Biblioteca Júlio Teixeira ESA/RS

REVISTA ELETRÔNICA

OAB RIO GRANDE DO SUL ESA

Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

A INTERDISCIPLINARIDADE DA LGPD

THE INTERDISCIPLINARITY OF THE LGPD

Ana Claudia Redecker[1]
Denise Ferreira Ramos Raupp[2]

Resumo: Desde o início da operação da ANPD, é clara a preocupação da entidade em preencher lacunas deixadas pela Lei Geral de Proteção de Dados Pessoais. São várias as publicações já realizadas pela Autoridade, esclarecendo conceitos, papeis e procedimentos para a atuação em segmentos de mercado específicos. Porém, percebendo espaço para discutir a norma sobre outro prisma, este artigo busca trazer uma visão aplicada sobre as boas práticas e a governança abordada pela Lei, a partir de disciplinas fundamentais para sua efetiva implementação: (a) segurança da informação e (b) gestão por processos. É imperativo o entendimento de que ambos os temas serão tratados como ferramentas/instrumentos para o cumprimento dos requisitos jurídicos da norma. Para melhor compreensão do leitor acerca da relação dos conceitos e disciplinas trazidos pela Lei, será feito um breve relato sobre governança. Com o intuito de promover uma visão sistêmica dessa regulação, será apresentado um *Framework* que reúne as disciplinas: Direito, Segurança da Informação e Gestão por Processos.

Palavras-chave: ANPD. Lei Geral de Proteção de Dados Pessoais. Governança. Segurança da Informação.

Abstract: Since the beginning of the operation of the ANPD, it is clear the concern of the entity to fill gaps left by the General Law of Protection of Personal Data. There are several publications already carried out by the Authority, clarifying concepts, roles and procedures for acting in specific market segments. However, perceiving space to discuss the norm from another perspective, this article seeks to bring an applied view on the good practices and governance addressed by the Law, from fundamental disciplines for its effective implementation: (a) information security and (b) management by processes. It is imperative to understand that both topics will be treated as tools/instruments for compliance with the legal requirements of the Law. For a better understanding of the reader about the relationship of the concepts and disciplines brought by the Law, a brief report on governance will be made. In order to promote a systemic view of the standard, a Framework will be presented that brings together the disciplines: Law, Information Security and Process Management.

Keywords: ANPD. General Law of Protection of Personal Data. Governance. Information Security.

[1] Advogada, Professora de cursos de graduação e pós-graduação da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Especialista em Ciências Políticas, Mestre em Direito pela PUCRS.

[2] Discente do curso de Especialização em Direito Digital e Proteção de Dados da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Mestre em Administração Estratégica pela PUCRS. Superintendente de Governança e Compliance do Badesul Agência de Fomento RS.

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB ESA RIO GRANDE DO SUL
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

1 INTRODUÇÃO

A Lei nº 13.709, promulgada em 2018, que dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), entrou em vigor no dia 18 de setembro de 2020. Os artigos que mencionam as sanções a serem aplicadas apenas começaram a vigorar a partir de agosto de 2021.

O texto normativo vai além do estabelecimento de questões jurídicas, impõe, explicitamente, a necessidade da tomada de medidas técnicas e administrativas para com a segurança dos dados pessoais e sugere a adoção de boas práticas e de governança para o efetivo cumprimento legal. Em relação às questões legais, restaram algumas lacunas na Lei que a própria Autoridade Nacional de Proteção de Dados (ANPD) tem buscado esclarecer. Porém, ainda há espaço para dúvidas acerca de uma visão sistêmica sobre a gama de ferramentas e procedimentos a serem adotados em conjunto com os requisitos jurídicos.

Desde sua promulgação a Lei trouxe a figura da ANPD, autarquia formada para a regulação e fiscalização da LGPD. Alguns avanços foram conquistados para a adequada atuação da Autoridade. Dentre suas competências estão: (a) Promover a disseminação de conhecimentos sobre as normas e as políticas públicas relacionadas à proteção de dados pessoais e às medidas de segurança; e (b) Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais (BRASIL, 2022).

É clara a preocupação da ANPD em preencher lacunas deixadas pela Lei. São várias as publicações já realizadas pela Autoridade, esclarecendo conceitos, papeis e procedimentos para a atuação em segmentos de mercado específicos. Algumas Notas Técnicas com encaminhamentos já foram emitidas, o que apoia no entendimento de controladores na aplicação prática da legislação. Porém, percebendo espaço para discutir a norma sobre outro prisma, este artigo busca trazer uma visão aplicada sobre as boas práticas e a governança abordada pela LGPD, a partir de disciplinas fundamentais para sua efetiva implementação: (a) segurança da informação e (b) gestão por processos. É imperativo o entendimento de que ambos os temas serão tratados como ferramentas/instrumentos para o cumprimento dos requisitos jurídicos da Lei. Para melhor compreensão do leitor acerca da relação dos conceitos e disciplinas trazidos pela Lei, será feito um breve relato sobre governança. Com o intuito de

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

promover uma visão sistêmica da norma, será apresentado um Framework que reúne as disciplinas: Direito, Segurança da Informação e Gestão por Processos.

2 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS

A ANPD foi trazida pela Lei nº 13.709/2018, porém, sua criação somente aconteceu na promulgação da Medida Provisória nº 869/2018, convertida na Lei nº 13.853/2019. A operação iniciou, efetivamente, a partir da nomeação do seu primeiro diretor-presidente, em novembro de 2020. Mais adiante, importante conquista ocorreu, não somente para a própria entidade, mas para a sociedade, quando da conversão da Medida Provisória nº 1.124/2022 na Lei nº 14.460/2022, que transforma a ANPD em uma autarquia de natureza especial e, pouco tempo depois, o Decreto nº 11.401/2023, a vinculou ao Ministério da Justiça e Segurança Pública. Este enquadramento na administração federal vai além do que a descentralização[3].

Além disso, ser designada como autarquia em regime especial, lhe confere distinções importantes, como, por exemplo, maior grau de autonomia técnica para execução de competências parajudiciais e a tomada de decisões com maior participação dos administrados (Torres, 2022).

É possível perceber que a ANPD tem atuado na regulamentação de lacunas da LGPD publicando materiais didáticos para consumo de toda sociedade, nos quais se esclarecem conceitos e aplicações. Também pode-se utilizar como referência, as Notas Técnicas publicadas pela Autoridade, quanto aos encaminhamentos por ela ditado em cada um dos casos de análise[4].

3 MAS POR QUE FALAR EM GOVERNANÇA?

A intenção aqui não é discorrer sobre conceitos de governança, tampouco discutir amplamente sobre as intenções do legislador ou sobre a forma como esse conceito foi aplicado. O objetivo é trazer um conhecimento mínimo sobre governança para orientar o leitor sobre as

[3] Ser Autarquia, significa, conforme o Decreto-Lei nº 200/1967, inciso I do seu Art 5º: I – o serviço autônomo, criado por lei, com personalidade jurídica, patrimônio e receita próprios, para executar atividades típicas da Administração Pública, que requeiram, para seu melhor funcionamento, gestão administrativa e financeira descentralizada (Brasil, 2003)

[4] Análises realizadas pela ANPD acessíveis em: Publicações da ANPD — Autoridade Nacional de Proteção de Dados (www.gov.br)

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

disciplinas que serão tratadas com um pouco mais de profundidade (segurança da informação e gestão por processos), permitindo entender a conexão entre todos esses conceitos.

A governança trata, em sua forma mais ampla, da maneira como as organizações conduzem seu conjunto de obrigações para atingimento dos resultados. Empresas que não mantém a mínima ordem, documentação e formalização, não dispõem de governança. Mais do que isso, a governança impõe a necessidade de um tripé: Liderança – visão, objetivo, gestão; Estratégia – como atingir os objetivos, metas, prazos, responsáveis, recursos; e Controle – monitoramento e mensuração (indicadores).

A governança também reflete a necessidade de colegiados e alçadas de decisão para evitar condutas em benefício próprio ao invés do benefício da organização. A partir do momento em que o negócio cresce e mais pessoas têm poder de decisão, para evitar situações de conflito de interesse, deve haver um processo de governança bem estabelecido.

A forma como a governança é trazida na LGPD indica mais a necessidade de organização e visão integrada do que a necessidade de segregação por situação de conflitos de interesse, embora esse risco também seja mitigado com a instauração de governança. Hilb (2009) traz um conceito bastante condizente com essa abordagem: “a Governança Corporativa é como um sistema pelo qual empresas são estrategicamente dirigidas, integrativamente gerenciadas e holisticamente controladas, de forma empreendedora e ética e de maneira apropriada a cada contexto específico”. (Hilb, 2009). O Instituto Brasileiro de Governança Corporativa (IBGC) traz ainda os princípios básicos de Governança Corporativa, que reforçam alguns princípios trazidos pela LGPD: (a)Integridade, (b)Transparência, (c)Equidade, (d)Prestação de Contas (*accountability*), e (e)Sustentabilidade (Responsabilidade Corporativa) (IBGC, 2023).

A LGPD destaca em alguns trechos a importância da governança. É mencionada, pela primeira vez, no Art. 49, em capítulo exclusivo, dedicado a Segurança e Boas Práticas.

No mesmo capítulo, VII – Da Segurança e das Boas Práticas, encontra-se outra seção, Seção II – Das Boas Práticas e da Governança, onde o legislador evidencia a Governança, orientando, inclusive, a implementação de um programa de governança em privacidade. No Art. 50 é perceptível a intenção do legislador em requerer que exista governança nos processos.

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB ESA RIO GRANDE DO SUL
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

A preocupação da ANPD é reforçada na publicação do Regulamento de Dosimetria e Aplicação de Sanções Administrativas, publicado em fevereiro de 2023.

A governança pode ser associada a muitos temas porque expõe a necessidade de uma gestão organizada e transparente acerca do que está sendo tratado. Coube aqui trazer a ideia de governança de dados, visto que o dado pessoal é o objeto central da LGPD. O *Data Governance Institute* traz um conceito para Governança de Dados que vem ao encontro dos princípios da LGPD, pois afirma tratar-se de "um sistema de direitos de decisão e responsabilização por processos relacionados à informação, executado de acordo com modelos acordados que descrevem quem pode tomar quais ações com quais informações e quando, em que circunstâncias, usando quais métodos (DGI, 2003)". Obviamente os princípios da LGPD trazem mais requisitos, mas a governança de dados por si só já estabelece uma série de exigências em relação à gestão de dados.

Por último, mas não menos importante, no Capítulo VIII – Da Fiscalização, fica claro que, caso haja infração cometida pelos agentes de tratamento de dados, a sanção pode ser atenuada caso o agente comprove, em sua defesa, que adota política de boas práticas e de governança em sua organização (Art. 52, § 1º, inciso IX). Essa intenção é ratificada no Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

A partir do exposto sobre governança E sobre os pontos em que a LGPD e o Regulamento de Dosimetria mencionam, este artigo busca trazer a relação e a integração da governança com a segurança da informação e com gestão por processos. Este último não é mencionado em específico na Lei, mas encontra-se no conceito de "boas práticas e de governança", e metodologicamente, é condição básica para a implementação de todos os requisitos por ela instituídos, tornando-se *sine qua non* para o estabelecimento da governança.

4 A SEGURANÇA DA INFORMAÇÃO NA LGPD

A informação constitui um dos ativos mais relevantes para qualquer organização. É a partir da informação que se desenvolve a oferta de produtos ou serviços ou a gestão de recursos. Por este motivo, buscar mecanismos que protejam a informação é essencial.

O Gabinete de Segurança Institucional (GSI) define Informação como sendo "dados, processados ou não, que podem ser utilizados para produção e para transmissão de

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

conhecimento, contidos em qualquer meio, suporte ou formato" (Brasil, 2019). Porém, no mesmo glossário, não é trazido o conceito de dado por si só, que por sua vez, não carrega consigo informação. Um dado isolado não traz a quem o recebe quaisquer informações úteis. O glossário apresenta a definição de Dado Pessoal, "informação relacionada a pessoa natural identificada ou identificável" (Brasil, 2019). Parte-se do pressuposto que, em termos conceituais, o Dado Pessoal iguala-se a Informação (sobre alguém), pois já carrega consigo relação, não sendo mais um dado isolado e sem sentido. Conforme a Norma ABNT NBR ISOIEC 27002-2013, a "Segurança da Informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware". A ABNT NBR ISOIEC 27001-2013, amplia o conceito, trazendo a noção de sistema de gestão:

> "O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados" (ABNT NBR ISOIEC 27001-2013).

Ao buscar referências sobre a relação entre a segurança da informação e a governança, pontua-se este conceito de Guimarães, Souza Neto e Lyra (2018) que, inclusive, categoriza a governança de segurança da informação a partir da governança corporativa:

> "Governança de segurança da informação é o subconjunto da governança corporativa que provê direção estratégica, garante que os objetivos serão atingidos, gerencia riscos apropriadamente, usa os recursos organizacionais com responsabilidade e monitora o sucesso ou falhas do programa de segurança institucional". (Isaca, 2015, *apud*, Guimarães, Souza Neto E Lyra, 2018, p.92)

Este conceito vem ao encontro do que foi tratado no capítulo 2, sobre a governança como uma abordagem sistêmica e integradora, do cuidado dos responsáveis com o processo de ponta-a-ponta.

Minimamente esclarecidos os conceitos de segurança da informação e governança, o *Framework* buscará incorporar os pontos da LGPD que evidenciam essa relação.

5 A GESTÃO POR PROCESSOS NA LGPD

De forma simplista, para apoiar na construção do que este artigo busca entregar ao leitor (o *Framework*), serão trazidos os seguintes conceitos: processo, gestão por processo e governança em processo.

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB ESA RIO GRANDE DO SUL
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

Partindo do básico, toda ação executada a partir de etapas, pode ser considerada um processo. Desde as coisas mais simples do dia a dia de uma pessoa até situações mais complexas das organizações. Muitos conceitos e relações misturam-se nesse contexto: processo, rotina, hábito, etapa, cultura, passos, etapas, ações e assim por diante. Nesse sentido:

> "Processo é o título dado a uma série de atividades/objeto, transformando entradas (*inputs*) em saídas/produtos (*outputs*), de modo a atribuir determinado grau (tangível) de agregação de valor. Um processo deve necessariamente começar e terminar em outro processo ou em um dos seis clientes externos (obrigatório, cliente final, cliente intermediário, fornecedor, sociedade e monitorador) " (Pavani Junior e Scucuglia, 2011).

Seja qual for o negócio de uma empresa, não há operação sem a execução de processo. Pode ser que os processos não estejam descritos, mas eles existem. À medida que as empresas entendem a importância de conhecer seus processos para que seja possível gerenciá-los, inicia a gestão da empresa por meio de seus processos e não por decisões sem fundamento. A gestão por processo evolve entender os processos, priorizá-los com base na agregação de valor ao cliente e a mensuração dos seus resultados. O CBOK 4.0 conceitua Gerenciamento de Processo de Negócio (*Business Process Management* – BPM) como:

> "uma abordagem de gerenciamento disciplinada para identificar, projetar, executar, documentar, medir, monitorar e controlar processos de negócio, tanto automatizados como não automatizados, para alcançar resultados consistentes e direcionados, alinhados aos objetivos estratégicos da organização. O BPM envolve a definição deliberada, colaborativa e, cada vez mais assistida, por tecnologia, melhoria, inovação e gerenciamento de processos de negócio de ponta a ponta que direcionam resultados de negócio, criam valor para os clientes e permitem que uma organização atinja seus objetivos de negócio com mais agilidade" (Kirchmer, Scarsig e Frantz, 2020).

Não é à toa que a LGPD chama muito a atenção para "as boas práticas e governança". Foi muito assertivo aproximar a necessidade de governança na aplicação da Lei, pois são os mecanismos de governança que se relacionam com os princípios e os requisitos trazidos pela LGPD. Conforme o CBOK 4.0, as responsabilidades típicas da Governança de Processo incluem:

> "Definir princípios, práticas e padrões do Gerenciamento de Processo de Negócio;
> Garantir que os princípios, práticas e padrões do Gerenciamento de Processo de Negócio sejam escaláveis no escopo atual e escopo futuro da implementação do Gerenciamento de Processo de Negócio;
> Fornecer orientação, mentoria e treinamento sobre as melhores práticas e padrões, reforçando a conformidade a eles (Kirchmer, Scarsig e Frantz, 2020).

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB ESA RIO GRANDE DO SUL
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

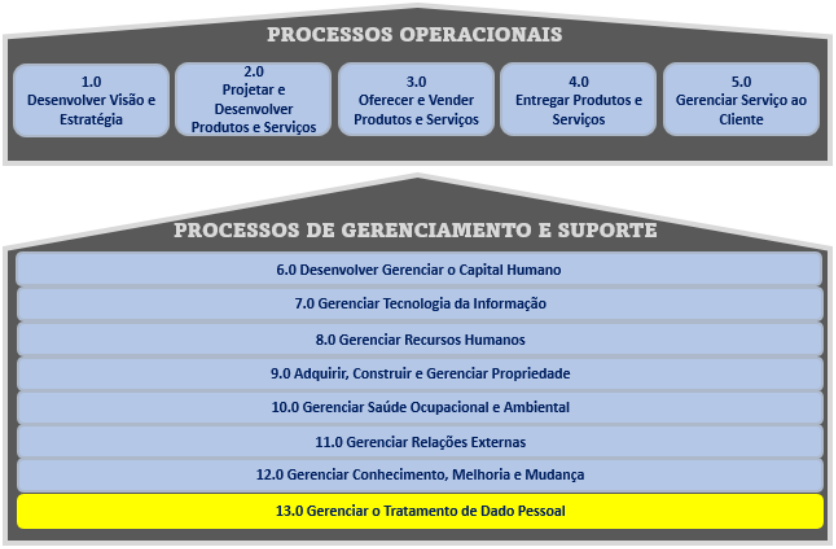
Vale a pena lembrar que a ANPD, ao definir "políticas de boas práticas e de governança" no regulamento sobre dosimetria, traz a necessidade de normas e de processos internos para garantir o cumprimento à Lei.

A Figura a seguir, adaptada do Framework APQC (CBOK 4.0), traz uma sugestão para inclusão do processo de gestão de tratamento de dados pessoais na arquitetura de processos das organizações: "Gerenciar o tratamento de Dados Pessoal". Esse processo é transversal, ou seja, as atividades inerentes a este processo devem considerar todos os outros processos da organização onde haja Dado Pessoal e Dado Pessoal Sensível.

É altamente recomendável que o gerenciamento desse processo seja realizado ou, ao menos, muito bem conhecido pelo Encarregado de Dados, pois para atender as atividades sob responsabilidade de quem ocupa esse papel na empresa, é primordial entender de maneira sistemática toda operação com Dado Pessoal.

Conforme o § 2º do Art. 44 da Lei, além de ser o contato principal para os titulares de dados e para a ANDP, procedendo com as solicitações e interações, o Encarregado deve "orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais". Dessa forma, o Encarregado deverá ser a referência sobre todas as etapas do processo relativo ao tratamento de dados pessoais e sua proteção, implicando no conhecimento amplo sobre tais questões.

Figura 1 – Framework APQC (CBOK 4.0) – Adaptado por nós.



Fonte: As autoras (2024) adaptado de Guia para gerenciamento de processos de negócios corpo comum de conhecimento: BPM CBOK 4.0 (Kirchmer, Scarsig e Frantz) (2020, 127).

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

Pela construção conceitual e relacional realizada até aqui, é possível sugerir que a governança traz os mecanismos necessários para a adequada gestão de quaisquer conteúdos, no âmbito deste artigo, o atendimento à LGPD no que diz respeito aos requisitos de Segurança da Informação e de Gestão dos Processos.

6 *FRAMEWORK*: A INTERDISCIPLINARIDADE DA LGPD

A partir da construção conceitual e relacional trazida anteriormente, pretende-se que o leitor alcance um mínimo entendimento para dispor da visão holística e integradora que o *Framework* tenta sistematizar. Para orientar a interpretação e o entendimento do *Framework*, importante algumas considerações e esclarecimentos prévios:

a) O *Framework* considera apenas dados em meio digital;

b) As atividades de "coleta", "atualização", "arquivamento", "compartilhamento" fazem parte do "armazenamento" dos dados pessoais pelo controlador;

c) Foram trazidos alguns elementos simbólicos para facilitar, visualmente, a identificação e diferenciação de alguns conceitos, portanto:

A cor azul escuro sempre irá se referir à Processo

A cor azul claro sempre irá se referir à Segurança da Informação

A cor vermelha sempre irá se referir às matérias de Direito

d) Da mesma forma, utilizou-se pequenos círculos coloridos, na tentativa de sugerir quais Princípios[5] (Art. 6º da Lei nº 13.709/2018) devem ser atendidos em cada etapa de tratamento dos dados pessoais, considerando os instrumentos jurídicos também recomendados para essas atividades, portanto:

e) Para relacionar os instrumentos de tecnologia da informação necessários à segurança da informação com as atividades do processo de tratamento de dados pessoais, foi utilizado o

[5] os princípios: segurança e prevenção, foram tratados em conjunto por utilizarem o mesmo tipo de instrumento de tecnologia da informação e das matérias de direito.

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

símbolo . Cada número representa uma das atividades de tratamento de dados pessoais. Portanto, os instrumentos de segurança da informação poderão ter um ou mais números associados a eles.

f) Deve-se considerar que a base para todo o processo se estabelece a partir da Lei Geral de Proteção de Dados Pessoais;

g) Importante alertar que o processo de gerenciamento de tratamento de dados pessoais depende do contexto organizacional no qual está inserido, ou seja, cada negócio dispõe de suas formas de operar, o que impacta na maneira de gerenciar o tratamento de dados pessoais.

h) Considera-se que o ROPA (*Recording of Processing Activities*, em português, Registro das Operações de Tratamento) e o RIPD (Relatório de Impacto de Dados Pessoais) devam conter a descrição detalhada do tratamento de dados pessoais, considerando, no mínimo, esses elementos apresentados.

Figura 2 - Framework A Interdisciplinaridade da LGPD

Fonte: As autoras (2024)

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

6.1 As Relações do Framework

A explicação das relações do *Framework* será apresentada a partir das atividades de tratamento de dados pessoais, demonstrando quais instrumentos do direito e de tecnologia da informação são sugeridos para o efetivo atendimento das exigências da Lei.

Destaca-se que, para toda operação, independentemente da atividade ou da etapa do ciclo de vida do dado pessoal, é imprescindível dispor de Segurança de Rede, são serviços imprescindíveis para a segurança da informação.

Os serviços de segurança de rede, realizados por equipamentos de tecnologia complexa, inclusive IA, com apoio de pessoas para análise das situações alertadas por tais equipamentos, são requeridos para identificar ameaças ao ambiente computacional das organizações. Isso inclui o monitoramento do padrão de comportamento dos usuários em rede, permitindo que anomalias no comportamento sejam detectadas como ameaça.

6.1.1 Coleta

Na etapa do processo “coleta”, a LGPD exige que o controlador aja de maneira transparente, não somente ao coletar, mas com todo o ciclo de vida do tratamento dos dados pessoais.

No “Termo de Uso” ou no “Aviso de Privacidade” é importante que os princípios da Finalidade, Necessidade e Adequação estejam claramente descritos e que os procedimentos da organização atentem para o princípio da “Não Discriminação” do titular.

Para a coleta respaldada por Hipótese de Tratamento “Consentimento”, é obrigatório haver um processo de gestão desses consentimentos, ou seja, é imperativo identificar quais foram os titulares que consentiram o tratamento dos dados e quais não consentiram. Além disso, o consentimento é revogável a qualquer tempo, dessa forma, a organização deve dispor de mecanismos para essa pronta revogação e que ela seja efetivamente aplicada nos procedimentos internos para não haver infração da Lei nesse ponto.

São ferramentas de tecnologia da informação: (a) Softwares que apoiam na gestão do consentimento – são essenciais neste processo, principalmente aqueles que proporcionam uma interface de fácil acesso ao titular para realizar a revogação; (b) Integração entre os bancos de dados do controlador e operadores também se torna imprescindível para que as informações sejam atualizadas automaticamente; (c) Software para Gestão Eletrônica de Documentos

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

(GED) – esse tipo de tecnologia permite a elaboração de formulários eletrônicos com todos os campos indexados. Permite que sejam marcados os campos cujos dados são informados por consentimento ou não, para que, de forma automática, não sejam mais utilizados para determinados processos da organização. Ex.: publicidade. Além da gestão do consentimento, o GED possibilita o controle de acesso e de compartilhamento de dados, ou seja, determinados usuários podem ter acesso a determinados dados e outros não; e, (d) Softwares para Gestão de Identidade – muitos serviços têm ocorrido de maneira completamente digital e independente de pessoas para intermediar. Dessa forma, ferramentas que confirmam a identidade dos titulares têm sido cada vez mais imprescindíveis para detecção e mitigação de fraudes.

6.1.2 Classificação

A Lei de Acesso à Informação, Lei nº 12.527/2011 já dispunha do regulamento para acesso à informação previsto na Constituição Federal, inclusive já apresentava em seu inciso IV do Art. 3º, a definição de "Informação pessoal: aquela relacionada à pessoa natural identificada ou identificável". Tal regulamento apresenta classificações possíveis para as informações produzidas pelos órgãos e entidades públicas no que diz respeito à negativa de acesso à informação aos cidadãos, além do prazo em que elas podem estar respaldadas por essa classificação.

Dentro deste contexto, pode-se estabelecer uma analogia com os dados pessoais e dados pessoais sensíveis, que se tornam mais uma "informação" a ser classificada e ter previsão para tempo de tratamento. No âmbito da gestão do processo, os instrumentos de tecnologia da informação e, provavelmente, os instrumentos do direito, poderão ser "aproveitados" para atender as duas leis ou, no mínimo, não poderão entrar em conflito.

As empresas públicas já devem dispor de Política de Divulgação de Informações, na qual definem quais tipos de informações estão classificadas em quais níveis de sigilo. Além disso, devem elaborar a Tabela de Temporalidade, na qual informam o prazo de guarda de cada informação e se ela pode ser eliminada ou não. Dessa forma, sugere-se incluir, de forma transversal, na Tabela de Temporalidade, em quais informações (documentos), estão presentes dados pessoais ou dados pessoais sensíveis, apoiando o controlador na identificação de quanto tempo é necessário armazenar tais dados ou proceder com o descarte.

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

O Software para Gestão Eletrônica de Documentos (GED) cujo objetivo é cumprir com o previsto na legislação no que diz respeito à classificação, é ferramenta de tecnologia da informação. É primordial dispor de GED, que, habitualmente, possuem as funcionalidades de classificação quanto ao grau de sigilo e quanto ao prazo, além de emitir alertas sobre esses prazos para encaminhamentos necessários (decidir manter ou eliminar).

6.1.3 Atualização

A atualização dos dados pessoais é tanto um direito do titular quanto um interesse do controlador, principalmente quando se trata de dados de contato. Alguns segmentos, têm a obrigação de manter os dados dos clientes atualizados, é o caso de todos aqueles enquadrados como "pessoas obrigadas", conforme a Lei nº 9.613/1998, que dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores.

A necessidade de atualização deve estar clara no Termo de Uso assinado pelo titular e, a depender da situação, nos instrumentos jurídicos que acordam a relação entre as partes. São ferramentas de tecnologia da informação: (a) Software para Gestão Eletrônica de Documentos (GED) – conforme já descrito para os procedimentos anteriores, o GED é fundamental para alertas sobre prazos, inclusive sobre prazos para atualização cadastral; e (b) Software para Gestão de Identidade/Software para Controle de Acesso – sempre que for oferecida a possibilidade de autosserviço, ou seja, do próprio titular realizar procedimento de forma digital, é importante garantir que o acesso e as alterações estão sendo realizadas pelo próprio titular e não por terceiros não autorizados, pois corre-se o risco de compartilhar dados pessoais sem autorização do titular.

6.1.4 Arquivamento

O arquivamento pode ser entendido como uma ação intermediária das empresas para aqueles dados que não estão mais sendo utilizados na operação, mas ainda exigem um prazo de guarda para respaldo à alguma obrigação legal. Dessa forma, podem (e devem) ser mantidos em nível de acesso mais restrito e de forma igualmente segura.

No arquivamento é importante instituir um Protocolo de Arquivamento, um "resumo" dos dados que estão sendo reservados/apartados da operação do negócio. São ferramentas de tecnologia da informação: (a) Software para Gestão Eletrônica de Documentos (GED) – para

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

este caso, o GED pode apoiar, inclusive, na salvaguarda e gerenciamento dos Protocolos de Arquivamento; e (b) Técnicas de Pseudo Anonimização – esse tipo de técnica permite que os dados sejam parcialmente ocultados, aplica-se para que, em casos de acesso indevido, não seja possível identificar os dados. Porém, o detentor do dado, deve possuir a chave para retornar o dado ao estado original.

6.1.5 Compartilhamento

Nos casos de compartilhamento de dados pessoais com operadores ou parceiros de negócio, são muitos os instrumentos do direito e de tecnologia da informação necessários, visto o risco de violação, tanto do direito do titular em saber com quem seus dados estão sendo compartilhados quanto à exposição indevida dos dados.

É de extrema importância o cuidado com as cláusulas em instrumentos que acordam relação entre as partes que estão compartilhando dados pessoais, como contratos, termos de parceria, convênios etc. É necessário ficar claro o papel de cada um dos agentes e suas responsabilidades. Para o titular, é imprescindível a transparência, ou seja, por meio de Avisos de Privacidade, ele pode ser atualizado sobre novos compartilhamentos anteriormente não descritos na Política de Privacidade ou no Termo de Uso. Isso para que ele tenha condições de exercer o direito de decisão sobre seus dados pessoais.

Neste procedimento, todos os instrumentos de tecnologia de informação apresentados no *Framework* são necessários para a segurança e gestão dos dados pessoais. Destaca-se: (a) Técnicas de Pseudo Anonimização – conforme já descrito, essa técnica permite que apenas as partes autorizadas tenham acesso ao dado pessoal identificável. Normalmente se usa a criptografia. Meios de comunicação utilizam essa técnica para segurança das informações compartilhadas, como o WhatsApp, por exemplo; e, (b) Segurança de Rede – uma das ferramentas para segurança de rede, o VPN (*Virtual Private Network*) mitiga o acesso de pessoas não autorizadas a dados que estão navegando na internet. Ou seja, ao trafegar dados via VPN, o risco de expor os dados à usuário não autorizado está mitigado.

6.1.6 Transferência

A transferência de dados pessoais consiste em concedê-los para outro controlador. A LGPD inclui o conceito de “transferência” na atividade de tratamento “compartilhamento”, o

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

que leva ao entendimento de que o controlador original poderia manter os dados sob sua guarda. Para não haver confusão entre a aplicação prática das atividades de tratamento "compartilhamento" e "transferência", aconselha-se considerar que, ao transferir os dados pessoais a outro controlador, a manutenção da guarda dos dados apenas se justificariam pelas mesmas hipóteses previstas no Art. 16 da LGPD.

Neste caso, os dados estariam sendo armazenados pelo controlador de origem que transferiu os dados a outro controlador para qualquer outra atividade de tratamento. Ratifica-se que, qualquer das hipóteses, deve ter sido formalmente avisada ao titular no momento da coleta e, se for o caso, consentida.

6. 2 Descarte

O final do ciclo de vida dos dados pessoais ocorre no descarte. O controlador deve eliminar todo e qualquer dado livre de obrigação de armazenamento. Para isso é importante ter bem definida a classificação e temporalidade dos dados pessoais. O Art. 15 da LGPD apresenta as hipóteses para o término do tratamento de dados pessoais.

O Protocolo de Descarte é importante para que o controlador tenha a informação sobre o tratamento dados pessoais de determinado titular por determinado período. Sugere-se manter o registro apenas do CPF para tal identificação. A Tabela de Temporalidade apoia no controle do prazo para eliminação dos dados a serem descartados.

Para essa etapa, o fundamental é manter o controle sobre o que e quando descartar, além da gestão do Protocolo de Descarte. O Software para Gestão Eletrônica de Documentos (GED) é a ferramenta de tecnologia da informação. Além disso, para este caso, novamente o GED é indicado para a salvaguarda e gerenciamento dos Protocolos de Arquivamento.

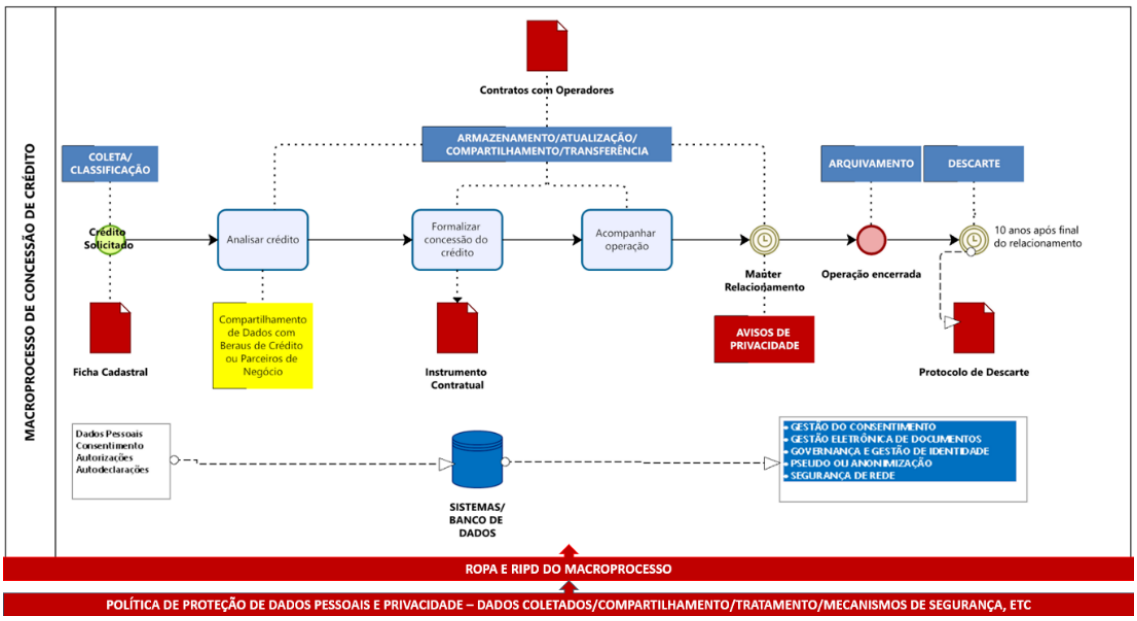
6. 3 Visão de um processo de negócio

O Framework apresenta as relações entre as atividades de tratamento, os instrumentos do direito e os de tecnologia da informação para apoiar na governança do processo de tratamento de dados pessoais. Porém, para demonstrar que esse é, de fato, um processo de gerenciamento transversal aos processos de negócio, exemplifica-se a seguir a dinâmica dessas relações na governança de um processo de negócio.

REVISTA ELETRÔNICA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

No exemplo, consta um macroprocesso de concessão de crédito, em linhas bem genéricas, contando somente com o "caminho feliz", ou seja, sem ramificações ou caminhos alternativos.

Figura 3 - Caminho Feliz do Macroprocesso de Concessão de Crédito



Fonte: As Autoras (2024)

Destaca-se a importância do ROPA (Registro das Atividades de Tratamento, em português) e do RIPD (Relatório de Impacto aos Dados Pessoais, em português) na figura 3. Nesses instrumentos deverá ser descrito o processo de gerenciamento de tratamento de dados pessoais "dentro" do processo de negócio. Ou seja, cada processo de negócio deverá constar no ROPA e no RIPD com a abordagem do processo de gerenciamento tratamento de dados pessoais.

Por sua vez, na Política de Proteção de Dados Pessoais e Privacidade, deverá constar todos os elementos pertinentes às atividades de tratamento, de forma clara, objetiva e completa para o perfeito entendimento do titular dos dados pessoais.

7 CONCLUSÕES

Este artigo buscou trazer uma visão aplicada sobre as boas práticas e a governança abordada pela Lei, a partir de disciplinas fundamentais para sua efetiva implementação: (a)

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB ESA RIO GRANDE DO SUL
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

segurança da informação e (b) gestão por processos. É importante ratificar que as relações e sugestões apresentadas são exemplificativas, não tendo a pretensão de abranger todos os conteúdos disciplinares envolvidos na LGPD, tampouco todas as ferramentas disponíveis para sua implementação. A ideia foi trazer uma abordagem aplicada da Lei, considerando as disciplinas trazidas pelo legislador.

O *Framework* para ser aplicado em organizações de segmento específico, requer que se verifique a aplicabilidade e adaptações relevantes de acordo com o contexto. Outra sugestão seria expor o Framework à especialistas de processos e de segurança da informação para complementação.

Realizar essa pesquisa apresentou-se bastante interessante, visto a dificuldade vivenciada por muitas pessoas no início da implementação da LGPD. As diferentes tecnologias que já existiam e as que surgiram para atender as exigências da Lei no que diz respeito à segurança da informação trazem muitas dúvidas sobre a aplicação. O *Framework* traz uma tentativa de organizar a aplicação das exigências de cunho jurídico, de gestão de processo e de tecnologia que se apresentam durante a jornada de aprendizagem na implantação do processo de gerenciamento do tratamento de dados pessoais.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Decreto nº 11.401, de 23 de janeiro de 2023**. Dispõe sobre a vinculação das entidades da administração pública federal indireta. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/Decreto/D11401.htm. Aceso em: 15 maio 2024.

BRASIL. **Decreto-Lei nº 200, de 25 de fevereiro de 1967**. Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Brasília, DF: Presidência da República, 2003. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm. Acesso em 20 maio 2024.

BRASIL. **Glossário de Segurança da Informação.** Imprensa Nacional, 2019. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em 01 maio 2024.

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2022. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 5 março 2024.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF. Presidência da República, 2019. Disponível em https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 29 abril 2024.

BRASIL. **Portaria nº 93, de 26 de setembro de 2019**. Aprova o Glossário de Segurança da Informação. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 29 abril 2024.

BRASIL. **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023**. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, DF: Presidência da República, 2023. Disponível em https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em 03 maio 2024.

GUIMARÃES, Rogério. SOUZA NETO, João. LYRA, Maurício Rocha. Modelo de Governança de Segurança da Informação para a Administração Pública Federal. **Perspectivas em Gestão & Conhecimento**, João Pessoa, PB, v. 8, n. 3, p. 90-109, set/dez. 2018. DOI: https://doi.org/10.21714/2236-417X2018v8n3. Disponível em: https://periodicos.ufpb.br/index.php/pgc/article/view/34717/21768. Acesso em 2 de maio 2024.

HILB, Martin. **A Nova Governança Corporativa**: ferramentas bem-sucedidas para conselho de administração. 1 ed. São Paulo: Saint Paul, 2009.

IBGC. **Código das Melhores Práticas de Governança Corporativa**. 5 ed. São Paulo: Instituto Brasileiro de Governança Corporativa, 2023.

IDG. Defining Data Governance. Data Governance Institute, 2007. Disponível em: http://datagovernance.com/defining-data-governance . Acesso em 30 abril 2024.

KIRCHMER, Mathias. SCARSIG, Marc. FRANTZ, Pater. **Guia para o gerenciamento de processos de negócios corpo comum de conhecimento:** BPM CBOK 4.0. Tradução Valéria Mendonça de Albuquerque Mello. 1 ed. Brasília: ABPMP Brasil, 2020.

Biblioteca Júlio Teixeira ESA/RS
REVISTA ELETRÔNICA
OAB RIO GRANDE DO SUL ESA
Volume 15 – Número 1 (2024) - Porto Alegre/RS – Brasil
ISSN 2595-4598

MENEZES, Karina. **Gestão de identidade e acessos (IAM): o que é, por que adotar na sua empresa e principais ferramentas**. IdBlog, 2020. Disponível em: https://blog.idwall.co/gestao-de-identidade-e-acessos-iam/#penci-Provedor-de-identidade-IdP. Acesso em 01 maio 2024.

PAVANI JÚNIO, Orlando. SCUCUGLIA, Rafael. **Mapeamento e Gestão por Processos – BPM.** 1. ed. São Paulo: M. Books do Brasil Editora Ltda., 2011.

TORRES, Isabella Macedo. **Autoridade Nacional de Proteção de Dados**: Análise de competências e funcionamento a partir da definição da natureza jurídica. 2022. Dissertação (Mestrado em Direito Constitucional) – Programa de Pós-Graduação Stricto Sensu, Faculdade de Direito, Universidade Federal Fluminense, Niterói, 2022. Disponível em: https://ppgdc.uff.br/wp-content/uploads/sites/681/2023/01/ISABELLA-MACEDO.pdf . Acesso em: 2 maio 2024.