em questão
E-ISSN 1808-5245

Lei Geral de Proteção de Dados e a elaboração do Relatório de Impacto à Proteção de Dados Pessoais

Marcelo Minghelli [I]
[I] Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil;
marcelo.minghelli@ufsc.br; https://orcid.org/0000-0002-5964-2441

Bárbara Balbis Garcia [II]
[II] Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil;
babibalbis@gmail.com; https://orcid.org/0000-0003-4530-0974

Mariene Alves do Vale [III]
[III] Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil;
marieneavale@gmail.com; https://orcid.org/0000-0003-2172-5177

Patricia Siqueira Santos [III]
[III] Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil;
patriciasiqueirass@gmail.com; https://orcid.org/0000-0003-3622-3372

Resumo: Está em vigor no Brasil desde 2020 a Lei n. 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados, e a Autoridade Nacional de Proteção de Dados começou a divulgar a lista de processos sancionatórios de empresas e órgãos públicos que aguardam conclusão a partir de março de 2023. Tomando como base esses primeiros processos instaurados pela Coordenação-Geral de Fiscalização, esta pesquisa buscou analisar, sob a ótica da gestão da informação, de que forma as informações de infrações, incidentes e eventuais sanções aplicadas ou aplicáveis disponibilizadas, bem como as principais características jurídicas das Instituições autuadas, poderão contribuir para a elaboração e aperfeiçoamento do Relatório de Impacto à Proteção de Dados Pessoais do Núcleo Telessaúde da Universidade Federal de Santa Catarina. A pesquisa é considerada de abordagem qualitativa e conta com objetivos exploratórios e descritivos. Visa analisar as práticas referentes à Lei no Núcleo Telessaúde e propor melhorias a partir do mapeamento dos processos administrativos sancionatórios instaurados pela Autoridade Nacional, bem como, a partir dela, identificar o perfil dos agentes de tratamento investigados, assim como as principais causas de autuação. Dos nove processos de 2023, três são de instituições da saúde e as condutas apontam falhas na adoção de medidas de segurança administrativas ou de gestão, tais informações contribuem para análises pertinentes ao Telessaúde. O estudo apoia a mudança do fluxograma do Relatório, inserindo etapa de análise de riscos por meio das informações dos processos, perspectiva viável apenas com aplicação de conhecimentos em gestão da informação.

Palavras-chave: Lei Geral de Proteção de Dados; Relatório de Impacto; telessaúde; sanções administrativas

1 Introdução

Sancionada em 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) entrou em vigor no Brasil a partir de agosto de 2020. Em julho de 2019, foi aprovada a criação da Autoridade Nacional de Proteção de Dados (ANPD). Este é o órgão responsável pela elaboração das diretrizes para a Política Nacional de Proteção de Dados Pessoais e de Privacidade e, dentre diversas outras competências, é quem fiscaliza e aplica sanções em casos de tratamentos de dados que foram realizados em descumprimento à legislação, instaurando processos administrativos que assegurem o contraditório, a ampla defesa e o direito de recurso (Autoridade Nacional de Proteção de Dados, 2023b).

Para estarem adequados à legislação, os agentes de tratamento de dados das esferas pública e privada precisam estar em conformidade com o ordenamento jurídico. Nesse sentido, a LGPD elenca uma série de providências que devem ser adotadas, por exemplo, as boas práticas elencadas nos artigos 46 e seguintes. As boas práticas são entendidas como medidas operacionais (tecnologia da informação) ou organizacionais (administrativas) que permitem a correta execução do tratamento de dados, diminuindo significativamente os eventuais riscos aos direitos dos titulares de dados. Entende-se que as medidas operacionais estão relacionadas com riscos ou eventuais incidentes que possam vir a ocorrer durante um processo de tratamento de dados e os métodos e instrumentos de tecnologia da informação a ele aplicados. Já as medidas organizacionais têm relação com eventuais incidentes ou inconsistências na estrutura organizacional e de gestão de uma instituição ou empresa, que possuam potencial de causar eventuais danos aos direitos dos titulares de dados.

A indicação de um encarregado de dados, a elaboração de um Relatório de Impacto e a existência de um protocolo para eventuais incidentes de privacidade são exemplos de boas práticas, cuja ausência pode resultar na aplicação de uma sanção aos agentes de tratamento de dados nos termos do artigo 50 e seguintes da Lei 13.709/2018.

Por meio do seu site, a ANPD divulgou os primeiros processos administrativos sancionatórios instaurados pela Coordenação-Geral de Fiscalização (CGF) em 2023.

Dentre diversas competências listadas no Regimento Interno da ANPD, a CGF é um órgão interno e específico da ANPD, cuja função é fiscalizar e aplicar as sanções necessárias, previstas no artigo 52 da LGPD, por meio de processos administrativos. As divulgações apresentam nove processos de oito instituições, sendo apenas uma empresa privada (Autoridade Nacional de Proteção de Dados, 2023c): Telekall; Ministério da Saúde (dois processos); Instituto de Pesquisas Jardim Botânico do Rio de Janeiro; Secretaria de Educação do Distrito Federal; Secretaria de Estado da Saúde de Santa Catarina; Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo (IAMSPE); Secretaria de Desenvolvimento Social, Criança e Juventude do Estado de Pernambuco; e Instituto Nacional do Seguro Social (INSS).

Por mais recente que seja a atividade de fiscalização, é possível analisar as informações disponibilizadas nos processos administrativos em andamento e os que já foram concluídos. Conforme indicado em seu site, a ANPD criou uma página de acesso público para a divulgação completa desses processos (Autoridade Nacional de Proteção de Dados, 2023c), incluindo documentos dos processos sancionatórios, assim como indicando quais foram as sanções aplicadas em cada um dos casos, para confirmar ou não uma infração.

As atividades de fiscalização e de aplicação de sanções fornecem significativas informações sobre como a ANPD interpreta a LGPD, bem como analisa o tratamento de dados realizado atualmente por instituições públicas e privadas em diferentes setores da sociedade e da economia.

Essas informações são importantes para as atividades de compliance e boas práticas dos agentes de tratamento, servindo de orientação preventiva para o tratamento de dados por eles realizado. Assim, acompanhar e analisar essas informações serão atividades fundamentais para os agentes de tratamento não só para manter a conformidade, mas também para orientar novas práticas de proteção aos direitos dos titulares de dados.

Em outras palavras, com base nas informações disponibilizadas pela ANPD, pode-se mapear um conjunto de categorias e disponibilizá-las num formato adequado, para que seja feita uma gestão da informação que oriente as atividades de compliance e boas práticas, como o Relatório de Impacto à Proteção

de Dados (RIPD). No caso apontado neste estudo, o Relatório de Impacto criado e elaborado pela equipe do Núcleo Telessaúde da Universidade Federal de Santa Catarina (UFSC) (Telessaúde UFSC, 2022), sendo esta uma das boas práticas utilizadas.

Além do Relatório de Impacto, o Núcleo Telessaúde UFSC também dispõe de uma Política de Privacidade, de um Termo de Uso do serviço e de um Protocolo de Incidentes de privacidade, disponibilizados no site da instituição, de maneira acessível aos usuários. É oferecida ainda uma capacitação gratuita sobre privacidade dos dados, via Moodle, para uma melhor compreensão acerca dos termos da LGPD e sua relação com os dados pessoais dos titulares (Telessaúde UFSC, 2023a).

O Núcleo Telessaúde UFSC faz parte do Programa Nacional Telessaúde Brasil Redes, do Ministério da Saúde, e hoje atua em 100% dos municípios catarinenses. Disponibiliza serviços de educação permanente e apoio à tomada de decisão clínica dos profissionais que atuam no Sistema Único de Saúde (SUS), tendo como foco a atenção básica e o oferecimento de serviços como a Teleconsultoria, Telemedicina, Tele-Educação, Telediagnóstico e Segunda Opinião Formativa (Telessaúde UFSC, 2023b).

Uma vez que as atividades do Núcleo Telessaúde UFSC são responsáveis por democratizar os serviços de saúde e oferecer acesso e apoio na tomada de decisão clínica dos profissionais da área, necessitam de um vasto banco de dados, que inclui informações tanto desses profissionais, como de usuários do SUS, sendo então necessária a implementação de processos e políticas internas, que garantam o cumprimento das normas previstas na LGPD.

O Núcleo Telessaúde UFSC foi escolhido para esta análise por ser parte de uma política pública na área da saúde e por tratar um significativo volume de dados pessoais e dados pessoais sensíveis, conforme se observa pelo seu RIPD (Telessaúde UFSC, 2022):

a) dados dos pacientes do Núcleo Telessaúde UFSC;
b) dados clínicos dos pacientes do Núcleo Telessaúde UFSC;
c) dados para cada lesão indicada na solicitação;
d) dados para cada imagem adquirida.

O Telessaúde UFSC possui um amplo e complexo tratamento de dados pessoais e dados pessoais sensíveis, que pode afetar significativamente os direitos dos titulares em caso de eventual incidente de privacidade. Esse aspecto do tratamento exige instrumentos de gestão da informação adequados que assegurem os direitos dos titulares, principalmente um Relatório de Impacto atualizado e operacional.

É necessário, portanto, fazer um acompanhamento regular dos processos de forma a manter o RIPD e, consequentemente, as boas práticas adotadas, frequentemente atualizadas em conformidade com a LGPD.

Assim, esta pesquisa busca responder à questão de como os processos administrativos sancionatórios e as ações de fiscalização iniciadas pela ANPD podem contribuir para o aperfeiçoamento do modelo de Relatório de Impacto à Proteção de Dados adotado pelo Núcleo Telessaúde UFSC.

Tem como objetivo analisar os processos tendo por base as seguintes categorias jurídicas: Agentes de Tratamento (pessoa jurídica de direito privado e pessoa jurídica de direito público), infrações e incidentes e eventual sanção aplicada ou aplicável.

2 Conceitos da LGPD

Regida pela Lei n. 13.709, de 14 de agosto de 2018, a LGPD é a legislação brasileira que estabelece regras e diretrizes para o tratamento de dados pessoais por empresas, organizações e entidades públicas e privadas, com objetivo principal de proteger a privacidade dos indivíduos e garantir o controle sobre suas informações pessoais. Estabelece princípios fundamentais que devem ser observados no tratamento de **dados pessoais**, tais como a finalidade, a necessidade, a transparência e a segurança (Brasil, 2018).

Uma das principais inovações trazidas pela LGPD é a necessidade de consentimento do titular para o tratamento de seus dados pessoais, que se referem "[...] a qualquer informação relacionada à pessoa natural identificada ou identificável" (Brasil, 2018), podendo ser, por exemplo, nome, endereço, número de telefone, endereço de e-mail, CPF, entre outros dados que permitam a identificação de uma pessoa específica. É importante destacar que a identificação

pode ocorrer por meio da combinação desses dados com outras informações disponíveis.

Já os **dados pessoais sensíveis** são um subconjunto especial de dados pessoais, que merecem uma camada maior de proteção, devido ao seu alto potencial de causar discriminação ou danos significativos se forem utilizados indevidamente, conforme definição no Art. 5º da LGPD (Brasil, 2018). Os dados pessoais sensíveis podem abranger informações como origem racial ou étnica, convicções religiosas, opiniões políticas, filiação sindical, dados genéticos, dados biométricos, dados de saúde ou dados sobre a vida sexual de uma pessoa.

A atividade de **tratamento de dados** é caracterizada por:

> [...] 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, controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018).

Para estar em conformidade, é necessário que as instituições, por meio de seus controladores, analisem seus processos internos e como estão sendo utilizados e tratados os dados pessoais, avaliando se o tratamento está dentro de uma das bases legais existentes. Caso não esteja, deverão buscar adequação ou a eliminação desses dados. Segundo Maldonado (2019, p. 122):

> Eliminar um dado pessoal ou banco de dados pessoais significa excluí-los, definitivamente, do poder de controle do controlador, não importando o procedimento empregado para atingir tal finalidade. Ou seja, tornar inviável que o controlador possa tratar os dados objeto da eliminação.

O Art. 6º da LGPD aponta que a atividade de tratamento de dados deverá observar o princípio da boa fé, por meio de um comportamento leal e ético, que esteja justificado ou amparado na legislação. Além disso, o referido artigo também relaciona outros dez princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e, por fim, responsabilização e prestação de contas.

Criada em 2020, a **Autoridade Nacional de Proteção de Dados (ANPD)** é um órgão fiscalizador vinculado à Presidência da República e dispõe de plena autonomia técnica e decisória em território brasileiro. Seu objetivo é fiscalizar e

proteger os direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural, conforme aponta em seu planejamento estratégico atual e também na própria LGPD no Art. 55-J. (Autoridade Nacional de Proteção de Dados, 2022).

São 24 incisos relacionados na legislação apontando as competências da ANPD, que demonstram, de maneira geral, que este é o órgão superior responsável pela proteção de dados pessoais, bem como pela elaboração das diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade. Ela deverá, também, oferecer as devidas orientações aos agentes de tratamento, para o cumprimento das normas e regulamentos da legislação e, caso verifique possíveis descumprimentos, deverá, sob o rigor da Lei, fazer a devida análise, seguida de sanção administrativa e demais atribuições previstas em Lei.

As **medidas de segurança** estão previstas no Art. 46 da LGPD[1] e são classificadas em dois grandes grupos: as medidas técnicas ou operacionais, no âmbito da tecnologia da informação; e as medidas administrativas ou de gestão.

Jimene (2019, p. 330) classifica e define as medidas de segurança técnicas da seguinte forma: "[...] são aquelas adotadas no âmbito da Tecnologia da Informação, com o uso de recursos informáticos dotados de funcionalidades voltadas à garantia da segurança da informação". São exemplos: criptografia, mecanismos de segurança em softwares e hardwares, testes de vulnerabilidade, etc. Já as medidas administrativas são "[...] as atividades realizadas no âmbito administrativo-gerencial dos agentes de tratamento, incluindo-se as de natureza jurídica" (Jimene, 2019, p. 330). Nesse caso, são exemplos: política de privacidade, contratos de confidencialidade, capacitação de empregados, controle de acesso a arquivos físicos, etc.

As **boas práticas e a governança** desempenham um papel fundamental na conformidade com a legislação e na construção de relações de confiança entre as empresas e os titulares dos dados. Referem-se às ações, procedimentos e políticas que as organizações devem adotar para garantir a proteção e privacidade dos dados pessoais, envolvendo desde a implementação de medidas técnicas e organizacionais até a conscientização e treinamento dos colaboradores. Já a governança, por sua vez, é o conjunto de processos, estruturas e políticas que

garantem a conformidade com a LGPD e a efetiva gestão dos dados pessoais (Brasil, 2018).

No que se refere à implementação de boas práticas e de governança adequadas, as instituições devem adotar uma abordagem estratégica, envolvendo a realização de uma análise de risco, a designação de um encarregado de proteção de dados (DPO), bem como a criação de políticas internas que estabeleçam diretrizes claras sobre como os dados pessoais devem ser tratados.

As medidas de segurança e boas práticas são critérios a serem analisados no processo administrativo que apura a necessidade de aplicação de sanções. Em outras palavras, sua ausência pode resultar na aplicação de sanções e sua reiterada inobservância pode agravar a sanção aplicada nos termos do Art. 52 da LGPD (Brasil, 2018).

Conforme aponta o Art. 37 da LGPD, "[...] o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (Brasil, 2018). Sendo assim, é possível dizer que o que caracteriza o **Controlador** é a capacidade dada a ele de determinar as finalidades para as quais os dados serão coletados, armazenados, tratados e compartilhados, bem como a sua capacidade também de eleição das bases legais que legitimam o tratamento proposto. Ainda discorrendo sobre o Controlador, o Art. 5°, inciso VI da LGPD diz que ele é a "[...] pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", e o **Operador** é a "[...] pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (Brasil, 2018).

Cabe esclarecer que a legislação trata por Agentes de Tratamento tanto a figura do controlador como do operador, apontando obrigações que envolvam tanto um como o outro. Conforme a LGPD expõe no Art. 46, os agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas para a proteção dos dados pessoais que armazenam, vedando-os a acessos que não tenham sido prévia e legalmente autorizados, bem como protegendo-os de possíveis incidentes de segurança ou outras formas de tratamento ilícitos ou inadequados.

De acordo com o exposto no Art. 5º, inciso XVII da LGPD, o **Relatório de Impacto à Proteção de Dados (RIPD)** é a "[...] documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (Brasil, 2018). Conforme a legislação, é a ANPD que dispõe da autoridade para solicitar ao controlador dos dados que lhe conceda o acesso ao RIPD, para que sejam verificadas as conformidades de tratamento dos dados em relação aos parâmetros da Lei.

Gomes (2021, p. 271) afirma que uma das principais funções do RIPD "[...] é a prevenção e mitigação dos riscos aos direitos dos titulares de dados". Afirma ainda que "o RIPD somente é obrigatório caso haja o tratamento de dados que possam gerar riscos às liberdades civis e aos direitos fundamentais do seu titular" e que, por isso, é necessário primeiro identificar quais serão os dados tratados por determinada instituição e se isso constituirá em riscos.

Especificamente no que tange à área da saúde, é notável a necessidade desse tipo de instrumento, uma vez que a área trata de diversos dados pessoais e dados pessoais sensíveis, dispostos em sistemas, prontuários físicos e eletrônicos, receituários, resultados de laudos e exames, comunicação entre profissionais e pacientes, histórico de saúde dos indivíduos, dentre diversos outros parâmetros, que em sua maioria são considerados dados pessoais sensíveis e, portanto, podem eventualmente gerar riscos às liberdades civis e aos direitos fundamentais do seu titular (Dallari; Monaco, 2021).

O RIPD está ligado ao cumprimento do princípio da responsabilidade e da prestação de contas, uma vez que a titularidade dos dados sempre será da pessoa natural cujos dados são tratados pelos agentes de tratamento, conforme disposto nos Artigos 17 e 18 da LGPD, independentemente da base de legitimidade aplicada ao tratamento, como o consentimento ou a tutela da saúde, descritos nos Artigos 7° e 11 da LGPD (Brasil, 2018).

Para garantir a conformidade e o cumprimento das disposições da Lei n. 13.709, de 14 de agosto de 2018, foram estabelecidas **sanções administrativas**, essenciais para compreender as implicações e consequências legais da violação das disposições da legislação, bem como para o entendimento do papel da ANPD

na possível aplicação de penalidades. As mesmas podem ser observadas nos Artigos 52 e 54 da LGPD.

Segundo Viviane Maldonado, em seu livro *LGPD: sanções e decisões judiciais*, as sanções administrativas são medidas punitivas aplicadas pela autoridade de proteção de dados competente, em resposta às infrações cometidas por organizações que tratam dados pessoais. As sanções têm como objetivo desencorajar práticas inadequadas e garantir o cumprimento das obrigações estabelecidas na LGPD (Maldonado, 2022). De acordo com a Lei n. 13.709/2018, em seu Art. 52, a sanção administrativa consiste na imposição de penalidades pela autoridade de proteção de dados, em decorrência do descumprimento das disposições da LGPD. Essas penalidades podem variar de advertências simples até multas administrativas, a depender da gravidade da infração e do impacto causado aos direitos dos titulares dos dados (Brasil, 2018).

Estão estruturados na LGPD diferentes tipos de sanções administrativas, que foram descritas de acordo com a gravidade das infrações e a natureza das consequências causadas aos titulares dos dados. Dentre as principais sanções previstas estão: advertência, multa simples, multa diária, publicização da infração e bloqueio ou eliminação dos dados pessoais. Importante mencionar que as sanções administrativas só serão aplicadas após procedimento administrativo instaurado.

Conforme a LGPD, o **processo administrativo** é um conjunto de etapas e procedimentos estabelecidos pela ANPD para a apuração de possíveis infrações e a aplicação de sanções previstas na Lei. De acordo com o disposto no Art. 53 da LGPD, um processo administrativo é instaurado mediante provocação ou por meio de ofício emitido pela ANPD, além disso, deverá seguir as garantias de ampla defesa, contraditório, presunção de inocência e devido processo legal.

Maldonado (2022) explora a definição de processo administrativo no contexto da LGPD, destacando a importância desse procedimento como um instrumento de fiscalização e responsabilização dos agentes de tratamento de dados e enfatizando a necessidade de garantir a segurança e a privacidade dos titulares de dados pessoais. O processo administrativo na LGPD representa um avanço significativo na proteção dos direitos individuais no âmbito do tratamento

de dados pessoais (Maldonado, 2022). A autora ainda ressalta que a ANPD, enquanto autoridade responsável pela condução dos processos administrativos, desempenha papel fundamental na aplicação da lei e na defesa desses direitos.

Ao considerar as contribuições de Maldonado (2022), percebe-se a relevância do processo administrativo como um mecanismo de *accountability* e também como garantia da privacidade e segurança dos dados pessoais.

O **Titular de Dados** é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (Brasil, 2018). Em relação aos direitos do titular de dados pessoais, a LGPD regulamenta que ele deve ter pleno acesso às informações sobre o tratamento dos seus dados, devendo essas informações ser disponibilizadas de forma clara, adequada e ostensiva, de acordo com o princípio do livre acesso da referida Lei, que demanda os seguintes pontos: a finalidade específica do tratamento; a forma e duração do tratamento, observados os segredos comercial e industrial; a identificação do controlador; as informações de contato do controlador; as informações acerca do uso compartilhado de dados pelo controlador e a finalidade; as responsabilidades dos agentes que realizarão o tratamento; e, por fim, os próprios direitos do titular (Brasil, 2018).

A **Coordenação-Geral de Fiscalização (CGF)** é um órgão específico singular da ANPD, exercendo o papel de verificação do cumprimento das normas e regulamentos relativos à LGPD, bem como de eventuais infrações à proteção de dados pessoais (Autoridade Nacional de Proteção de Dados, 2023b). Dentre uma lista de 26 competências, descritas no Regimento Interno da ANPD, a CGF é principalmente responsável por "I- fiscalizar e aplicar as sanções previstas no artigo 52 da Lei n. 13.709, de 2018, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso", bem como "II- proferir decisão em primeira instância nos processos administrativos sancionadores da ANPD".

3 LGPD e Ciência da Informação

A ciência da informação evoluiu observando as necessidades de solução dos problemas informacionais que se modificaram ao longo dos anos (Saracevic, 1996). Sendo assim, como afirmam Oliveira, Motta, Melo e Esteves (2020):

> Sempre que uma nova legislação promove novas regras, formatos e padrões no tratamento da informação, as áreas de conhecimento dedicadas a este tema precisam se dedicar a sua compreensão, não apenas para se adequar ao ambiente regulatório advindo da nova legislação, mas principalmente para contribuir para soluções técnicas para os desafios que são inerentes ao surgimento de uma nova regra.

Os autores apontam que a LGPD tem grande potencial de impacto no trabalho dos profissionais da informação, principalmente no que se refere à gestão documental e gestão da informação. É preciso, portanto, criação de ações que atendam aos objetivos da nova Lei em vigor.

No que tange à gestão da informação, conforme Choo (2003), pode ser compreendida como um ciclo contínuo de seis atividades: identificação das necessidades; aquisição; organização e armazenamento; desenvolvimento de produtos e serviços; distribuição e utilização da informação.

Tal embasamento teórico apoia a compreensão dos fatores necessários para a construção do RIPD, que é definido pelo artigo 5, inciso VII, da Lei Geral de Proteção de Dados. Isso porque ele deve conter um descritivo completo do tratamento de dados realizado pelos agentes de tratamento, quais dados são tratados, que riscos existem para os titulares dos dados, assim como detalha toda a conformidade da instituição com a legislação, especificando o tratamento previsto no que tange à coleta e à recepção, produção e reprodução dos dados, utilização, acesso, transmissão, distribuição, transferência, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, bem como a difusão ou extração dos dados. Por fim e, principalmente, o RIPD determina a todos os atores envolvidos no tratamento de dados, quais as medidas, salvaguardas e mecanismos devem ser utilizados para amenizar os riscos aos direitos e garantias fundamentais dos titulares de dados.

Quanto à gestão de documentos (GD), seu trabalho envolve etapas para a identificação, classificação, avaliação e destinação de documentos. Seus procedimentos são essenciais para que as organizações conduzam uma correta e eficiente adequação à LGPD e aquelas que já adotam práticas de GD tendem a encontrar mais facilidade de ajuste aos parâmetros da Lei (Schwaitzer; Nascimento; Costa, 2021).

Cabe destacar que a preservação de dados ou informações pode também

envolver a documentação adequada dos processos e contextos associados a esses dados ou informações, facilitando a compreensão e a interpretação futuras. E aqui, mais uma vez podemos observar a similaridade com outro apontamento da LGPD, no que diz respeito à criação de um instrumento, chamado de Relatório de Impacto, que documenta o tratamento de dados, agentes de tratamento, boas práticas e segurança em relação aos dados, bem como o que fazer no caso de um eventual incidente de segurança e a conformidade de todo o processo com o ordenamento jurídico nacional.

4 Aspectos metodológicos

Esta pesquisa é considerada de abordagem qualitativa (Creswell, 2010; Gray, 2012) tendo objetivos exploratório e descritivo (Marconi; Lakatos, 2010).

A abordagem qualitativa possibilita uma maior proximidade com a realidade, por meio de um olhar investigativo, que visa promover o aprendizado sobre o problema, trazendo à tona uma perspectiva interpretativa sobre os dados.

O objetivo exploratório busca uma familiaridade com o contexto estabelecido, apresentando as suas características e, neste caso em específico, expondo também uma investigação de pontos de melhoria. Trata-se de um tema recente, visto que a LGPD foi sancionada em 2018, entrou em vigor em 2020 e somente em março de 2023 a ANPD disponibilizou, pela primeira vez, a lista de processos administrativos sancionatórios instaurados, porém, ainda na fase de instrução (Autoridade Nacional de Proteção de Dados, 2023c).

Além disso, caracteriza-se como uma pesquisa de objetivo descritivo pelo fato de buscar analisar diferentes fontes de informação e relacioná-las, de modo a apresentar sugestões de melhoria ao Relatório de Impacto do Núcleo Telessaúde UFSC.

Tendo em vista a disponibilidade e a facilidade de acesso às informações na web (Guimarães, 2008), esta será a primeira fonte de informação utilizada. Os processos instaurados estão brevemente descritos no portal da ANPD, assim, é possível contar com uma publicação de origem governamental de caráter informativo aos cidadãos (Vergueiro, 2000).

A pesquisa documental, por sua vez, poderá ser realizada por meio do

acesso aos documentos do Núcleo Telessaúde UFSC, a fim de analisar os instrumentos legais e os processos existentes relacionados à LGPD. A partir da relação com a investigação dos processos administrativos sancionatórios instaurados pela ANPD, será possível avaliar se existem riscos nas práticas do Núcleo e como os mecanismos em vigor podem ser melhorados.

5 Análise dos resultados

Esta seção traz uma análise das empresas e instituições autuadas nos primeiros processos administrativos sancionatórios instaurados pela ANPD em 2023, buscando trazer os seguintes pontos em comum: n. do processo, nome da instituição, setor, esfera e a sua adequação à LGPD, conforme Quadros um a oito, apresentados na sequência, que indicam as condutas observadas como Medidas Administrativas (MA) e Medidas de Tecnologia da Informação (TI).

Das oito instituições presentes na lista dos processos administrativos sancionatórios da ANPD, apenas uma representa uma empresa privada e sete são órgãos públicos, sendo que, destes, dois são da área da saúde (com três processos no total). Tal cenário chama a atenção por ser a saúde uma área ampla e que abrange dados pessoais e dados pessoais sensíveis dos milhares de usuários do Sistema Único de Saúde - o SUS, e que seria de suma importância estar operando dentro dos rigores da lei, para preservar os direitos dos titulares dos dados.

Quadro 1 - Processos Ministério da Saúde

N. dos Processos	1) 00261.000456/2022-12 e 2) 00261.001882/2022-73
Instituição	Ministério da Saúde
Setor	Público
Esfera	Estatal
Conduta observada (MA)	1) Não atendimento à requisição da ANPD; ausência de encarregado de dados pessoais; ausência de comunicação de incidente de segurança. 2) Ausência de comunicação de incidentes de segurança aos titulares; ausência de medidas de segurança

Fonte: Autoridade Nacional de Proteção de Dados (2023c).

Adequação à LGPD: No site oficial do órgão há uma área dedicada a informações sobre a LGPD com dados de contato do encarregado de dados. O ministério nomeou os encarregados de dados por meio da Portaria GM/MS n. 953, de 11 de maio de 2023. Como canal para registrar as manifestações é utilizada a

Plataforma Fala.Br, um sistema web do governo federal que tem como objetivo unificar as centrais de Ouvidoria e Acesso à Informação. Também há menção sobre a participação do ministério em um grupo de trabalho sobre a LGPD que tem como objetivo orientar a adequação do Ministério da Saúde em níveis estratégico, tático e operacional (Brasil, 2022). Ainda na área dedicada à LGPD no site oficial, há uma página denominada Registro de Incidentes com Dados Pessoais (Brasil, 2023). Nela estão apresentados três incidentes, com o período em que cada um ocorreu, a natureza dos dados potencialmente expostos e a comunicação aos titulares desses dados:

a) risco de acesso indevido ao Sistema de Cadastro e Permissão de Acesso (SCPA), no período de 27/11/2021 a 04/05/2022. A falha permitia a consulta individual através do CPF do titular dos dados a nome completo, endereço, telefone, data de nascimento, nome da mãe e cartão nacional de saúde (CNS);
b) possível vazamento de credencial do Sistema de Cadastramento de Usuários do Sistema Único de Saúde (CADSUS) que expôs dados demográficos, no período de 22/04/2019 a 29/06/2022. Essa falha permitia o acesso a CPF; nome; nome social; nome da mãe; nome do pai; sexo; raça/cor; etnia indígena; data de nascimento; tipo sanguíneo; data de óbito; justificativa do preenchimento da data de óbito; nacionalidade; país de nascimento; município de nascimento; e data de naturalização, portaria de naturalização e data de entrada no Brasil;
c) possível crime cibernético relativo à venda ilegal das bases de dados de sistemas governamentais, como o CADSUS e o e-SUS Notifica na data de 04/11/2022. Em análise preliminar não foi possível identificar se as bases comercializadas estavam atualizadas.

Quadro 2 - Processo Telekall Inforservice

N. do Processo	00261.000489/2022-62
Instituição	Telekall Inforservice
Setor	Privado
Conduta observada (MA)	Ausência de comprovação de hipótese legal; ausência de registro de operações (TI); não envio de Relatório de Impacto de Proteção de Dados; ausência de encarregado de dados pessoais; não atendimento à requisição da ANPD

Fonte: Autoridade Nacional de Proteção de Dados (2023c).

Adequação à LGPD: A empresa Telekall (Autoridade Nacional de Proteção de Dados, 2023a) é do ramo de telemarketing e está com o seu CNPJ inapto por omissão de declarações. Foi cadastrada junto à Receita Federal em 09/02/2021 e tem como razão social o nome *Emmanuel Gomes de Jesus*. Sobre as demais informações que esta pesquisa tenta levantar, não foi possível localizar em fontes públicas outros dados da empresa como número de funcionários, adequação à LGPD, ou mesmo se há um encarregado de dados nomeado na instituição.

Quadro 3 - Processo Instituto de Pesquisas Jardim Botânico do Rio de Janeiro

N. do Processo	00261.000574/2022-21
Instituição	Instituto de Pesquisas Jardim Botânico do Rio de Janeiro
Setor	Público
Esfera	Federal - Responde ao Ministério do Meio Ambiente
Conduta observada (MA)	Não comunicação de incidente de segurança; não atendimento à requisição da ANPD

Fonte: Autoridade Nacional de Proteção de Dados (2023c).

O Instituto tem como missão: "Promover, realizar e difundir pesquisas científicas, com ênfase na flora, visando à conservação e à valorização da biodiversidade, bem como realizar atividades que promovam a integração da ciência, educação, cultura e natureza" (Instituto de Pesquisas Jardim Botânico do Rio de Janeiro, 2023).

Adequação à LGPD: Há no site oficial do Instituto uma área dedicada à LGPD. Nela está discriminado o encarregado de dados da instituição e o substituto eventual. Há dois canais de contato para solicitações do titular dos dados, a plataforma web Fala.BR e um endereço de e-mail. Não há nenhuma menção de incidentes com dados pessoais ou do processo n. 00261.000574/2022-21.

Quadro 4 - Processo Secretaria de Educação do Distrito Federal

N. do Processo	00261.001192/2022-14
Instituição	Secretaria de Educação do Distrito Federal
Setor	Público
Esfera	Estadual
Conduta observada (MA)	Não atendimento à requisição da ANPD.

Fonte: Autoridade Nacional de Proteção de Dados (2023c).

Adequação à LGPD: Há no site oficial uma página com conteúdo educacional sobre a LGPD com os principais conceitos, etapas que os dados devem ou podem passar, o decreto no Distrito Federal e Autoridade Nacional de Proteção de Dados (Distrito Federal, 2023). Na mesma página há um aviso de privacidade e proteção de dados pessoais com um canal de e-mail para solicitações dos titulares dos dados. Não há menção sobre incidentes com dados pessoais ou do processo n. 00261.001192/2022-14.

Quadro 5 - Processo Secretaria de Estado da Saúde de Santa Catarina

N. do Processo	00261.001886/2022-51
Instituição	Secretaria de Estado da Saúde de Santa Catarina
Setor	Público
Esfera	Estadual
Conduta observada (MA)	Ausência de comunicação de incidente de segurança aos titulares; ausência de medidas de segurança; não atendimento a determinações da ANPD

Fonte: Autoridade Nacional de Proteção de Dados (2023c).

Adequação à LGPD: No site oficial há uma área dedicada à LGPD com o nome do encarregado e um contato de e-mail para solicitações dos titulares dos dados. Na mesma página web há descrições das atribuições do encarregado de dados (Santa Catarina, 2021). Não há citação sobre o processo n. 00261.001886/2022-51 ou sobre eventuais incidentes com os dados pessoais.

Quadro 6 - Processo Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo (IAMSPE)

N. do Processo	00261.001969/2022-41
Instituição	Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo (IAMSPE)
Setor	Público
Esfera	Estadual
Conduta observada (MA)	Ausência de comunicação de incidentes de segurança aos titulares; ausência de medidas de segurança

Fonte: Autoridade Nacional de Proteção de Dados (2023c).

O IAMSPE oferece atendimento aos usuários por meio de uma rede própria distribuída em 163 municípios do Estado de São Paulo. A rede conta com hospitais e laboratórios de análise clínica e de imagem (Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo, 2023).

Adequação à LGPD: No site oficial há uma área dedicada para Política e Proteção de Dados Pessoais, onde está descrito um resumo da LGPD com as

obrigações do IAMSPE frente à proteção de dados pessoais. Consta também o nome do encarregado de dados e um endereço de e-mail para solicitações dos titulares dos dados. Não há menção a nenhum incidente com os dados pessoais.

Quadro 7 - Processo Secretaria de Desenvolvimento Social, Criança e Juventude do Estado de Pernambuco

N. do Processo	00261.001963/2022-73
Instituição	Secretaria de Desenvolvimento Social, Criança e Juventude-PE
Setor	Público
Esfera	Estadual
Conduta observada (MA)	Ausência de comunicação de incidente de segurança aos titulares; ausência de medidas de segurança

Fonte: Autoridade Nacional de Proteção de Dados (2023c).

Adequação à LGPD: No site oficial não há uma área específica para LGPD, somente um comunicado oficial com data de 12 de junho de 2022. O comunicado descreve um compromisso da Secretaria em se adequar à LGPD. Em anexo ao comunicado constam duas portarias: a primeira nomeando a encarregada de dados e a segunda nomeando a equipe de apoio. Em anexo ao mesmo comunicado também está o plano de comunicação de política de proteção de dados pessoais que descreve um plano de ação com marcos para a adequação da secretaria à LGPD. Por último, no comunicado oficial há uma nota de esclarecimento sobre o incidente com dados pessoais sensíveis que causou o Processo n. 00261.001963/2022-73. Essa nota cita a possível exposição de planilha que continha dados dos beneficiários do programa assistencial da Secretaria de Desenvolvimento Social, Criança e Juventude (Pernambuco, 2022).

Quadro 8 - Processo Instituto Nacional do Seguro Social (INSS)

N. do Processo	00261.001888/2023-21
Instituição	Instituto Nacional do Seguro Social (INSS)
Setor	Público
Esfera	Nacional
Conduta observada (MA)	Ausência de comunicação de incidente de segurança aos titulares; não atendimento de medida preventiva adotada pela ANPD

Fonte: Autoridade Nacional de Proteção de Dados (2023c).

Adequação à LGPD: Existe no site oficial do INSS uma área dedicada à LGPD. Trata sobre o que é a Lei, os direitos dos usuários, informa sobre os dados coletados, tratados e armazenados pela instituição e indica os respectivos agentes de tratamento de dados pessoais, sendo o Controlador o próprio INSS; o Operador

a Dataprev e disponibiliza o e-mail do Encarregado: encarregado@inss.gov.br. Também oferece acesso para download do material "A LGPD E O INSS" (Instituto Nacional do Seguro Social, 2021).

6 Considerações finais

Em uma visão geral, chama atenção o fato de que dos nove processos administrativos sancionatórios de 2023, apenas uma instituição autuada é privada, o que denota o ponto de que as instituições públicas podem estar mais vulneráveis a incidentes de segurança, questão que pode ser explorada em pesquisas posteriores.

Outro aspecto relevante para este estudo, com base nas informações disponibilizadas pela ANPD, é que dos oito processos em que foram autuadas instituições públicas, três deles são da área da saúde.

Essa informação aponta, pelo menos com os dados que foram possíveis coletar, que o tratamento de dados pessoais sensíveis, como os dados referentes à saúde[2], estão sendo objeto de maior cuidado no processo fiscalizatório da ANPD até o presente momento.

Já as condutas observadas apontam para uma nítida falha na adoção de medidas de segurança administrativas ou de gestão, demonstrando a inadequação do tratamento de dados nos padrões exigidos pela LGPD, inobstante o tempo de adequação disponibilizado desde o início da vigência do dispositivo legal.

Observa-se ainda, no que se refere às condutas observadas, que duas instituições deixaram de entregar o RIPD quando solicitadas pela ANPD, agravando a situação de inobservância às medidas de segurança necessárias para o adequado tratamento de dados.

Essas informações devem ser inseridas no âmbito do tratamento de dados realizado por instituições, em especial o do Núcleo Telessaúde UFSC, para aperfeiçoar as medidas de segurança e o RIPD, incorporando ao seu fluxo de reexame informações atualizadas que possam prevenir com maior eficiência eventuais riscos aos direitos dos titulares.

Em síntese, o processo de adequação do tratamento de dados à LGPD exige, além de uma visão jurídica, um processo adequado de gestão da

informação. Com a definição clara dos fluxos de informação decorrentes do tratamento de dados, dos atores envolvidos no processo e da revisão constante das boas práticas implementadas pelos controladores.

No caso do Núcleo Telessaúde UFSC, o fluxo de atualização do RIPD passou a contar com uma nova fase em que são inseridas as informações dos processos sancionatórios da ANPD. Elas são analisadas e posteriormente incorporadas, quando pertinentes, como novas medidas de segurança ou boas práticas de caráter preventivo.

O presente estudo contribui para a mudança do fluxograma de controle e reexame do RIPD, inserindo uma nova etapa de análise dos riscos, trazendo as informações atualizadas dos processos sancionatórios da ANPD. Esse aspecto permite aos agentes de tratamento uma visão mais ampla, que transcende à análise de suas práticas e métodos de tratamento de dados, cobrindo dimensões e realidades diferentes. Essa perspectiva só se torna viável com a adoção de conhecimentos na área de gestão da informação.

Financiamento

Fundação de Amparo à Pesquisa e Extensão Universitária (FAPEU), por meio de bolsa de mestrado concedida.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil) (ANPD). **Auto de Infração n. 3/2022/CGF/ANPD**. Brasília, 2023a.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil) (ANPD). **Autoridade Nacional de Proteção de Dados**. Brasília, 2023b.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil) (ANPD). **Planejamento estratégico ANPD 2021-2023**. Brasília, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil) (ANPD). **Processos Administrativos Sancionadores**. Brasília, 2023c.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, ano 155, n. 157, p. 59, 15 ago. 2018.

BRASIL. Ministério da Saúde. **Grupo de trabalho**. Brasília, 2022.

BRASIL. Ministério da Saúde. **Registro de incidentes com dados pessoais**. Brasília, 2023.

CHOO, Chun Wei. **Gestão de informação para a organização inteligente**: a arte de explorar o meio ambiente. Lisboa: Caminho, 2003.

CRESWELL, John W. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. Porto Alegre: Artmed, 2010.

DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). **LGPD na Saúde**. São Paulo: Thomson Reuters Brasil, 2021.

DISTRITO FEDERAL (Brasil). Secretaria de Estado de Educação. **LGPD**. Brasília: Secretaria de Estado de Educação, 2023.

GOMES, Maria Cecília Oliveira. Relatório de Impacto à Proteção de Dados: obrigatório para o tratamento de dados sensíveis? *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). **LGPD na Saúde**. São Paulo: Thomson Reuters Brasil, 2021.

GRAY, David E. **Pesquisa no mundo real**. 2. ed. Porto Alegre: Penso, 2012.

GUIMARÃES, Angelo de Moura. Internet. *In*: CAMPELLO, Bernadete Santos; CALDEIRA, Paulo da Terra (org.). **Introdução às fontes de informação**. 2. ed. Belo Horizonte: Autêntica, 2008. p. 159-178.

INSTITUTO DE ASSISTÊNCIA MÉDICA AO SERVIDOR PÚBLICO ESTADUAL DE SÃO PAULO. **Apresentação**. São Paulo, 2023.

INSTITUTO DE PESQUISAS JARDIM BOTÂNICO DO RIO DE JANEIRO. **Quem somos**. Rio de Janeiro, 2023.

INSTITUTO NACIONAL DO SEGURO SOCIAL (INSS). **A LGPD e o INSS**. Brasília: Instituto Nacional do Seguro Social, 2021.

JIMENE, Camilla do Vale. Da segurança e do sigilo dos dados. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **LGPD: Lei Geral de Proteção de Dados - Comentada**. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega (coord.). **LGPD**: sanções e decisões judiciais. São Paulo: Thomson Reuters Brasil, 2022.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

OLIVEIRA et al. (2020). Empoderamento digital, proteção de dados e LGPD. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, João Pessoa, v. 15, n. 3, 2020.

PERNAMBUCO. Secretaria de Desenvolvimento Social, Criança, Juventude e Prevenção à Violência e às Drogas. **Comunicado oficial sobre a adequação à Lei Geral de Proteção de Dados - LGPD (Lei n. 13.709/2018)**. Recife: SDSCJPVD, 2022.

SANTA CATARINA. Secretaria de Estado da Saúde. **Proteção de dados no âmbito da SES**. Florianópolis: Secretaria de Estado da Saúde, 2021.

SARACEVIC, Tefko. Ciência da Informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 1, n. 1, p. 41-62, jan./jun. 1996.

SCHWAITZER, Lenora; NASCIMENTO, Nathália; COSTA, Alexandre de Souza. Reflexões sobre a contribuição da gestão de documentos para programas de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). **Revista Acervo (Arquivo Nacional)**, v. 34, n. 3, 2021.

TELESSAÚDE UFSC. **Curso de noções básicas em LGPD para Usuários do Telessaúde - UFSC**. Florianópolis, 2023a.

TELESSAÚDE UFSC. **Relatório de impacto à proteção de dados pessoais**. Florianópolis, 2022.

TELESSAÚDE UFSC. **Resumo executivo**. Florianópolis, 2023b.

VERGUEIRO, Waldomiro. Publicações governamentais. *In*: CAMPELLO, Bernadete Santos; CENDÓN, Beatriz Valadares; KREMER, Jeannette Marguerite (org.). **Fontes de informação para pesquisadores e profissionais**. Belo Horizonte: Ed. da UFMG, 2000. p. 111-120.

General Data Protection Law and the preparation of the Personal Data Protection Impact Report

Abstract: It has been in force in Brazil since 2020, Law No. 13,709, of August 14, 2018 - General Data Protection Law, and the National Data Protection Authority began to disclose the list of sanctioning processes of companies and public institutions after March 2023. Based on these first proceedings initiated by the General Inspection Coordination, this research sought to analyze, from the

perspective of information management, how the information on infractions, incidents, and any sanctions applied or applicable, as well as the main legal characteristics of the institutions fined, could contribute to the preparation and improvement of the Personal Data Protection Impact Report of the Federal University of Santa Catarina Telehealth Centers. The research has a qualitative approach, exploratory and descriptive objectives. It aims to analyze the practices related to the Law at the Telehealth Center and propose improvements based on the mapping of the administrative sanctioning processes initiated by the National Authority, as well as, from there, to identify the profile of the treatment agents investigated, as well as the main causes of assessment. Of the nine processes in 2023, three are from health institutions and the conduct indicates failures in the adoption of administrative or management security measures. Such information contributes to analyses relevant to Telehealth. The study contributes to changing the Report's flowchart, inserting a risk analysis step through process information, a viable perspective only with the application of knowledge in information management.

Keywords: General Data Protection Law; impact report; telehealth; administrative sanctions

Recebido: 28/01/2024
Aceito: 17/05/2024

Declaração de autoria

Concepção e elaboração do estudo: Marcelo Minghelli, Bárbara Balbis.
Coleta de dados: Marcelo Minghelli, Bárbara Balbis.
Análise e interpretação de dados: Marcelo Minghelli, Bárbara Balbis, Mariene Alves.
Redação: Bárbara Balbis, Mariene Alves, Patricia Siqueira.
Revisão crítica do manuscrito: Patricia Siqueira, Mariene Alves.

Como citar
MINGHELLI, Marcelo; GARCIA, Bárbara Balbis; VALE, Mariene Alves do; SANTOS, Patricia Siqueira. Lei Geral de Proteção de Dados e a elaboração do Relatório de Impacto à Proteção de Dados Pessoais. **Em Questão**, Porto Alegre, v. 30, e-138249, 2024. DOI: https://doi.org/10.1590/1808-5245.30.138249

Parecer(es) aberto(s):

https://doi.org/10.1590/1808-5245.30.138249A

https://doi.org/10.1590/1808-5245.30.138249B

https://doi.org/10.1590/1808-5245.30.138249C

[1] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (Brasil, 2018).

[2] Inciso II, do Art. 5°, da Lei Geral de Proteção de Dados Pessoais (Brasil, 2018).