, observar requisitos de segurança da informação, como a coleta e acesso apenas por atendente autorizado.

Nos casos das Ouvidorias que utilizarem como canal de captação de manifestações as urnas coletoras, onde as manifestações estarão registradas em um formulário em papel, os seguintes requisitos de segurança devem ser observados:

- O material utilizado na confecção da urna não deve ser transparente, evitando assim que seja possível a leitura dos formulários que estejam nela depositados; assim, ela pode ser translúcida ou adesivada;

- A urna deverá estar, permanentemente, trancada com cadeado;

- A coleta deverá ser realizada, exclusivamente, por servidor da Ouvidoria ou aquele por ela autorizado, com termo de confidencialidade devidamente assinado;

- A frequência de recolhimento deve ser pré-estabelecida e deverá estar afixada, junto à urna, para conhecimento do usuário.

Estas medidas visam evitar os riscos, por exemplo, de extravio de formulários dentro das urnas ou do não depósito de novos formulários, pelos usuários da Ouvidoria, visto a urna estar cheia.

De toda forma, é importante reforçar que a coleta de manifestações por meio de urnas não permite a verificação da titularidade, impedindo assim, o exercício de direitos previstos na LGPD, como de correção de dados incompletos, inexatos ou desatualizados, tratados em capítulo específico neste Guia.

Boas práticas: Nos casos de formulários em papel utilizados em ações itinerantes de Ouvidoria, importante que a sua coleta seja realizada, exclusivamente, por servidor ou colaborador da Ouvidoria devidamente autorizado e o mesmo se aplica àquele que fará a transferência dos dados do meio físico para o sistema informatizado de ouvidoria.

Em ações itinerantes, é importante também observar os cuidados com a guarda e manuseio dos formulários de manifestações coletados, para que não haja seu extravio ou acesso de pessoa não autorizada.

É bem comum, nessas ações, que haja o engajamento de servidores e colaboradores de outras áreas, distintas da Ouvidoria, com o intuito de ampliar o seu alcance. Todavia, é importante reforçar que, mesmo nessas ações, a coleta dos dados pessoais deve ser realizada, exclusivamente, por servidor. Na possibilidade de coleta por colaborador, ou seja, funcionários terceirizados ou estagiários, é importante que tenham, previamente, assinado termo de confidencialidade.

11.2. Boas práticas e riscos associados às etapas do processo de tratamento de manifestações de Ouvidoria

Nesta seção, estão reunidos os riscos e boas práticas identificados no processo de tratamento de manifestações de Ouvidoria, especificamente, em cada uma de suas etapas, sendo elas o acolhimento e registro, a tramitação, a conclusão ou resposta e a emissão de relatórios.

Não obstante essa disposição por etapas, é possível que um risco possa vir a ocorrer em mais de uma delas, estando apresentada aqui aquela considerada a que havia maior probabilidade de ocorrência do risco.

Etapa Acolhimento e registro

A etapa ou o momento de acolhimento e registro da demanda é o modo habitual por meio do qual os usuários que procuram a Ouvidoria realizam o primeiro contato com o atendimento em si. Nessa etapa, as demandas dos usuários são recepcionadas em forma de reclamações,

denúncias, solicitação de providências, elogios, dentre outras, culminando no conhecimento da alta gestão a fim de tomada de ações.

A coleta de dados realizada nesta etapa constitui-se em uma das operações de tratamento realizada durante o contato inicial dos(as) cidadãos(ãs) nas Ouvidorias.

Importante observar que a coleta de dados deverá estar pautada no princípio da necessidade, como forma de assegurar ao titular que não sejam solicitados dados desnecessários ou excessivos diante da demanda apresentada, bem como que os seus dados não sejam utilizados para outros fins.

Como boas práticas, de maneira geral, no cadastro inicial do cidadão, se houver, e no registro da manifestação realizados nas Ouvidorias, elencam-se as seguintes ações a serem incorporadas ao trabalho da equipe da Ouvidoria e objeto de atualização, sempre que necessário:

1) A rotina de conferência dos dados coletados deverá ser realizada de forma atenta e minuciosa, com o objetivo de evitar erros na identificação do cidadão(ã);

2) Tendo em vista o princípio da necessidade, a Ouvidoria coletará os dados estritamente necessários ao atendimento da demanda apresentada pelo titular do dado e adotará medidas internas, que visem à proteção dos dados coletados de acessos não autorizados, de situações acidentais ou ilícitas. Desta forma, medidas de segurança deverão ser adotadas nos sistemas e procedimentos de coleta e armazenamento dos dados utilizados pela Ouvidoria;

3) Nos sistemas informatizados de autoatendimento das Ouvidorias, deverá ser esclarecido ao titular dos dados a finalidade e a necessidade de coleta dos dados, bem como a forma que ocorrerá o tratamento dos dados no âmbito do órgão e as medidas de contenção ou mitigação dos riscos associadas às violações de segurança, à luz do princípio da transparência previsto na Lei nº 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD) e

4) No caso da coleta de dados pessoais ou pessoais sensíveis complementares, para fins de estudo do perfil do usuário dos

serviços, para adequação de canais de atendimento e melhoria de políticas públicas, por exemplo, o titular deverá ser comunicado sobre essa possibilidade de utilização do dado no ato da coleta com clareza e objetividade.

A partir desse ponto, passam a ser apresentadas as boas práticas correlacionadas a riscos identificados na etapa de acolhimento e registro de manifestações de Ouvidoria.

A observância dos princípios da necessidade e finalidade é de extrema importância em todas as etapas do fluxo da manifestação de Ouvidoria, sobremaneira, na etapa de acolhimento e registro, quando ocorre a coleta dos dados pessoais.

Nesse sentido, a ANPD, posiciona-se no Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público que, *"muitas vezes, a coleta indiscriminada de dados pessoais é o ponto principal a ser considerado, de modo que, ao invés de eventual e posterior atribuição de sigilo, a proteção será mais efetiva com a própria dispensa da coleta ou com a eliminação da informação".*

Riscos: Inexistência, não apresentação ou falta de clareza do Termo de Uso e da Política de Privacidade.

Este risco corresponde a não apresentação do Termo de Uso e da Política de Privacidade ao titular do dado pessoal no ato de cadastro, junto à Ouvidoria ou de registro de manifestações, que pode se dar pela inexistência dos instrumentos ou pela não disponibilização no momento.

Pode haver, ainda, a apresentação do Termo de Uso e da Política de Privacidade, porém, pode não existir clareza na linguagem, dificultando ou, até mesmo, impedindo a compreensão.

E ambas situações podem ocasionar, inclusive, a inibição do registro de manifestações pelo titular, em razão da insegurança gerada ao usuário, pelo desconhecimento do uso que será dado à informação.

Boas práticas: Elaborar e apresentar ao usuário do serviço de Ouvidoria, no ato de cadastro, junto à Ouvidoria, se houver, ou de registro de manifestações, o Termo de Uso e a Política de Privacidade do serviço.

Em atenção ao princípio da transparência, o cidadão necessita ter ciência da finalidade com qual serão utilizados os seus dados pessoais, inclusive, com qual temporalidade. Para isso, ao utilizar os serviços da Ouvidoria, o usuário deve confirmar que leu, compreendeu e tem ciência dos termos e políticas aplicáveis, ficando a eles vinculado.

O Termo de Uso é o documento legal por meio do qual o órgão deverá definir as regras da utilização dos serviços informatizados de ouvidoria. Igualmente, por intermédio da Política de Privacidade, o órgão deve esclarecer como os dados pessoais dos usuários serão tratados.

Portanto, é imprescindível que a instituição elabore Termo de Uso e Política de Privacidade no tocante aos serviços de Ouvidoria do órgão e divulgue no sítio eletrônico oficial e, nele também, deve ser feita ampla divulgação, caso haja posterior atualização desses documentos.

Nos casos das Ouvidorias que utilizam cadastro prévio para realização de manifestações, a ciência do usuário no Termo de Uso e na Política de Privacidade poderá ser requisitada uma única vez, no ato do cadastro e não a cada manifestação registrada.

Para elaboração do Termo de Uso e da Política de Privacidade, pode ser utilizado, de maneira referencial, o Guia de Elaboração de Termo de Uso e Política de Privacidade para serviços públicos, publicado pelo Comitê Central de Governança de Dados do Poder Executivo Federal.

Risco: Coleta de dados realizada por atendente não autorizado.

Nesse caso, o risco decorre da ausência de compromisso dessa pessoa com os protocolos adotados pelo setor e a responsabilização direta sobre as informações coletadas.

Boas práticas: Definir os servidores e colaboradores das equipes que estarão autorizados a realizar os atendimentos aos titulares dos dados, promover as ações de capacitação necessárias e garantir a ciência do dever de sigilo por meio de assinatura de termo de confidencialidade ou documento análogo pelos colaboradores.

A Ouvidoria deverá definir os perfis de acesso ao sistema informatizado, junto com a área de tecnologia da informação, com

permissões específicas e compatíveis com a finalidade da utilização do dado.

Recomenda-se, inclusive, de acordo com o quantitativo de servidores que compõem a equipe, definir perfis distintos para as diversas operações que podem ser realizadas na ferramenta, a exemplo de cadastro, consulta, encaminhamentos, resposta, administração, gestão, entre outros.

No contexto específico da LGPD, ou seja, na coleta de dados pessoais na etapa de acolhimento do fluxo da manifestação de Ouvidoria, especificamente, quanto ao atendimento presencial do titular, é importante que seja realizada a seleção de quais servidores e colaboradores estarão autorizados para realização deste atendimento e haja a devida comunicação à equipe.

E, após essa definição, é importante observar se os colaboradores já assinaram o termo de confidencialidade, como mais uma medida de proteção dos dados pessoais.

Importante ressaltar que, nos casos de servidores públicos, os estatutos de servidores federais, estaduais e municipais, e em alguns casos, códigos de ética específicos de determinadas carreiras, em geral, já preveem a obrigação do sigilo profissional e, por este motivo, o termo de confidencialidade não se faz necessário.

Diferentemente, quanto aos colaboradores que atuam sob contrato de fornecimento de mão-de-obra especializada, a referida obrigação deve constar no contrato administrativo firmado com a pessoa jurídica e, neste caso, pela ausência de vínculo do colaborador com a administração pública, o termo de confidencialidade torna-se indispensável.

O mesmo se aplica caso o relacionamento do colaborador com o órgão público se dê por meio de outras formas de parcerias, como estágios, convênios e termos de cooperação, se for o caso.

Concomitantemente às definições e implementações em relação aos perfis e autorizações de acessos aos sistemas e informações de Ouvidoria, devem ser realizadas orientações constantes, promovidas capacitações periódicas e incentivado o estudo e a participação de cursos

e demais eventos voltados à Ouvidoria, à proteção de dados pessoas e à ética profissional.

Risco: Impossibilidade, via sistema informatizado, de verificação e autenticação da titularidade do usuário do serviço de Ouvidoria.

Para o exercício dos direitos previstos na LGPD, por meio das Ouvidorias Públicas, se faz necessário não apenas a identificação do titular do dado pessoal, como também a sua verificação e autenticação.

Isso se faz necessário para, entre outros, mitigar o risco de, equivocadamente, fornecer dados pessoais de um cidadão para outrem.

Boa prática: Implantar funcionalidade no sistema informatizado de Ouvidoria que permita a verificação e autenticidade da titularidade do usuário do serviço de Ouvidoria.

Para que o titular possa exercer os direitos de que trata a LGPD por meio eletrônico, sem que precise, necessariamente, direcionar-se presencialmente a um ponto de atendimento, para identificação, os sistemas de ouvidoria devem contar com ferramenta que permita essa verificação e autenticação com segurança.

A verificação da autenticidade da identidade do titular contribui para a segurança e efetividade do processo de atendimento às manifestações registradas para o exercício dos direitos previstos na LGPD, em seus incisos III, IV e VI do art. 18 e o caput do art. 20.

Neste contexto, as Ouvidorias que utilizam o FalaBR, e atendam ao requisito de verificação do cadastro do usuário pela validação do selo Gov. BR já atendem a este requisito e, aquelas que possuam sistema próprio e específico, podem considerar a utilização do login único do Governo Federal – o gov.br -, disponibilizado gratuitamente a Estados e Municípios.

A Conta gov.br é um meio de acesso digital do usuário aos serviços públicos digitais que garante a identificação de cada cidadão que acessa os serviços digitais do governo federal. Por meio de processo simples de adesão, junto ao Ministério da Economia, é possível utilizar a funcionalidade no sistema informatizado de Ouvidoria já em uso.

Para aquelas Ouvidorias que optem por utilizar o gov.br em seus sistemas informatizados, uma recomendação importante é que escolham, entre os níveis de autenticação bronze, prata e ouro disponíveis, o Nível Verificado – Prata ou Nível Comprovado Ouro

O procedimento para solicitação de integração ao gov.br inicia-se com o encaminhamento de e-mail ao endereço atendimentogovbr@economia.gov.br.

ATENÇÃO!

Nos casos de Ouvidorias que utilizem outro mecanismo eletrônico de verificação, lembramos que, nos termos do art. 28 da Lei 14.129/2021, o Cadastro de Pessoas Físicas (CPF) e o Cadastro Nacional da Pessoa Jurídica (CNPJ) são os números suficientes para identificação do cidadão ou da pessoa jurídica. Assim, esses devem ser os únicos números de identificação solicitados na etapa de acolhimento e registro, bem como nos cadastros dos sistemas informatizados de Ouvidoria, se houver.

Não obstante a aplicação da Lei aos Estados, Distrito Federal e Municípios depender de regulamentação em atos normativos próprios, é recomendável que sejam seguidos os mesmos parâmetros, de forma a garantir maior uniformidade de atendimento aos usuários dos serviços públicos, de maneira geral.

Nos atendimentos presenciais, é importante que essa verificação de titularidade seja realizada pelo atendente autorizado, por meio da apresentação de documento oficial. Uma boa prática, nos atendimentos presenciais, é a elaboração e aplicação de *check list* ou roteiro, com o intuito de garantir que essa verificação seja realizada.

Enquanto não implantada funcionalidade que permita a verificação e autenticação eletrônica, recomenda-se às Ouvidorias que só respondam a pedidos de que tratam incisos III, IV e VI do art. 18 e o caput do art. 20 da LGPD mediante atendimento presencial, no qual a verificação poderá ser realizada por atendente autorizado. Contudo, importante ficar claro que essa deve ser uma medida provisória, devendo ser providenciada a adequação do sistema informatizado em uso com a maior brevidade possível.

Etapa Tramitação

A tramitação é a movimentação de documentos ou processo, tanto interno ou externamente na entidade. No caso específico da Ouvidoria, a tramitação está associada à fase de condução das manifestações recepcionadas junto às unidades técnicas com vistas a apurar e tomar providências em relação às manifestações registradas.

Neste sentido, algumas boas práticas podem ser implementadas a fim de mitigar os riscos relacionados a esta etapa, a exemplo da rotina de conferência e revisão dos dados coletados antes de proceder à tramitação da manifestação para a área responsável, bem como as seguintes:

a) No caso da necessidade de esclarecimentos adicionais, demandado pelo responsável pela informação no órgão ou do acréscimo de dados pelo titular, após etapa de acolhimento e registro pela ouvidoria, deverá ser observado o princípio da necessidade, devendo ser coletados apenas os dados pessoais estritamente necessários para o atendimento da demanda. Nesse sentido, nas situações em que o gestor da área solicitar dados pessoais do titular adicionais para análise da demanda, a Ouvidoria deverá solicitar a justificativa com o intuito de resguardar os princípios da necessidade, adequação e finalidade do tratamento de dados e a proteção do usuário, nos termos do Código de Defesa dos Usuários de Serviços Públicos;

b) Além da solicitação de justificativa pelo gestor para coleta adicional de dados na etapa de tramitação, também é uma boa prática questioná-lo se o dado ora necessário já não está disponível no órgão em algum outro banco de dados e

c) Nos sistemas de tramitação de manifestações orienta-se que seja apresentado aos servidores e colaboradores da Ouvidoria um campo específico, para preenchimento da finalidade a que se propõe a utilização dos dados coletados, a fim de reforçar a cultura do não aproveitamento dos dados para finalidade incompatível.

Desse ponto em diante, apresentam-se boas práticas especificamente relacionadas a riscos identificados na etapa de tramitação de manifestações de Ouvidoria.

Risco: Utilização dos dados coletados para finalidade incompatível.

Este risco pode ocorrer pelo desconhecimento do servidor ou colaborador da Política de Privacidade do órgão, onde devem constar as possíveis formas de utilização dos dados pessoais coletados.

Boa prática: Divulgar amplamente a Política de Privacidade no órgão e comunicar ao titular de dados pessoais alterações no Termo de Uso, quando houver.

A Política de Privacidade é um documento que deve esclarecer como todo o órgão, inclusive a Ouvidoria, lida com as informações coletadas de seus usuários, limitando as ações dos servidores públicos e colaboradores no uso desses dados.

Desta forma, além de devidamente instituída, é essencial que haja ampla disseminação interna da Política de Privacidade e ações contínuas de capacitação, bem como exista procedimento formal de apuração de conduta irregular de servidores e colaboradores, no caso específico, relacionado a uso de dados pessoais de maneira incompatível com aquela definida na Política de Privacidade do órgão.

Importante, também, observar que quaisquer alterações no Termo de Uso e na Política de Privacidade precisam ser comunicadas aos usuários da Ouvidoria. O envio de e-mails e a divulgação no sítio eletrônico oficial da Ouvidoria são exemplos de como pode se dar essa comunicação.

Risco: Modificação indevida dos dados realizada por servidor ou colaborador da Ouvidoria ou por erro do sistema informatizado de ouvidoria

Dentre as operações de tratamento, entende-se como modificação o ato ou efeito de alteração do dado, sendo, inclusive, direito assegurado ao titular, previsto no inciso III, art. 18 da LGPD, a correção de dados incompletos, inexatos ou desatualizados.

Todavia, a modificação deve ocorrer mediante provocação do titular ou se verificada incongruência com outra base, por exemplo, e não, deliberadamente, por servidor ou colaborador da Ouvidoria.

Outra causa possível para a ocorrência deste risco é a modificação decorrente de erro do servidor ou colaborador da Ouvidoria ou, ainda, por erro do sistema informatizado de ouvidoria.

Boa Prática: Definir bloqueios no sistema a fim de evitar modificações indevidas dos dados e dispor de registro de logs no sistema informatizado de Ouvidoria.

Para evitar a modificação indevida de dados pessoais, comprometendo sua integridade, é desejável que o sistema informatizado de Ouvidoria possua bloqueios que impeçam essa operação, sendo permitida, apenas, a alguns perfis de usuários do sistema, que possuam maiores permissões e que poderão realizar essa operação, exclusivamente, mediante solicitação do titular de dados pessoais ou se forem detectadas inconsistências a partir de outras bases.

Em adição, é necessário que os sistemas possuam registro de logs, que corresponde aos registros de atividades que um usuário realiza dentro do sistema. Eles, geralmente, estão registrados de forma cronológica por data e hora e é possível monitorar as atividades que são realizadas no sistema, sendo muito úteis em verificações futuras. Além disso, há a possibilidade de saber quem acessou o sistema na data e hora, quem realizou alterações de registro e o que foi alterado. Também pode ajudar a identificar quando um sistema está sendo atacado por hackers, pois há como registrar falhas de autenticação e identificar de qual endereço de IP está sendo acessado.

Os arquivos de *logs* devem ser protegidos com total segurança para que não haja alterações em suas informações. Como boa prática, um arquivo de registro de *logs* deve conter as seguintes informações:

- Datas e hora de entrada e saída do sistema;
- Identificação dos usuários;
- Em caso de Sistemas Web, devem ser armazenados o IP de acesso;
- Registros das tentativas de acesso (aceitas e rejeitadas) ao sistema e
- Informações que foram incluídas, alteradas e excluídas.

Ainda, é importante que os *logs* sejam monitorados e revisados com frequência, principalmente para evitar possíveis ataques de hackers e corrigir possíveis falhas de segurança que o sistema possa ter. O registro de *logs*, geralmente, não fica visível aos usuários do sistema, até mesmo por questões de privacidade das informações que são registradas e, dependendo do tamanho do *log*, pode se tornar inviável carregar as informações para a tela do usuário. Entretanto, o setor de tecnologia da informação deve ter acessos a essas informações e monitorar, constantemente, possíveis falhas de segurança.

Além disso, os registros de *logs* também devem ser feitos nos servidores de tecnologia da informação que estão hospedados nos sistemas para fins de acompanhamento de realização de backup ou outras alterações de infraestrutura que possam ocorrer.

Em síntese, os *logs* são informações fundamentais que a área de tecnologia da informação deve manter com total segurança, seja para verificar possíveis invasões dentro do sistema ou servidor de tecnologia da informação e comunicação (TIC), como para verificar quem realizou uma determinada alteração nas informações contidas no sistema.

Identificado o servidor ou colaborador de Ouvidoria que deu causa à modificação indevida de dados pessoais, deve ser dado conhecimento à área de apuração para tomada de providências necessárias à devida apuração do ocorrido.

Diferentemente, para evitar modificação de dados por força de erro do sistema informatizado, se faz necessária a manutenção de uma boa governança de tecnologia da informação, que tem papel essencial para a Ouvidoria digital. Assim, possuir documentação de sistemas, infraestrutura e banco de dados ajuda, sobremaneira, a evitar erros que possam ocorrer durante os processos.

Ainda, para garantir a integridade dos dados é preciso que a organização possua logs de alterações de backup, pois caso seja necessária a restauração de algum backup, é importante que não afete nenhuma solicitação já realizada pela ouvidoria.

Risco: Perda dos dados por falha na infraestrutura de tecnologia da informação.

Este risco se refere à falha ou indisponibilidade do sistema informatizado que acarrete a eliminação indevida de dados armazenados.

Boa Prática: Buscar, junto à área de tecnologia da informação, a disponibilidade de infraestrutura adequada para suporte ao funcionamento do sistema informatizado de Ouvidoria e ao banco de dados.

Para garantir a segurança dos dados armazenados no sistema informatizado em uso pela Ouvidoria, é necessário, além do atendimento aos requisitos constantes na Política de Segurança da Informação, que ele seja acompanhado por equipe especializada que garanta sua manutenção.

Nesse contexto, não apenas o sistema, como toda a infraestrutura de tecnologia que dá suporte ao seu funcionamento, deve ser garantida pelo órgão ao qual a Ouvidoria está vinculada.

A infraestrutura de tecnologia consiste em um conjunto de componentes necessários para a operação e gerenciamento de serviços de tecnologia que são, além do *software*, as máquinas e equipamentos utilizados, o gerenciamento de dados e serviço e as redes.

Para tanto, são necessários investimentos em pessoal, sistemas e equipamentos e, para tanto, deverá o gestor máximo do órgão compreender a importância do tema, e envidar esforços no sentido de prover a infraestrutura adequada.

Risco: Perda dos dados por extravio de documentos em papel.

Este risco se refere especificamente ao extravio de documentos da Ouvidoria que constem em pastas ou papel, como exemplo, formulários de manifestação preenchidos, relatórios de manifestação impressos a partir do sistema informatizado e relatórios gerenciais de ouvidoria que estejam em meio físico.

Boa Prática Convém implantar controles e definir o perímetro de segurança para proteção das áreas onde estejam os documentos em papel.

De acordo com a ISO 27002, convém que as informações que constem em papel sejam guardadas em lugar seguro, como cofres ou arquivos trancáveis, especialmente, quando o ambiente estiver trancado ou desocupado, ou seja, fora do horário de funcionamento da Ouvidoria.

Importante, ainda, para proteção do ambiente físico, que portas e janelas sejam trancadas quando estiverem sem um servidor da equipe de Ouvidoria no ambiente, bem como haja proteção externa nessas janelas, especialmente, quando a sala da Ouvidoria fica localizada no térreo.

Ainda nesse contexto, importante que o ambiente físico contenha proteção contra incêndio, como portas corta-fogo e inundações.

Por fim, importante observar, quando do uso de impressoras a autorização de uso, bem como a retirada imediata de documentos que contenham informações pessoais desses equipamentos.

Risco: Vazamento de dados por pessoa com acesso autorizado, de forma deliberada ou não.

O vazamento, neste contexto, consiste em pessoa autorizada acessar os dados de ouvidoria e/ou dar acesso, de forma deliberada ou não, a terceiro não autorizado.

Boas práticas: Manter ações de capacitação e orientação constantes, disseminação do Código de Ética aplicável e fomento à Política Correicional.

De maneira análoga à modificação de dados por servidor ou colaborador da Ouvidoria, de maneira deliberada ou não, no caso de identificado o vazamento de dados pessoais, deverá ser dado conhecimento do fato à área de tratamento de incidentes de TIC e à área de apuração. Além disso, o fato deverá ser comunicado aos titulares, de acordo com as disposições da ANPD, bem como será necessária a elaboração do já mencionado Plano de Resposta a Incidentes de Segurança.

Para coibir conduta irregular do servidor da Ouvidoria, bem como dos gestores que respondem às manifestações e pedidos de acesso à informação que contenham dados pessoais existentes, apresenta-se como uma boa prática o fomento à Política Correicional, nos termos da

legislação aplicável ao ente federativo, que preveja as sanções àquele que utilize o dado com finalidade inapropriada.

Uma vez existente a política e definidos os procedimentos, ao ser detectado indício de conduta irregular do servidor, devem-se adotar medidas urgentes de comunicação ao órgão correicionais, para que sejam adotadas as medidas cabíveis.

No caso de a conduta irregular ser cometida por colaborador de Ouvidoria, que nela atua sob formalização de contrato administrativo, deverão ser aplicadas as sanções previstas no termo contratual.

Neste contexto, é importante que haja o alinhamento da Ouvidoria com o Programa de Integridade do órgão ao qual está vinculada, se já instituído e a proposição de medidas capazes de mitigar os riscos associados às suas atividades.

Poderá a Ouvidoria, ainda, contribuir com a criação de indicadores capazes de demonstrar os ajustes necessários à prevenção, detecção e apuração de condutas inadequadas no âmbito do órgão.

Em por fim, Para coibir desvios de condutas, apresenta-se como uma boa prática a atuação preventiva com ações de capacitação e orientação constantes e disseminação do Código de Ética aplicável.

Risco: Vazamento de dados decorrente do registro e tramitação de manifestações em meio físico ou por e-mail, nos quais não é possível o rastreamento de quem teve acesso.

Este risco está sendo aqui abordado no contexto da tramitação física (em papel) ou eletrônica, especificamente, por meio de e-mail, de manifestações, sendo essas situações em que não existem meios de controle efetivo de quais servidores e colaboradores, ou até mesmo terceiros, tiveram acesso àquelas informações.

Boa prática: Dar preferência ao registro e tramitação de manifestações por sistema informatizado, a exemplo do Fala.BR, disponibilizado gratuitamente pela Ouvidoria-Geral da União.

Num contexto de crescente digitalização de serviços públicos, a Ouvidoria é impulsionada a se adequar a esta realidade, não apenas pela

ampliação do acesso ao serviço, como também, considerando os requisitos de proteção de dados pessoais, de observância obrigatória, previstos na LAI e, mais recentemente, na LGPD.

Nesse sentido, consiste em boa prática dispor de sistema informatizado para registro, tramitação e conclusão de manifestações, utilizando-se de documentos em meio físico ou o uso do correio eletrônico apenas de maneira residual ou excepcional.

O Fala.BR é a plataforma integrada de ouvidoria e acesso à informação do Poder Executivo Federal, desenvolvido pela Controladoria-Geral da União (CGU), que permite a qualquer cidadão encaminhar manifestações e pedidos de acesso à informação pela mesma ferramenta.

Qualquer Estado ou Município pode utilizar a plataforma gratuitamente, devendo, para tanto, fazer a adesão à Rede Nacional de Ouvidorias e ao sistema Fala.Br propriamente dito.

Conforme orientações da Ouvidoria-Geral da União (OGU), para adesão é necessário o preenchimento e envio de Termo de Adesão Eletrônico constante no site www.gov.br/ouvidorias.

Etapa Conclusão ou Resposta

A etapa de conclusão ou resposta consiste no momento do fluxo da manifestação, em que a área ou gestor responsável pelo processo, serviço ou informação, encaminha a resposta da manifestação à Ouvidoria, a qual, por sua vez, deverá analisá-la.

Nesta análise, que deve anteceder o encaminhamento ao usuário, a Ouvidoria pode propor complementações ou alterações na resposta, inclusive, para garantir a sua compreensão pelo usuário.

Importante observar alguns riscos potenciais que podem ocorrer nesta etapa e, a critério de cada Ouvidoria, realizar ações que visem a mitigá-los, como as boas práticas dispostas a seguir:

Risco: Acesso a titular de dado a dado pessoal de outrem.

Na etapa de acolhimento e registro é possível, observados os princípios da finalidade e necessidade, que tenha havido a coleta de dados

pessoais do usuário do serviço de Ouvidoria. Da mesma forma, existe a possibilidade de, na resposta do gestor, conter outros dados pessoais, os quais são encaminhados ao titular como parte das providências adotadas.

Neste contexto, o risco ora apresentado consiste em encaminhar a resposta da manifestação que contenha dados pessoais a terceiros, e não ao titular dos dados.

Boa prática: Realizar conferência dos dados pessoais contidos na resposta do gestor antes de encaminhar resposta ao manifestante.

No recebimento da resposta do encarregado ou área competente com dados pessoais, o ouvidor deverá observar se os dados correspondem ao titular que ingressou com a demanda e, em negativo, retornar a demanda para o encarregado ou área competente para análise e correção.

A resposta final deve ser emitida sempre ao titular dos dados pessoais constantes na inicial. O cuidado do ouvidor, ao realizar a análise final antes de encaminhar a resposta ao demandante, deverá realizar um check-list básico, confirmando os dados pessoais entre outras informações coletadas na inicial, para assegurar que está encaminhando a resposta ao real titular dos dados pessoais. Em caso de conflito de dados, deve-se reportar ao setor que elaborou a resposta para que possa reavaliar o documento e realizar as correções necessárias.

Importante reforçar que a existência de dados pessoais não pode ser argumento para a negativa do pedido de acesso à informação, reiterando o argumento do início do Guia de harmonia entre LAI e LGPD.

Risco: Ausência de informações estruturadas que permitam a tomada de decisão pelo Controlador quanto às manifestações apresentadas pelos titulares de dados pessoais.

Em qualquer ação, processo ou projeto, a informação correta é essencial para que os gestores consigam decidir da melhor forma. Nesse contexto, este risco consiste na ausência das informações e conhecimentos necessários para a tomada de decisão do controlador quanto ao requerimento do titular do exercício de direitos de que tratam a LGPD.

Boa prática: Criar Unidade de Governança para Proteção de Dados Pessoais para subsidiar a tomada de decisão pelo controlador.

Para tomada de decisão, no que concerne à proteção de dados pessoais, são necessárias informações relacionadas, entre outros, à própria Lei Geral de Proteção de Dados (LGPD), Lei de Acesso à Informação (LAI), Lei de Defesa dos Usuários de Serviços Públicos, Marco Civil da Internet, gestão de riscos e processos.

Quanto à segurança da informação, são informações relevantes para a tomada de decisão as boas práticas produzidas pela International Organization for Standardization (ISO), em especial, as ISO 31000, 31010, 27001, 27002, 27004, 27005, 27701, 29100.

Neste contexto, considerando a multidisciplinaridade dos conhecimentos e informações necessárias, é interessante que o órgão disponha de Comitê de Proteção de Dados Pessoais ou colegiado análogo, não apenas para coordenar e orientar a implementação das ações necessárias à adequação à LGPD, como já mencionado neste Guia, mas também para assessorar o controlador e o encarregado na tomada de decisão em relação às manifestações dos titulares de dados.

É aconselhável, ainda, que a composição do referido comitê contemple pessoas envolvidas na governança de dados mais ampla da instituição, para que as decisões a respeito de dados pessoais estejam em consonância com outras medidas relativas à gestão de dados de forma geral.

Etapa Emissão de Relatórios

Uma das atribuições precípuas da Ouvidoria, realizada de maneira concomitante com os processos de atendimento, é a proposição de correção e melhorias nos serviços e políticas públicas, que se dá, em geral, por meio da produção de informações estratégicas e emissão de relatórios gerenciais.

O Modelo de Maturidade em Ouvidoria Pública (MMOuP), desenvolvido pela Controladoria-Geral da União, com consultoria do Programa da União Europeia para Coesão Social na América Latina (EUROsociAL), atribui nível otimizado no objetivo gestão estratégica de informações, às ouvidorias que realizam *"(...) análises quantitativas e qualitativas dos dados coletados, segundo metodologia científica*

transparente e validada e por meio de parâmetros definidos em conjunto por ela e pelos gestores responsáveis pela tomada de decisão".

Além disso, o modelo considera estar no nível máximo de maturidade no elemento *"produção de informações estratégicas"*, as ouvidorias que *"além do encaminhamento dos processos de manifestações de ouvidoria, a unidade produz anualmente o Relatório de Gestão de que tratam os artigos 14 e 15 da Lei 13.460, de 2017, e instituiu rotinas de comunicação aos gestores dos serviços, periodicamente ou em decorrência de eventos concretos por ela identificados. Adicionalmente, dados quantitativos relacionados às avaliações de serviços e manifestações são disponibilizados automaticamente aos gestores por meio de painéis gerenciais".*

Em adição, independentemente do processo regular de análise dos dados, sempre que uma informação considerada estratégica para o órgão é levada ao conhecimento da ouvidoria por meio de uma manifestação ou por outras formas, deverá a ouvidoria realizar a análise de maneira sistêmica, considerando, inclusive, dados de outros processos ou sistemas, externos à ouvidoria e registrá-la em relatório temático, que deverá ser encaminhado tempestivamente aos gestores, para tomada de decisão.

Nesse contexto, a temática da proteção de dados pessoais, com o advento da LGPD, passa formalmente a integrar os temas que poderão ser apresentados à ouvidoria pelos seus usuários ou, conforme denomina a Lei, pelos titulares de dados pessoais. Assim, como ocorre com os demais temas a ela apresentados, espera-se da ouvidoria a proposição de aprimoramento dos serviços e das políticas públicas voltadas à proteção dos dados pessoais a partir da análise das manifestações registradas na Ouvidoria.

Como nas demais etapas do fluxo da Ouvidoria, alguns riscos relacionados à proteção de dados são identificados na etapa de emissão de relatórios, e algumas medidas poderão ser implementadas, com o fim de mitigá-los, como as que serão tratadas a seguir.

Risco: Na avaliação dos dados para produção de análises estatísticas e relatórios gerenciais, dispor de dados pessoais em documentos preparatórios ou versões internas do documento.

O acesso aos dados pessoais dos usuários da Ouvidoria armazenados no sistema informatizado de ouvidoria deve ser controlado pela infraestrutura de segurança da informação, como permissões de acesso.

Aqueles que acessam os dados para realização de avaliações, análises e emissões de relatórios gerenciais e estatísticos devem zelar pela confidencialidade dos dados e a privacidade dos usuários não apenas no produto final daquele trabalho, onde constem os dados, como também em toda documentação preparatória emitida ou consultada.

Como exemplo desta documentação preparatória, é possível citar planilhas com dados das manifestações, documentos em rascunho ou versões anteriores antes da finalização.

Boa prática: Garantir que o armazenamento de arquivos de Ouvidoria obedeça a Política de Segurança da Informação do órgão.

A Política de Segurança da Informação reúne as sistemáticas e procedimentos de segurança da informação aplicáveis no âmbito do órgão público, para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e informações tratadas, além de visar garantir a consistência, a privacidade e a confiabilidade dos dados e informações.

Exemplo prático de procedimento de segurança que poderá constar na Política para mitigar o risco analisado é limitar os modelos de extração de dados gerenciais do sistema a fim de que os campos de qualificação não sejam exportáveis.

Nesse contexto, poderão as Ouvidorias fomentar e contribuir com a instituição de Política de Segurança da Informação, no âmbito dos órgãos aos quais estão vinculadas e, ainda, naqueles em que já tenha havido a referida instituição, que nela estejam contempladas questões específicas relacionadas ao tratamento de dados pessoais, conforme diretrizes da LGPD.

Constarão nesta Política os requisitos de segurança para o armazenamento de documentos, entre eles, aqueles utilizados em Ouvidoria, como planilhas e relatórios de manifestações, bem como os tópicos a seguir:

a) Procedimentos de prevenção e detecção de vírus;

b) Gestão de riscos;

c) Classificação das informações como confidencial, restrito ostensivo;

d) Políticas de acesso aos sistemas;

e) Plano de treinamento de segurança da informação;

f) Plano de Respostas a Incidentes de Segurança;

g) Padrões mínimos de qualidade e

h) Consequências de violações de dados.

Boa prática: Garantir que o princípio da necessidade norteie todas as ações da Ouvidoria, inclusive a realização de análises estatísticas e produção de relatórios gerenciais.

É importante que o princípio da necessidade norteie todas as ações da Ouvidoria, inclusive a produção de análises estatísticas e relatórios gerenciais, nas quais devem constar, mesmo em documentos preparatórios ou versões internas do documento, exclusivamente, os dados necessários à análise a ser realizada.

Risco: Na emissão de relatórios gerenciais e estatísticos, equivocadamente, divulgar dados pessoais.

A divulgação de dados pessoais em relatórios elaborados pela ouvidoria só será possível se atender aos princípios da finalidade, adequação e necessidade. Caso ocorra qualquer divulgação, sem a observância desses, ensejará não apenas o descumprimento da Lei e responsabilização do agente que deu causa, como também a perda da credibilidade da ouvidoria perante seu usuário.

Boa prática: Sistema informatizado de ouvidoria dispor de funcionalidade que permita a pseudonimização dos dados em consonância com a finalidade de tratamento

Com a utilização da técnica de pseudonimização, o dado perde a

possibilidade de associação, direta ou indireta, a um indivíduo. Do ponto de vista da segurança da informação, essa técnica visa a contribuir para haver uma maior segurança dos dados, diminuindo os possíveis danos causados por um vazamento.

No contexto da Ouvidoria, é importante que o sistema informatizado utilizado possua esta funcionalidade a ser aplicada aos dados pessoais excessivos e desnecessários, visando a proteção no caso das manifestações do tipo denúncias, conforme Resolução nº 3, de 13 de Setembro de 2019 da Rede Nacional de Ouvidorias, que estabelece a Norma Modelo sobre Medidas Gerais de Salvaguarda à Identidade de Denunciantes, sem prejuízo de ampliação para outras tipologias, de acordo com a especificidade da Ouvidoria.

O sistema Fala.BR, já apresentado neste Guia, realiza o processo de pseudonimização de denúncias e informações sobre sua operacionalização estão disponíveis no Manual do sistema disponibilizado na Wiki da CGU.

Além disso, em âmbito federal, Portaria CGU nº 581, de 09 de março de 2021, que estabelece orientações para o exercício das competências das unidades do Sistema de Ouvidoria do Poder Executivo federal, entre outros, dispõe sobre o processo de pseudononimização de denúncias, especificamente, em seus artigos 34 e 35.

Esta Portaria estabelece como elementos de identificação, no mínimo, dados cadastrais, atributos genéticos, atributos biométricos e dados biográficos e, como meios de pseudonimização a serem adotados, dentre outros, produção de extrato, produção de versão tarjada e redução a termo de gravação ou relato descritivo de imagem.

Boa prática: Realizar conferência dos relatórios gerenciais, por superior ou par, a fim de garantir que não haja divulgação de dados pessoais sem observância dos princípios da finalidade, adequação e necessidade.

Ao emitir um relatório ou documento gerencial em Ouvidoria, é necessário analisar, cuidadosamente, se o dado pessoal ali contido é necessário para a análise e providência em relação à demanda apresentada. Caso contrário, os dados não devem constar no relatório ou documento.

É possível exemplificar, com a situação comumente apresentada à Ouvidoria, na qual, o número do CPF do titular consta na demanda, porém, não é necessário para seu atendimento. Neste caso, poderá ser aplicada técnica para mascarar os dados, da seguinte forma: ***000. ***-**.

No caso de relatórios gerados automaticamente nos sistemas informatizados de Ouvidoria, uma vez que eles correspondem a uma extração dos dados cadastrados no próprio sistema, faz-se necessário que o procedimento de pseudonimização, quando aplicável, ocorra de maneira adequada nas etapas iniciais do fluxo de Ouvidoria para que, na etapa final de emissão de relatórios, não haja divulgação equivocada de dados pessoais cadastrados.

Importante, ainda, com o advento da LGPD, que os relatórios comumente emitidos sejam revisados, com o intuito de identificar a divulgação indevida de dados pessoais.

É possível, também, que os relatórios de ouvidoria sejam gerados em ferramentas de edição de textos como Microsoft Word ou LibreOffice Writer, a partir de consultas aos sistemas de ouvidoria, o que pode aumentar, sobremaneira, o risco da divulgação indevida de dados pessoais. Formas de mitigar esse risco são a inclusão de etapas revisionais, por superior hierárquico ou um par, bem como estabelecimento de modelo padrão de relatórios, sempre que possível.

11.3. Boas práticas relacionadas ao compartilhamento de dados entre Ouvidorias

Pela relevância do tema às Ouvidorias, esta última seção do capítulo de Boas Práticas aplicadas à Ouvidoria para atendimento à LGPD deste Guia destina-se a tratar do risco associado ao compartilhamento de dados pessoais entre Ouvidorias e da boa prática que poderá ser implementada para que esse processo ocorra conforme diretrizes da LGPD.

Risco: Compartilhamento de dados pessoais sem informar ao titular de dados essa finalidade.

Este risco tem semelhança com a utilização dos dados coletados para finalidade não informada ao titular, tratado na etapa tramitação, todavia, nessa seção é apresentado na perspectiva do compartilhamento de dados pessoais entre Ouvidorias.

Boas Práticas: Solicitar consentimento do titular para o compartilhamento de dados entre Ouvidorias

Não obstante o consentimento não ser a base legal apropriada para o tratamento de dados pessoais pela Ouvidoria, ele se faz necessário no compartilhamento de dados de uma Ouvidoria para outra.

Essa cautela presta-se não apenas à proteção dos dados pessoas, mas também à proteção ao denunciante, conforme disposto nos parágrafos §§ 5º e 6º da Resolução nº 03/2019 da Rede Nacional de Ouvidorias, que estabelecem que *"o encaminhamento de denúncias com elementos de identificação entre unidades de ouvidoria deverá ser precedido do consentimento do denunciante"* e *"na negativa ou ausência de consentimento, a unidade que tenha recebido originalmente a denúncia somente poderá encaminhá-la ou compartilhá-la após a sua pseudonimização"*, respectivamente.

Boas Práticas: Formalizar parceria entre Ouvidorias para compartilhamento de dados pessoais e comunicar ao titular de dados no Termo de Uso.

É bem comum em Ouvidoria o recebimento de manifestações de competência de outro órgão público. Nessa situação e, com o intuito de tornar mais fácil para o usuário da Ouvidoria chegar naquele órgão que, de fato, poderá tomar alguma providência em relação à demanda que ele apresenta, muitas Ouvidorias faziam o encaminhamento da manifestação à Ouvidoria do órgão competente, comunicando ao usuário.

Todavia, alguns cuidados precisam ser tomados para realização desse procedimento. Nos termos da Lei, esse encaminhamento entre

Ouvidorias corresponde ao compartilhamento de dados pessoais entre controladores, uma vez que cada órgão corresponde a um controlador distinto.

Nesse sentido, a ANPD destina capítulo específico no Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, denominado "Compartilhamento de Dados Pessoais pelo Poder Público", detalhando os principais requisitos que devem ser observados nesses processos de compartilhamento.

Em breve síntese, numa interpretação trazida para o contexto das Ouvidorias Públicas, recomenda-se que esse encaminhamento de manifestações para outras Ouvidorias e, consequentemente, outros controladores, só seja realizada se houver ato formal firmado entre as partes, a exemplo de contratos, convênios ou instrumentos congêneres.

Da mesma forma, é possível que decreto regulamentador que estabeleça um sistema já traga essa previsão, bem como acordos por adesão, como o da Rede Nacional de Ouvidorias (Renouv), também são suficientes para esta finalidade.

Outra possibilidade prevista pela ANPD no referido Guia é *"a expedição de decisão administrativa pela autoridade competente, que autorize o acesso aos dados e estabeleça os requisitos definidos como condição para o compartilhamento".*

Importante pontuar, ainda, que uma vez formalizado ato ou expedida a decisão administrativa de compartilhamento de dados pessoais, essa finalidade deve ser informada ao titular de dados pessoais, no Termo de Uso do sistema informatizado de Ouvidoria. Recomenda-se, ainda, que haja transparência ativa dos Termos de Uso e dos casos de compartilhamento de dados com outras instituições.

Assim, caso não haja o ato formal ou a expedição de decisão administrativa nesse sentido, nem o consentimento do titular, recomenda-se que as Ouvidorias não compartilhem manifestações umas com as outras, notadamente, aquelas que contenham dados pessoais. Nessas situações, é uma boa prática que a Ouvidoria conclua a manifestação,

orientando o usuário qual órgão público é competente para responder a sua demanda, informando, inclusive, os canais de acesso à Ouvidoria daquele órgão, se houver.

Para maior detalhamento sobre os requisitos para o compartilhamento de dados pessoais pelo Poder Público, recomenda-se a leitura do Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, da ANPD.

Por fim, é importante destacar que no caso de proteção ao denunciante, são aplicadas proteções adicionais decorrentes dos regimes das Leis nº 13.460/2017 e nº 13.608, de 10 de janeiro de 2018, que dispõe sobre o serviço telefônico de recebimento de denúncias e sobre recompensa por informações que auxiliem nas investigações policiais; e altera o art. 4º da Lei nº 10.201, de 14 de fevereiro de 2001, para prover recursos do Fundo Nacional de Segurança Pública para esses fins, conforme pode ser observada na regulamentação federal, - Decreto nº 10.153/2019 - e na Norma Modelo sobre Medidas Gerais de Salvaguarda à Identidade de Denunciantes da Rede Nacional de Ouvidorias, aprovada pela Resolução nº 03/2019.

12. CONSIDERAÇÕES FINAIS

O presente Guia de Boas Práticas foi elaborado com o objetivo de apoiar as Ouvidorias Públicas na aplicação da Lei Geral de Proteção de Dados Pessoais, apresentando conceitos da Lei, bem como orientações contidas nos guias produzidos pela ANPD e pelo Comitê Central de Governança de Dados do Poder Executivo Federal, aplicadas ao contexto de atuação das Ouvidorias Públicas.

Este Guia traz, inicialmente, uma importante contextualização das Ouvidorias Públicas e o advento da Lei Geral de Proteção de Dados Pessoais e as Ouvidorias digitais. Em seguida, discorre sobre conceitos da própria LGPD e outros conceitos relevantes correlacionados à Ouvidoria para então tratar das possíveis implicações da Lei na sua atuação.

O Guia também esclarece a base legal para tratamento de dados pessoais pelas Ouvidorias Públicas, aborda os direitos dos titulares de dados pessoais e traz orientações sobre os agentes de tratamento. Por oportuno, este material trata também da relação entre a LAI e a LGPD e a importância de a Ouvidoria conhecer os riscos relevantes relacionados às suas atividades.

E após todo este conteúdo, o Guia apresenta, em termos práticos e objetivos, um passo a passo inicial para adequação das Ouvidorias à LGPD e um rol de riscos e respectivas boas práticas que visam mitiga-los. Estas boas práticas estão divididas em três partes, sendo elas aquelas relacionadas ao acesso não autorizado aos sistemas e documentos da Ouvidoria, às etapas do fluxo de manifestações de Ouvidoria e ao compartilhamento de dados entre Ouvidorias.

Por fim, cabe ressaltar que este é um documento da Rede Nacional de Ouvidoria desenvolvido por Ouvidorias Públicas para Ouvidorias Públicas, que deverá estar em constante atualização e aperfeiçoamento a partir da contribuição de todas as Ouvidorias integrantes da Rede.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas. NBR ISO/IEC 31000:2018. Gestão de riscos – Diretrizes. Rio de Janeiro. 2018.

Associação Brasileira de Normas Técnicas. NBR 27002:2013. Tecnologia da informação - Técnicas de segurança - Código de Prática para controles de segurança da informação. Rio de Janeiro. 2013.

Artigo LGPD e LAI: uma análise sobre a relação entre elas. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2020/lei-acesso-informacao-lai-lei-geral-protecao-dados-pessoais-lgpd>

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. 1ª ed. Brasília; 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. 1ª ed. Brasília; 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf>

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. 2ª ed. Brasília; 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf>

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público. 1ª ed. Brasília; 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html>

BRASIL. Controladoria-Geral da União. Modelo de Maturidade em Ouvidoria, 2021. Disponível em: <https://www.gov.br/ouvidorias/pt-br/ouvidorias/modelo-de-maturidade-em-ouvidoria-publica>

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal . Guia de Elaboração de Inventário de Dados Pessoais. Lei Geral de Proteção de Dados Pessoais. Versão 1.1 Brasília, abril de 2021. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf>

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal . Guia e template para elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd>

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal. Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais (LGPD). Agosto, 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf>

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal. Guia de Avaliação de Riscos de Segurança e Privacidade - Lei Geral de Proteção de Dados Pessoais. Versão 1.0 Brasília, novembro de 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf>

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal. Guia de Resposta a Incidentes de Segurança. Lei Geral de Proteção de Dados Pessoais (LGPD). Versão 1.0 Brasília, setembro de 2021. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_resposta_incidentes.pdf>

BRASIL. Comitê Central de Governança de Dados do Poder Executivo Federal. Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos. Lei Geral de Proteção de Dados Pessoais (LGPD). Versão 1.2. Brasília, setembro de 2021. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf>

BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). [Internet]. Diário Oficial da União, Brasília; 2017. [citado 2021 dez. 14]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>

BRASIL. Lei nº 13.460, de 26 de junho de 2017. Dispõe sobre a participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm>

BRASIL. Portaria nº 581, de 9 de março de 2021. CGU. Disponível em:<https://www.gov.br/ouvidorias/pt-br/ouvidorias/legislacao/portarias/portaria-no-581-consolidada-v2.pdf>

BRASIL. Resolução nº 7, de 30 de novembro de 2021. Coordenação Geral da Rede Nacional de Ouvidorias. Controladoria-Geral da União. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-n-7-de-30-de-novembro-de-2021-364253953>

BRASIL. Controladoria-Geral da União – CGU. Enunciado n. 4, de 10 de março de 2022. Disponível em: <https://repositorio.cgu.gov.br/handle/1/67735>

BRASIL. Controladoria-Geral da União – CGU. Metodologia de gestão de riscos. Brasília, abril de 2018. Disponível em: <https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf>

COSO – Gerenciamento de riscos corporativos – integrado com estratégia e performance - Sumário Executivo - 2017.

MINAS GERAIS. Controladoria-Geral do Estado. Guia Metodológico da Gestão de Riscos Estratégicos. Minas Gerais, maio de 2020. Disponível em <https://bancodoconhecimento.conaci.org.br/bitstream/123456789/271/1/Guia_Metodologico_de_Gestao_de_Riscos_Estrategicos.pdf>

PERNAMBUCO. Lei nº 16.420, de 17 de setembro de 2018. Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública estadual. Disponível em: <https://legis.alepe.pe.gov.

Supremo Tribunal Federal. ADI nº 6393 MC /DF. Relator: Ministra Rosa Weber. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5896399>

ONU. Resolução 75/186. Disponível em: <https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F75%2F186&Language=S&DeviceType=Mobile>

UNICEF. Declaração Universal das Nações Unidas. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>