ASPECTOS GERAIS PARA A IMPLANTAÇÃO E ADEQUAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS EM UM INSTITUTO DE PREVIDÊNCIA DE SANTA CATARINA (IPREV).

Eduardo Lopes Jonker- eduardo.jonker@sea.sc.gov.br

RESUMO

O presente relato descreve as ações extensionistas para a identificação de aspectos gerais e estruturação de diretrizes visando a adequação do Instituto de Previdência de Santa Catarina (IPREV-SC) à Lei nº 13.709/2018 (LGPD). A iniciativa fundamenta-se na necessidade imperativa de proteger dados pessoais e sensíveis, garantindo o direito à privacidade de aproximadamente 150.000 segurados do regime próprio. A metodologia adotada foi o estudo de caso com abordagem qualitativa e indutiva, fundamentada no acompanhamento das comissões internas de implantação da lei e de gestão documental. As ações envolveram o mapeamento do ciclo de vida dos dados, desde a coleta no protocolo até o descarte final, além da análise de fluxos em sistemas digitais como o portal GOV.BR e o sistema PIQL/CIASC. Os resultados demonstram que a conformidade legal no setor público depende da indissociabilidade entre segurança da informação e gestão arquivística rigorosa. A experiência promoveu uma mudança na cultura organizacional, estabelecendo níveis de sigilo e critérios para o tratamento de dados previdenciários. Conclui-se que a governança de dados fortalece a transparência pública e a proteção dos direitos fundamentais, servindo como modelo de modernização administrativa para outras autarquias estaduais.

Palavras-chave: LGPD, Segurança da Informação, Governança, Previdência Social.

1 INTRODUÇÃO

A proteção de dados pessoais consolidou-se, na contemporaneidade, como um dos pilares fundamentais da cidadania e da dignidade da pessoa humana na era digital. Este fenómeno foi impulsionado pela crescente vulnerabilidade de informações em bases de dados massivas, o fenómeno do Big Data, onde a capacidade de processamento e cruzamento de dados superou as barreiras físicas e geográficas tradicionais. Como observam Lima, Almeida e Maroso (2020), a proteção de dados não é um fim em si mesma, mas um meio de garantir a liberdade individual contra o tratamento automatizado e a vigilância. No Brasil, o reconhecimento da relevância do tema culminou na promulgação da Emenda Constitucional nº 115/2022, que elevou a proteção de dados pessoais à categoria de direito fundamental, inserindo-o no rol das garantias individuais da Constituição Federal de 1988.

No âmbito da Administração Pública, o desafio de implementação da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) assume contornos específicos e de alta complexidade. Diferente do setor privado, onde o consentimento muitas vezes rege as relações, o Estado trata dados baseando-se no cumprimento de obrigações legais e na execução de políticas públicas. Mendes (2019) argumenta que a autodeterminação informativa é o conceito-chave que permite ao cidadão manter o controlo sobre o fluxo de suas informações, mesmo quando estas estão sob custódia estatal. É neste cenário que o Instituto de Previdência de Santa Catarina (IPREV-SC), autarquia gestora do Regime Próprio de Previdência Social (RPPS) dos servidores estaduais, emerge como um ponto focal de análise.

O IPREV-SC lida quotidianamente com um volume crítico de dados que a legislação classifica como "sensíveis" (Art. 5º, II da LGPD). Segundo Pozzo e Martins (2020), o tratamento de dados na Administração Pública exige um dever de cuidado redobrado, uma vez que o titular muitas vezes não tem a opção de não fornecer o dado caso queira aceder a um serviço essencial ou benefício previdenciário. No contexto do IPREV, informações que revelam históricos de saúde para perícias médicas ou contextos socioeconómicos para pensões alimentares constituem o núcleo da vida privada dos segurados. Portanto, a gestão dessas informações não é apenas uma tarefa burocrática, mas um exercício de custódia de direitos fundamentais.

A instituição encontra-se atualmente em uma intersecção tensa entre dois marcos regulatórios: o dever de transparência plena, regido pela Lei de Acesso à Informação (LAI – Lei nº 12.527/2011), e a obrigação de sigilo imposta pela LGPD. Conforme destaca Pinheiro (2020), a conformidade não se limita a aspetos jurídicos, mas envolve uma profunda revisão da arquitetura tecnológica e dos processos internos. Enquanto a LAI busca "abrir" o Estado para o controlo social, a LGPD impõe limites para garantir que essa abertura não resulte na exposição indevida do indivíduo.

Esta ação extensionista e de gestão visa identificar e aprofundar os aspectos gerais da Lei nº 13.709/2018 para a implementação de tecnologias de proteção no instituto. A iniciativa não se limitou a uma conformidade estática, mas buscou promover uma mudança na cultura organizacional. Como reforçam Schwaitzer, Nascimento e Costa (2020), a gestão documental é o alicerce indispensável para a privacidade, pois permite definir o ciclo de vida do dado — desde a entrada no protocolo até o descarte seguro.

A justificativa para esta ação reside na transformação do dado pessoal em um ativo de poder. A digitalização de processos previdenciários, embora traga agilidade, cria "superfícies de ataque" que podem comprometer a segurança financeira dos segurados. Caruso e Steffen (1999) já alertavam que a segurança da informação deve ser pautada pela confidencialidade, integridade e disponibilidade. Diante da digitalização de mais de 9 milhões de páginas, o risco de exposição tornou-se uma variável crítica que o Estado não pode ignorar.

O objetivo central deste relato é descrever como o IPREV-SC estruturou seu diagnóstico de adequação, superando barreiras culturais para transformar a proteção de dados em uma ferramenta de governança pública moderna. Ao longo deste texto, serão discutidos os procedimentos que permitiram mapear o fluxo do dado e como as reflexões críticas sobre a tensão LAI versus LGPD moldaram uma nova forma de servir ao cidadão catarinense, assegurando que o avanço tecnológico caminhe pari passu com a ética e a proteção aos natura e inalienável dos direitos fundamentais.

No entanto, a adequação tecnológica e normativa, por si só, é insuficiente se não estiver acompanhada de um processo contínuo de conscientização e aculturamento do servidor público. No contexto do IPREV-SC, o servidor atua como a linha de frente do tratamento de dados, sendo o "agente de tratamento" que maneja, diariamente, informações de alta sensibilidade. Como assevera Pinheiro (2020), o elo mais vulnerável de qualquer sistema de segurança da informação não reside nos códigos de programação, mas no comportamento humano. A necessidade de conscientização transcende o mero conhecimento técnico da lei; ela exige a compreensão ética de que o dado pessoal é um prolongamento da personalidade do segurado. Sem um programa de treinamento eficaz que sensibilize o corpo funcional sobre os riscos de acessos indevidos, vazamentos acidentais ou compartilhamentos informais, o instituto permanece exposto a sanções e, sobretudo, ao comprometimento da confiança pública. Portanto, a educação continuada e o desenvolvimento de uma "mentalidade de proteção de dados" são indispensáveis para garantir que o servidor não apenas cumpra uma norma, mas reconheça seu papel como guardião da privacidade do cidadão catarinense (POZZO; MARTINS, 2020).

2 CONTEXTO E REFERENCIAL TEÓRICO

A ação extensionista e de gestão desenvolve-se no cerne do Instituto de Previdência de Santa Catarina (IPREV-SC), autarquia que detém a responsabilidade jurídica e administrativa pela gestão do Regime Próprio de Previdência Social (RPPS) dos servidores estaduais. O contexto institucional do IPREV é caracterizado por um ecossistema informacional de alta complexidade e criticidade, onde o manejo de dados transcende o simples registro administrativo para tornar-se a guarda de um patrimônio biográfico e financeiro dos segurados. Este patrimônio inclui dados biométricos, históricos funcionais detalhados e, primordialmente, registros de saúde originados de perícias médicas e processos de invalidez. Conforme aponta Mendes (2019), o tratamento de dados pessoais pelo Poder Público não encontra justificativa apenas na execução fria de políticas, mas deve estar umbilicalmente vinculado à finalidade pública, à transparência e ao interesse social, respeitando os limites da intervenção estatal na esfera privada.

A base teórica que sustenta esta intervenção fundamenta-se na tridimensionalidade da proteção de dados: a conformidade jurídica (estrita legalidade), a segurança técnica (tecnologia e infraestrutura) e a dimensão ética (valores e cultura). Historicamente, o conceito jurídico de privacidade sofreu mutações profundas, evoluindo do clássico "direito de ser deixado só" (*the right to be let alone*) para o paradigma moderno da autodeterminação informativa. Este novo conceito garante ao cidadão não apenas o sigilo, mas o controle efetivo sobre o fluxo, a correção e o destino de suas informações em posse de terceiros ou do Estado (LIMA; ALMEIDA; MAROSO, 2020). No cenário previdenciário, onde a relação entre segurado e autarquia é assimétrica, esse direito torna-se a garantia de que a vida privada do servidor não será devassada além do estritamente necessário para o ato concessório.

No campo da tecnologia, a Segurança da Informação é aplicada através da tríade clássica CID: Confidencialidade (acesso restrito), Integridade (exatidão dos dados) e Disponibilidade (acesso quando necessário). Como asseveram Caruso e Steffen (1999), a segurança da informação é um processo dinâmico que exige a identificação constante de ameaças e a implementação de salvaguardas que protejam o ativo informacional contra acessos não autorizados ou destruição acidental. Pinheiro (2020) ressalta que a governança pública moderna exige uma transição disruptiva: o Estado deve abandonar o modelo mental de "propriedade do

dado" para adotar um modelo de "custódia responsável". Nesse novo desenho, o IPREV-SC atua como um fiel depositário de informações que pertencem, em última instância, ao titular.

Dessa forma, a implementação da LGPD na autarquia exige a adoção do conceito de *Privacy by Design*. Este princípio determina que a privacidade e a proteção de dados não sejam tratadas como um "acessório" de última hora, mas que sejam integradas organicamente em toda a arquitetura dos sistemas de concessão de benefícios, desde a sua concepção técnica até a interface de atendimento ao usuário. Dada a natureza intrínseca das atividades previdenciárias, o tratamento de Dados Pessoais Sensíveis (conforme definido no Art. 5º, II da LGPD) — que abrangem convicções religiosas, opiniões políticas e, especialmente, informações de saúde — impõe ao instituto um dever de cuidado redobrado e a implementação de medidas técnicas de segurança aptas a prevenir incidentes que poderiam causar danos irreparáveis à honra ou à vida financeira dos segurados (POZZO; MARTINS, 2020).

A eficácia dessa proteção, entretanto, é dependente de uma Gestão Documental robusta. Não há privacidade onde há desordem arquivística. De acordo com Schwaitzer, Nascimento e Costa (2020), a contribuição da gestão de documentos para os programas de conformidade reside na capacidade de mapear o ciclo de vida do dado, permitindo que o IPREV-SC identifique com precisão o que deve ser guardado, por quanto tempo e sob quais condições de sigilo, evitando a acumulação temerária de dados obsoletos que apenas ampliam a superfície de riscos da instituição.

3 PROCEDIMENTOS METODOLÓGICOS / DESCRIÇÃO DAS AÇÕES

A metodologia adotada para a execução desta atividade extensionista fundamentou-se em um estudo de caso indutivo, exploratório e descritivo. De acordo com a literatura metodológica, o método indutivo permitiu que as conclusões fossem construídas a partir da observação direta de premissas particulares no IPREV-SC para a formulação de diretrizes mais amplas de governança. A abordagem foi predominantemente qualitativa, focada na compreensão da relação entre o sujeito (servidor/segurado) e o mundo digital (bases de dados), buscando soluções que não poderiam ser traduzidas meramente em métricas numéricas.

3.1 Caracterização da Pesquisa e Coleta de Dados

A pesquisa concentrou-se no ambiente organizacional do IPREV-SC, em Florianópolis, abrangendo todos os seus setores operacionais e estratégicos. Para a fundamentação teórica e técnica, utilizou-se a pesquisa bibliográfica e documental, analisando livros, artigos, dissertações, teses, além de um arcabouço legal composto por Leis, Normas e Resoluções federais e estaduais.

A coleta de dados empíricos foi realizada através de:

- Entrevistas Semi-estruturadas: Realizadas com os membros da comissão de estudo e implantação da LGPD e com a comissão de gestão documental. Essas entrevistas permitiram diagnosticar a situação real dos fluxos de trabalho e a percepção de risco dos servidores.
- Observação Participante: O desenvolvimento das ações foi conduzido por servidores do próprio IPREV, inseridos no cotidiano do setor, o que facilitou a identificação de "gargalos" nos procedimentos de tratamento da informação.

3.2 Descrição das Ações e Estratégias de Implementação

As ações foram coordenadas de forma interdisciplinar pelas comissões de LGPD e Gestão Documental. O planejamento operacional dividiu-se nas seguintes frentes:

A) Mapeamento do Ciclo de Vida do Dado e Gestão de Processos: A estratégia central foi o mapeamento completo do dado, desde a sua captura inicial até o seu descarte final ou guarda permanente. Isso incluiu a identificação de bases de dados inerentes a recursos humanos, folha de pagamentos e perícias médicas. Foram analisados os sistemas de terceiros e a parceria com o portal GOV.BR, visando garantir que a autenticação dos segurados ocorra sob níveis de segurança "prata" ou "ouro", mitigando riscos de fraudes.

B) Integração com a Gestão Documental e Digitalização: Dada a existência de mais de 8 milhões de documentos físicos, a atividade focou na digitalização e indexação da massa documental utilizando o sistema PIQL/CIASC. Este sistema utiliza tecnologias de OCR (Optical Character Recognition) para permitir a busca automatizada e o controle de acesso granular. As ações incluíram o ajuste das Tabelas de Temporalidade Documental (TTD) para

definir prazos de guarda que variam de 5 anos (formulários bancários) a 95 anos (processos de aposentadoria), conforme as normas do CONARQ e do Estado de Santa Catarina.

C) Diagnóstico de Vulnerabilidades e Infraestrutura Lógica: Foram realizados levantamentos sobre a segurança física (acesso a salas de servidores e arquivos) e lógica (políticas de senhas, permissões de grupo em servidores Windows e uso de certificados digitais). A descrição das ações engloba a revisão de contratos de terceirização para incluir cláusulas de responsabilidade compartilhada no tratamento de dados, conforme as exigências do Art. 13.709/2018.

D) Interação Dialógica e Sensibilização: Para além dos aspectos técnicos, foram desenvolvidas campanhas de sensibilização para promover uma transformação na cultura organizacional. A interação dialógica ocorreu por meio de reuniões entre as áreas jurídica, financeira, tecnológica e de RH, buscando alinhar a eficiência administrativa à proteção dos direitos fundamentais da privacidade dos segurados.

Este conjunto de procedimentos permitiu que o IPREV-SC passasse de uma postura reativa para uma proativa, estabelecendo métricas de auditoria para validar a efetividade das novas políticas de proteção de dados propostas.

4 RESULTADOS E IMPACTOS

Os resultados desta ação extensionista materializaram-se, primeiramente, na estruturação de uma matriz de níveis de sigilo aplicada aos processos previdenciários. Esta classificação permitiu ao IPREV-SC distinguir claramente entre dados de acesso público e dados que exigem camadas de proteção especial, como históricos médicos de perícias e informações socioeconômicas de pensionistas. Um marco fundamental foi a integração das Tabelas de Temporalidade Documental (TTD) com as diretrizes da LGPD; essa convergência garantiu que os prazos de guarda e os métodos de descarte fossem revisados sob a ótica da privacidade, assegurando que dados pessoais não sejam retidos além do período legalmente necessário (SCHWAITZER; NASCIMENTO; COSTA, 2020).

Em termos quantitativos, a iniciativa impactou a governança de um acervo digital massivo, composto por aproximadamente 9 milhões de páginas digitalizadas, o que equivale a uma base superior a cinco Terabytes de dados. A implementação de tecnologias como o sistema PIQL/CIASC e o uso de ferramentas de OCR (Reconhecimento Óptico de Caracteres)

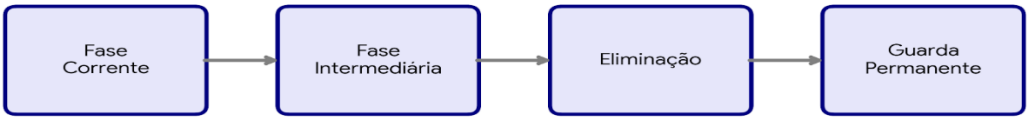
permitiram uma indexação precisa, reduzindo o risco de acessos indevidos e facilitando a auditabilidade do tratamento de dados.

O impacto qualitativo foi observado no aumento da maturidade organizacional. A formalização de critérios rigorosos para o compartilhamento de informações com outros órgãos (interoperabilidade) mitigou riscos jurídicos e fortaleceu a confiança do segurado na instituição. Percebeu-se uma evolução na cultura dos servidores, que passaram a compreender a proteção de dados não como um entrave burocrático, mas como um dever ético e legal.

Por fim, a ação evidenciou a indissociabilidade entre ensino, pesquisa e extensão. A aplicação de conceitos teóricos de governança e *compliance* digital na resolução de problemas reais do instituto permitiu ao corpo técnico e aos envolvidos o desenvolvimento de competências críticas. O projeto transformou o IPREV-SC em um laboratório de práticas modernas de administração pública, resultando em uma gestão mais transparente, segura e centrada na proteção dos direitos fundamentais do cidadão catarinense.

Ciclo de Vida do Dado (LGPD)

Ciclo de Vida Documental (IPREV)



5 DISCUSSÃO E REFLEXÕES CRÍTICAS

A implementação da Lei Geral de Proteção de Dados (LGPD) no Instituto de Previdência de Santa Catarina (IPREV-SC) não se restringiu a uma mera adequação tecnológica; ela revelou um profundo embate conceitual e pragmático com a Lei de Acesso à Informação (LAI – Lei nº 12.527/2011). Este cenário expõe o que a doutrina moderna chama de "tensão de direitos fundamentais": de um lado, o princípio da publicidade e o controle social da administração; de outro, a proteção da personalidade e a autodeterminação informativa (MENDES, 2019).

Enquanto a LAI estabelece a publicidade como regra geral e o sigilo como exceção — visando garantir a transparência necessária para a manutenção do Estado Democrático de Direito — a LGPD impõe limites rigorosos para a proteção dos dados pessoais. No contexto de um órgão previdenciário como o IPREV, essa contraposição não é meramente acadêmica, mas cotidiana. O instituto maneja informações que estão no cerne da vida privada do servidor, como históricos de doenças graves para fins de isenção de imposto de renda ou aposentadoria por invalidez, e dados socioeconômicos de dependentes em processos de pensão por morte (POZZO; MARTINS, 2020).

A reflexão crítica sobre a prática extensionista demonstra que o gestor público enfrenta um "juízo de proporcionalidade" constante. Por exemplo: se a remuneração de um servidor é dado público consolidado pelo STF em nome da transparência, o CID (Classificação Internacional de Doenças) anexado ao seu prontuário previdenciário é um dado pessoal sensível (Art. 5º, II da LGPD) que exige sigilo absoluto. Como bem observam Lima, Almeida e Maroso (2020), a LGPD não veio para anular a LAI, mas para qualificar a transparência: o que deve ser público é o ato administrativo e o gasto, não a intimidade do cidadão-servidor.

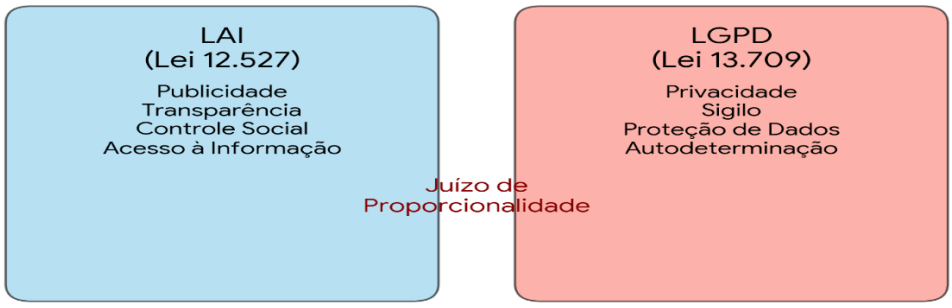
A superação do impasse entre LAI e LGPD no IPREV-SC ocorreu pela adoção estratégica da anonimização. Esta técnica permite que a administração cumpra seu dever de prestar contas sem expor a identidade dos titulares em situações de vulnerabilidade. A reflexão sobre o uso do sistema PIQL/CIASC e da tecnologia OCR evidenciou que a tecnologia deve ser serviente ao Direito. A gestão eletrônica de documentos não serve apenas para "guardar arquivos", mas para garantir que o acesso seja granulado e rastreável, conforme os pilares da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade).

Além disso, a interação com a Comissão de Gestão Documental revelou que a proteção de dados é indissociável da arquivística. Conforme Schwaitzer, Nascimento e Costa (2020), a contribuição da gestão de documentos para programas de adequação à LGPD é o que permite identificar o exato momento em que um dado perde sua finalidade pública e deve ser eliminado, evitando a retenção eterna e o risco de vazamento desnecessário.

Um dos maiores limites encontrados na ação foi a resistência cultural. Muitos setores ainda operam sob a lógica da "posse do processo", ignorando que o verdadeiro proprietário do dado é o segurado. A discussão à luz do referencial teórico indica que a governança pública de dados exige uma mudança de paradigma: a transição de um modelo de burocracia documental para um modelo de governança digital ética.

A interdisciplinaridade mostrou-se vital. A solução dos conflitos entre LAI e LGPD não veio apenas do setor jurídico, mas da colaboração com a TI para criar fluxos de acesso seguro e com o RH para sensibilizar os servidores. Conforme Pinheiro (2020), o compliance digital na administração pública requer que cada agente entenda seu papel como custodiante de direitos alheios. A experiência fortaleceu a interação entre a prática acadêmica (ensino de gestão) e a sociedade (proteção dos segurados), gerando um conhecimento que pode ser replicado em outras autarquias do Estado.

Equilíbrio: Transparência (LAI) vs Privacidade (LGPD)



6 CONSIDERAÇÕES FINAIS

As considerações finais deste relato de extensão buscam sintetizar a complexidade da jornada de adequação do IPREV-SC, reafirmando que a implantação da LGPD é, acima de tudo, um projeto de modernização da cultura administrativa.

A adequação do IPREV-SC à LGPD demonstrou que a proteção de dados na Administração Pública não é um entrave, mas um catalisador de modernização. A principal contribuição deste relato para a área de Administração Pública reside na comprovação de que a gestão de dados sensíveis, quando integrada à gestão documental, fortalece a confiança do cidadão nas instituições. Como destaca Mendes (2019), a autodeterminação informativa é o que permite ao indivíduo deixar de ser um "objeto" do Estado para tornar-se um sujeito ativo no controle de sua biografia digital.

Como recomendações para futuros extensionistas e gestores, destaca-se que a adequação não é um ponto de destino, mas um estado de vigilância constante. O novo paradigma da inovação previdenciária aponta para o uso de Inteligência Artificial (IA) na análise de concessão de benefícios e detecção preditiva de fraudes. No entanto, conforme advertem Pozzo e Martins (2020), a adoção de tecnologias disruptivas e algoritmos no setor público deve ser acompanhada de uma governança ética rigorosa, garantindo a transparência algorítmica e o direito de revisão humana sobre decisões automatizadas que afetem direitos fundamentais.

A continuidade da iniciativa deve focar na automação dos direitos dos titulares (acesso, correção e exclusão) por meio de interfaces inteligentes. A inovação na área de proteção de dados exige o que Pinheiro (2020) classifica como "Segurança 5.0", onde o foco não está apenas na proteção contra invasões, mas na resiliência ética e na capacidade da IA de anonimizar dados em larga escala de forma instantânea. Sugere-se a expansão deste modelo de governança para as demais autarquias do Estado de Santa Catarina, criando uma rede unificada que utilize a IA para monitorar vulnerabilidades em tempo real.

Em última análise, o presente relato reafirma que a implementação da LGPD no Instituto de Previdência de Santa Catarina (IPREV-SC) transcende o mero cumprimento de uma obrigação normativa ou a execução de um checklist de conformidade legal. Ela se consolida como uma poderosa ferramenta de justiça social, pois, no contexto de um regime próprio de previdência, o dado pessoal não é um insumo inerte, mas o registro histórico de uma vida dedicada ao serviço público. Ao garantir que a tecnologia digital atue como um escudo para

proteger a privacidade e não como uma ferramenta para vulnerabilizar o servidor, o instituto estabelece um novo e rigoroso padrão de ética administrativa para o século XXI.

Este novo padrão exige a superação da visão burocrática tradicional em favor de uma governança algorítmica humanizada. A inovação no IPREV-SC, pautada pela responsabilidade e pelo conceito de custódia responsável dos dados (PINHEIRO, 2020), demonstra que é possível conciliar a eficiência operativa da máquina estatal com o respeito absoluto à intimidade. Como observa Mendes (2019), a proteção de dados é o que impede que o cidadão se torne um mero objeto de processamento estatal, devolvendo-lhe a dignidade de ser o senhor de suas próprias informações.

Ademais, a experiência descrita revela que a transformação digital da previdência catarinense é o único caminho viável para uma administração que pretenda ser, simultaneamente, eficiente, digital e profundamente humana. A inovação tecnológica, quando desprovida de uma base ética e de um referencial de proteção aos direitos fundamentais, corre o risco de desumanizar o atendimento e ampliar as desigualdades. Entretanto, ao integrar a LGPD ao ciclo de vida documental e à arquitetura de sistemas (Privacy by Design), o IPREV-SC protege o futuro do segurado, garantindo que o seu histórico de vida esteja seguro contra as incertezas e riscos do ciberespaço (POZZO; MARTINS, 2020).

Portanto, conclui-se que a jornada de adequação aqui relatada serve de paradigma para outras instituições da Administração Pública. Ela prova que a segurança da informação, aliada a uma gestão documental rigorosa e à sensibilização contínua do corpo funcional, é capaz de converter a complexidade da lei em valor público tangível. O IPREV-SC não apenas adequou seus sistemas; ele renovou o seu compromisso ético com os milhares de homens e mulheres que compõem o Estado de Santa Catarina, assegurando que o progresso tecnológico seja sempre acompanhado pelo respeito inalienável aos direitos da personalidade.

BIBLIOGRAFIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2013.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**: Lei de Acesso à Informação. Brasília, DF: Presidência da República, 2011.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**: Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. Ministério da Economia. **Guia de boas práticas para implementação da LGPD na administração pública federal**. Brasília: Governo Digital, 2020.

CARUSO, C. A. A.; STEFFEN, F. D. **Segurança em informática e de informações**. 2. ed. São Paulo: SENAC, 1999.

LIMA, A. P. M. C. de; ALMEIDA, D. de; MAROSO, E. P. **LGPD**: Lei Geral de Proteção de Dados. 1. ed. São Paulo: Literare Books International, 2020.

MENDES, L. S. **Privacidade e proteção de dados pessoais**: a construção do direito à autodeterminação informativa. 2. ed. São Paulo: Saraiva, 2019.

OLIVEIRA, J. E. da S. **Responsabilidade civil dos agentes de proteção de dados no Brasil**. 2019. Trabalho de Conclusão de Curso (Direito) – Universidade Federal da Paraíba, Santa Rita, 2019.

PINHEIRO, P. P. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018. 2. ed. São Paulo: Saraiva, 2020.

POZZO, A. N. D.; MARTINS, R. M. (org.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters, 2020.

ROMA, G. P.; LANGHI, P. J. P. **A ética e o uso de dados sem autorização ou consentimento para benefício próprio**. In: ENCONTRO DE INICIAÇÃO CIENTÍFICA DO CENTRO UNIVERSITÁRIO ANTONIO EUFRÁSIO DE TOLEDO, 16., 2020, Presidente Prudente. Anais [...]. Presidente Prudente: Toledo Prudente, 2020.

SANTA CATARINA. **Decreto Estadual nº 3.486, de 23 de agosto de 2010**. Aprova a Tabela de Temporalidade de Documentos das Atividades-Fim da Administração Pública Estadual. Diário Oficial do Estado, Florianópolis, 23 ago. 2010.

SANTA CATARINA. **Decreto Estadual nº 844, de 18 de setembro de 2020**. Institui o Comitê Gestor de Proteção de Dados Pessoais no âmbito da Administração Pública Estadual. Diário Oficial do Estado, Florianópolis, 2020.

SCHWAITZER, L.; NASCIMENTO, N.; COSTA, A. de S. **Reflexões sobre a contribuição da gestão de documentos para programas de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD)**. Acervo, Rio de Janeiro, v. 33, n. 2, p. 142-165, maio/ago. 2020.