ANÁLISE DAS PRÁTICAS DE TRATAMENTO DE DADOS SOB A ÓTICA DA LEI GERAL DE PROTEÇÃO DE DADOS NO CONTEXTO JURÍDICO BRASILEIRO PARA PROFISSIONAIS DE TECNOLOGIA DA INFORMAÇÃO

Luís Augusto Izeppi Braga[20]
Camila Leonardo Nandi de Albuquerque[21]

RESUMO

O presente artigo aborda as boas práticas e desafios enfrentados pelas empresas brasileiras de tecnologia da informação na realização do tratamento de dados, à luz da Lei Geral de Proteção de Dados (LGPD). O objetivo é investigar as práticas de tratamento dos dados utilizados por essas empresas brasileiras, seguindo as diretrizes estabelecidas pela LGPD. Para atingir esse propósito, serão apresentados, inicialmente, os conceitos, fundamentos e princípios necessários para o completo entendimento do tema relacionado à proteção de dados pessoais. Será conduzido um estudo sobre diferentes formas de tratamento de dados, incluindo anonimização e pseudo minimização, que estejam em conformidade com as diretrizes da LGPD. Isso visa contextualizar as modalidades de tratamento e processamento de dados, bem como sua adequação às disposições legais vigentes. Na sequência, busca-se contextualizar as formas de tratamento de dados, identificando as principais barreiras técnicas e jurídicas enfrentadas pelas empresas brasileiras durante a implementação dos métodos para tratamento dos dados sob sua responsabilidade. Por fim, serão apontadas soluções e estratégias de boas práticas que podem ser aplicadas pelas empresas para garantir a conformidade com a LGPD e a proteção efetiva da privacidade do titular dos dados. O método empregado na pesquisa é o levantamento bibliográfico, tendo como base a legislação e a doutrina pertinentes. O método de abordagem utilizado é o indutivo, que envolve chegar a conclusões com base em padrões e observações.

Palavras-chaves: Lei Geral de Proteção de Dados. Dados Sensíveis. Tratamento de dados. Conformidade. Privacidade. Boas práticas.

1 INTRODUÇÃO

Com o crescimento da digitalização e as diversas formas de comunicação entre os mais variados sistemas computacionais, têm surgido uma imensidão de dados que podem ser utilizados para tomada de decisões e desenvolvimento de tecnologias inovadoras em diversas áreas. Contudo, essa quantidade escalar de informações coletadas, além de seu

[20]Graduado em Ciência da Computação pela Unisul (2010). Especialista em Gestão de Projetos pelo Senac (2012). Graduado em Direito pelo Centro Universitário Univinte (2023). Engenheiro de Software. E-mail: luisaugustobraga@gmail.com. Lattes iD: http://lattes.cnpq.br/3194093388861263

[21] Graduada em Direito pela Unisul (2013). Especialista em Direito Empresarial pela Verbo Jurídico/Uniasselvi (2015). Mestre em Desenvolvimento Regional pela UnC (2019). Mestre em Direito pela Unesc (2021). Advogada (OAB/SC 39.114). E-mail: camilanandi_@hotmail.com. Lattes iD: http://lattes.cnpq.br/7317604500646001. ORCID iD: https://orcid.org/0000-0003-3466-6209

valor significativo para o entendimento do comportamento humano, traz consigo grandes desafios relacionados à privacidade e proteção de dados pessoais dos indivíduos.

O objetivo principal deste artigo é investigar as práticas de tratamento de dados armazenados utilizadas pelas empresas brasileiras de tecnologia à luz das diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD) . Em consonância com esse objetivo, busca-se identificar os desafios inerentes a essas práticas, bem como as estratégias adotadas por essas empresas para garantir conformidade com as exigências legais visando à preservação da privacidade dos dados pessoais dos cidadãos presentes nessas bases.

Os objetivos específicos definidos para esta pesquisa abrangem três áreas fundamentais. Primeiramente, realizar um estudo das diferentes formas de tratamento de dados que estejam em conformidade com as diretrizes da LGPD, bem como sua adequação às disposições legais vigentes. Em seguida, contextualizar as formas de tratamento de dados, concentrando-se nos métodos de tratamento e implementação da LGPD em empresas de tecnologia. Durante essa etapa, espera-se identificar e compreender as barreiras enfrentadas, que podem variar desde a adaptação das estruturas tecnológicas até a compreensão das exigências legais contidas na LGPD. Por fim, este trabalho avaliará as medidas adotadas pelas empresas para garantir a conformidade com a LGPD e a proteção efetiva da privacidade dos dados.

No decorrer deste artigo, serão explorados os pontos centrais delineados nesta introdução, permitindo uma análise das práticas de tratamento de dados sob a perspectiva da LGPD. A discussão e as conclusões resultantes dessa análise contribuirão para uma compreensão mais aprofundada das complexidades envolvidas nesse processo, além de enriquecer o debate sobre a proteção dos dados pessoais no contexto jurídico brasileiro.

2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Sancionada em 14 de agosto de 2018, a Lei nº 13.709/18 surgiu para regulamentar a manipulação de dados pessoais no Brasil. Seu objetivo é garantir a transparência, privacidade e proteção das informações de pessoas físicas.

A LGPD foi sancionada sob a influência do Regulamento Geral sobre a Proteção de Dados (GDPR), que entrou em vigor em 25 de maio de 2018 e é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e no Espaço Econômico Europeu. Sobre o que a GDPR

visa proteger:

> Basicamente, a principal preocupação é com a privacidade das pessoas e o cuidado com a segurança dos dados armazenados. Dessa maneira, a empresa não pode armazenar nenhuma informação que possa identificar um usuário sem o consentimento. Entre essas informações estão: cookies; informações pessoais; e-mail; endereço IP; comportamento de navegação; registros médicos; dados biométricos. (BRASIL, HSC, 2019)

Embora a LGPD e a GDPR sejam leis sancionadas em países diferentes, muito se assemelham, pois ambas buscam a imposição de controle rigoroso sobre a obtenção, processamento, compartilhamento e segurança dos dados.

No Brasil, conforme estabelecido pela Lei nº 14.010/20, as sanções previstas na LGPD passaram a vigorar a partir de 1º de agosto de 2021 e, para garantir a efetividade da lei, o Governo Federal criou a Autoridade Nacional de Proteção de Dados (ANPD), um órgão fiscalizador da Presidência da República.

> A Autoridade Nacional de Proteção de Dados fomentará a construção de uma cultura forte de proteção de dados pessoais no Brasil, por meio de ações de comunicação que permitam ao cidadão o acesso aos seus direitos como titular de dados pessoais, buscando sempre incentivar a aproximação com os cidadãos e a participação popular nos debates sobre o tema, na elaboração de normativos e no processo de fiscalização da adequação à Lei Geral de Proteção de Dados Pessoais. (BRASIL, ANPD, 2023, p. 23)

A ANPD é uma autarquia de natureza especial, uma entidade pública criada por lei para exercer atividades específicas de interesse público que requerem autonomia funcional, administrativa e financeira. Está vinculada ao Ministério da Justiça e Segurança Pública, com finalidade específica, possuindo maior autonomia em relação às autarquias comuns.

Sobre a ANPD, consideramos que “[...] é o grau máximo, hierarquicamente, na esfera administrativa da Lei Geral de Proteção de Dados. Este fator não elimina o poder de fiscalização de outros órgãos, apenas define as suas competências” (COMPUGRAF, 2019, p. 20).

Antes da criação da LGPD, os dados pessoais eram protegidos por diversas leis, cada uma com suas próprias diretrizes, como a Constituição Federal (artigo 5º, X, Direito à Privacidade), Código do Consumidor (Lei nº 9.613/1998), Acesso à Informação (Lei nº 12.527/2011), Crimes Cibernéticos (Lei nº 12.737/2012) e Marco Civil da Internet (Lei nº 12.965/2014).

Certamente, o sancionamento da LGPD representou um marco significativo, uma vez que é a primeira legislação no Brasil a focar diretamente na proteção da privacidade e

segurança dos dados pessoais, tratando-os como propriedade do titular e garantindo os direitos ao mesmo.

Com isso, a LGPD tornou-se uma centralizadora, estabelecendo padrões claros e exigências para o tratamento de dados pessoais por parte das organizações, o que reflete a crescente importância atribuída à proteção dos dados na era digital.

2.1 FUNDAMENTOS E PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD estabelece diversas possibilidades e formas para o tratamento de dados pessoais, sendo que cada uma está vinculada a requisitos legais específicos. Essas especificidades estão relacionadas à possibilidade ou forma de tratamento de dados pessoais e podem variar conforme a finalidade e o contexto do tratamento.

A seguir, são apresentados os fundamentos gerais sobre os requisitos legais para as diferentes formas de tratamento de dados, conforme o artigo 2º da LGPD.

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

Não há hierarquia entre os fundamentos; ambos trabalham de forma igualitária, buscando a proteção dos dados pessoais dos titulares.

A legislação, ao incluir a expressão “proteção de dados” em seu título, instiga a reflexão sobre os tipos de dados que ela aborda.

O artigo 5º da LGPD é referido como o “artigo das definições fundamentais”, onde são apresentadas as diversas definições.

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; [...]. (BRASIL, 2018)

Comumente, o ciclo de todo o processo se inicia com o recebimento, tratamento, armazenamento e descarte dos dados. Conforme seguem as definições.

> Recebimento de dados: É importante questionar a necessidade dos dados recebidos, já que muitas vezes são sensíveis e requerem atenção especial para garantir segurança e anonimização adequadas. Evite coletar dados desnecessários.
> Tratamento de dados: O tratamento de dados começa com quatro personagens fundamentais no processo, que são: titular, controlador, operador e encarregado.
> Armazenamento de dados: Garantir a disponibilidade dos dados é essencial para permitir o acesso quando necessário. Para isso, é importante ter um plano de armazenamento adequado. Seguindo as orientações do TCU, o armazenamento em nuvem pode ser uma opção viável, pois esses ambientes já oferecem diversas garantias de segurança.
> Descarte de dados: Quando o ciclo de operação dos dados se encerra será necessário descartar os dados, porém esse processo precisa de uma atenção especial. O titular precisa ser informado, de preferência lá no início (processo de captação do dado), qual o prazo que os dados estarão em posse do controlador. (GUILHEN, 2022, p. 38)

Definidas as etapas de recebimento, tratamento, armazenamento e descarte de dados, chega o momento de conhecer os personagens fundamentais no processo. Todos os personagens estão descritos no artigo 5º da LGPD e são:

> Art. 5º Para os fins desta Lei, considera-se: [...]
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador; [...] (BRASIL, 2018)

Ainda sobre o artigo 5º, X, LGPD, o tratamento de dados é definido como toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O artigo 6º da LGPD estabelece os princípios que orientam as práticas relacionadas ao tratamento de dados pessoais no Brasil, além dos fundamentos. Esses princípios fundamentais servem de orientação para boas práticas e condutas no tratamento de dados. Facilmente percebe-se que "boa-fé" e "consentimento" são palavras-chave do contexto, onde o titular do dado deverá ser abordado de forma

explícita, clara e correta para poder autorizar, tendo a liberdade para aceitar ou recusar o uso de suas informações pessoais por parte de terceiros.

Conforme o artigo 7º da LGPD, seguem os requisitos para o tratamento:

> Art. 7º O tratamento de dados pessoais somente poderá se dar nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018)

A coleta de dados se dará mediante o consentimento pelo titular — a menos que exista base legal para o tratamento — conforme o artigo 7º, I, da LGPD. Em consonância com o artigo 7º, II, da LGPD, a coleta deve ser para o cumprimento de obrigação legal ou regulatória pelo controlador e deve ser exposta ao titular de maneira clara. Uma vez que o titular deu consentimento e compreendeu a finalidade, a coleta deve ser limitada ao mínimo necessário para a realização de suas finalidades, com base no princípio da necessidade conforme artigo 6º, III, da LGPD.

Guilhen (2022, p. 81) ressalta que a Administração Pública poderá utilizar-se de todas e empresas privadas só poderão utilizar o termo de consentimento. Um resumo das bases legais que poderão ser utilizadas para o tratamento de dados no estágio de adoção da LGPD conforme a seguir:

- Base Legal:

a. Obrigação legal ou regulatória: Dados e dados sensíveis;

b. Interesse legítimo da administração: Somente dados;

c. Execução de políticas públicas: Dados e dados sensíveis;

d. Termo de Consentimento: Dados e dados sensíveis.

Essas são as diretrizes gerais sobre a coleta, armazenamento e tratamento de dados pessoais e dados pessoais sensíveis. É importante ressaltar que a LGPD prevê várias bases legais para o tratamento de dados, como execução de contratos, cumprimento de obrigação legal, exercício regular de direitos e o legítimo interesse do controlador. Mesmo existindo diversas bases legais, todas as possibilidades serão moldadas conforme a necessidade, ampliando o rol de requisitos específicos dependendo do contexto dos dados envolvidos.

2.2 SANÇÕES PREVISTAS PELA LGPD

As sanções previstas pela LGPD são aplicáveis em caso de descumprimento das disposições previstas no artigo 52º, 53º e 54º da LGPD.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração; [...]
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. [...]
> Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. [...]
> Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.
> Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. (BRASIL, 2018)

Como observado, as sanções podem incluir advertências, multas que podem chegar a até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração, publicidade da infração após devidamente apurada e confirmada a ocorrência, bloqueio ou eliminação dos dados pessoais relacionados à infração, entre outras medidas que

visam garantir conformidade.

Logo, é de extrema importância que as empresas estejam cientes de suas obrigações legais e adotem as medidas necessárias para garantir a conformidade com a legislação em estudo, a fim de evitar as possíveis sanções citadas.

3 DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

Os dados pessoais são divididos em **dados pessoais** e **dados pessoais sensíveis**, além da consideração sobre **dado anonimizado** na LGPD:

> O dado pessoal é considerado como toda informação associada a uma pessoa identificada ou identificável. Temos como exemplo de dados pessoais: nome, endereço residencial, endereço do correio eletrônico, número de celular, CPF, entre outros. Já os dados pessoais sensíveis são os dados capazes de gerar qualquer tipo de discriminação, como origem racial, etnia, opinião política, crenças religiosas, vida sexual, dados relacionados à saúde, entre outros. Há também os dados anonimizados, que são relacionados ao titular que não pode ser identificado. Esse dado não é considerado dado pessoal para a aplicabilidade da LGPD, à exceção de quando o processo de anonimização for revertido para fins de pesquisa e estatística. (CRUZ, 2021, p. 34)

É possível perceber que a diferença entre os tipos de dados está na natureza das informações. Dados pessoais sensíveis estão relacionados a informações “íntimas” e merecem uma proteção maior devido ao seu potencial impacto na privacidade e na vida do titular.

Com base no artigo 11º da LGPD, a coleta de dados sensíveis, como informações sobre saúde, orientação sexual e convicções religiosas, requer o consentimento explícito do titular, de forma específica e destacada para o tratamento dos mesmos. Fica evidenciado que um dado pessoal poderá se tornar um dado pessoal sensível, dependendo das circunstâncias.

3.1 ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO PARA PROTEÇÃO DE DADOS

Para Machado e Leão (2020, p. 8), “dados anonimizados são aqueles cujos titulares não podem ser identificados, dada a aplicação de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento". Para os efeitos da Lei, dado anonimizado não é dado pessoal”. Portanto, dados anonimizados são dados processados de tal forma que não é possível identificar seu titular, mesmo com o uso de meios técnicos razoáveis disponíveis na época.

Ainda de acordo com Machado e Leão (2020, p. 8), “dados pseudonimizados são aqueles dados que, submetidos a tratamento, não oferecem a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro”.

Fica explícito que dados pseudonimizados são dados que foram submetidos a um processo que os torna não diretamente associados a um indivíduo sem o uso de informações adicionais mantidas separadamente e de forma segura pelo controlador dos dados. Ou seja, ainda é possível associar os dados a um indivíduo, mas apenas se você tiver acesso à informação adicional mantida de forma segura pelo controlador.

É importante notar que, por conta da irreversibilidade do processo de anonimização, os dados anonimizados não estão sujeitos à aplicação da LGPD. No entanto, se houver a possibilidade de reverter o processo de anonimização e identificar os titulares, então esses dados serão tratados como dados pessoais e estariam sujeitos às proteções previstas na LGPD.

Considerando o caput do art. 6º da LGPD, onde estabelece que “as atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios [...]” (BRASIL, 2018), é importante ressaltar que todas as definições apresentadas até o momento estão diretamente ligadas ao tratamento de dados.

Portanto, a segurança dos dados será assegurada por meio de técnicas como criptografia, *hash*, autenticação e outras, que devem ser implementadas para controlar e proteger o acesso às informações.

4 DESAFIOS NA IMPLANTAÇÃO DA LGPD NAS EMPRESAS DE TECNOLOGIA

Dado o impacto das mudanças normativas e os diversos avanços tecnológicos sobre as organizações, torna-se crucial compreender os procedimentos, estratégias e desafios associados à LGPD no contexto das empresas de tecnologia.

A seguir, apresenta-se uma estrutura sequencial que se acredita ser a abordagem mais eficaz para a conformidade com a LGPD.

a) Criar o comitê para análises e decisões;

b) Definir um DPO (Oficial de proteção de dados);

c) Mapear e entender o ciclo de vida dos dados;

d) Adotar regulamentações e padrões de segurança da informação;

e) Auditar e monitorar o ambiente de contexto;

f) Criar relatório de impacto à proteção de dados pessoais (RIPD);

g) Criar plano de ação para emergência.

4.1 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

O RIPD ou *Data Protection Impact Assessment* (DPIA) é um documento de valor legal e deve detalhar todos os processos de tratamento pelos quais os dados pessoais passam durante o seu ciclo de vida. Donda explana que:

> O RIPD também conhecido como Data Protection Impact Assessment (DPIA) é um documento de valor legal e deve detalhar todos os processos de tratamento pelos quais os dados pessoais passam durante o seu ciclo de vida. Ele deve conter os riscos e controles de segurança aplicados. Ou seja, é um documento que exibe um panorama do tratamento de dados na sua empresa, e a criação desse documento pode ajudar a identificar pontos de atenção no processo de conformidade. (DONDA, 2020, p. 30)

A criação do RIPD, além de ser uma obrigação legal, ajudará a garantir que todos os requisitos legais estejam sendo cumpridos pela organização e pode ser iniciado em paralelo ao processo de conformidade dos processos internos.

O relatório de impacto à proteção de dados pessoais (RIPD) poderá ser solicitado ao controlador a qualquer momento pela autoridade nacional, com base no parágrafo 3º do artigo 10º da LGPD.

Tal relatório faz a diferença frente a ANPD no momento de avaliação de um incidente ou uma auditoria para decidir como aplicará as possíveis penalidades previstas no artigo 52º da LGPD.

Segundo Donda (2020, p. 127), “se a empresa adotar e documentar no relatório as boas práticas de segurança aplicadas e as medidas de correção adotadas de forma bem esclarecida, terá uma oportunidade de defesa mais forte e com base sólida”.

4.2 ANÁLISE E AVALIAÇÃO DE RISCOS

As tratativas sobre segurança e as boas práticas aparecem no capítulo VII, artigo 46º da LGPD e a política de segurança é item fundamental. O risco está associado ao potencial de que ameaças possam explorar vulnerabilidades de um ou grupo de ativos de informação e, consequentemente, causar dano.

> Dentre muitas definições o risco é uma condição existente, em uma organização ele sempre está presente acompanhado de fatores, tais fatores influenciam o risco de maneira positiva ou negativa. É importante saber que o risco é uma possibilidade, situação que difere ao perigo, pois, perigo é a origem de uma perda. Portanto, na análise e avaliação de riscos, os fatores e os próprios riscos devem ser tratados para que os perigos não se concretizem. (PIAZZA, 2015, p. 4)

Para identificar, analisar e avaliar os riscos, existe a NBR ISO/IEC 27005, que trata sobre segurança da informação, segurança cibernética e proteção à privacidade, fornecendo orientações para gestão de riscos de segurança da informação.

Todos os órgãos fiscalizadores e a ANPD poderão solicitar documentos para compreender como a gestão dos dados é realizada. O principal documento é o de Política de Segurança da Informação (PSI), além do plano de tratamento de dados.

4.3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Uma vez mapeados os riscos (analisados e avaliados), é chegada a hora de criar a política de segurança da informação. Para que isso seja possível, é necessário elencar a lista com as regras e objetivos claros, além do apoio de toda a organização.

A PSI precisa de ampla divulgação para que se tenha sucesso na aplicação, do comprometimento de todos e da publicação de um documento contendo as regras e a aprovação da alta gestão da organização.

O artigo 50º da LGPD aborda boas práticas e governança dos dados:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018)

O fato de conhecer as ameaças relacionadas ao tema é essencial para que o mapeamento de riscos seja realizado de maneira certeira. Só assim será possível adotar a medida mais eficaz contra a ameaça detectada.

Conhecendo as ameaças, chega-se ao momento de gerenciá-las. De acordo com Donda (2020, p. 92), “o gerenciamento de vulnerabilidade é a prática que permite identificar, classificar, corrigir e mitigar vulnerabilidades”. Para isso, é necessário conhecimento das tecnologias envolvidas e, em determinados casos, o uso de sistemas especializados em gerenciamento de vulnerabilidades.

Quando se trata de vulnerabilidade, podemos considerar hardwares, softwares, redes de computadores, pessoas e ambientes físicos. Portanto, adotar boas práticas de gerenciamento de vulnerabilidades permite detectar e mitigar eventuais falhas antes que

possam ser exploradas.

4.4 FINALIZAÇÃO DO CICLO DE TRATAMENTO DE DADOS

Chega-se ao momento de “término do tratamento de dados”. Esse assunto gera dúvidas sobre por quanto tempo é possível armazenar os dados pessoais. Contudo, não há uma resposta certeira para esse questionamento, uma vez que cada organização detém sua política para o consumo dos dados. Como boa prática, uma vez que os dados coletados não são mais necessários, o ideal é eliminá-los. Lembrando que essa informação deverá estar clara para o titular dos dados no momento da solicitação de consentimento. Os artigos 15º e 16º da LGPD apresentam as orientações para o termo.

Em suma, a eliminação de dados é um processo simples, mas exige atenção quando existe a necessidade de descarte de equipamentos físicos. Do ponto de vista da segurança da informação, deve-se ter certeza de que os dados foram eliminados de maneira que não permita que pessoas de má-fé possam recuperar as informações eliminadas, comprometendo a privacidade dos titulares. Sendo assim, é importante conhecer os métodos e formas ideais para a eliminação de dados.

4.5 DESAFIOS PARA AS EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO

A implementação da LGPD é obrigatória e de relevante importância para todas as empresas no Brasil, independentemente de porte e setor. No contexto deste artigo, o foco são as empresas de tecnologia e os principais desafios enfrentados no processo de adequação, bem como as soluções para alcançar a conformidade com a lei em estudo e para Reis:

> A Lei Geral de Proteção de Dados (LGPD) entrou em vigor em setembro de 2020, mas ainda é comum encontrar empresas brasileiras que não estão devidamente adaptadas às exigências legais. Essa realidade é preocupante, pois as empresas que não seguem as normas podem sofrer penalidades financeiras significativas, perder a confiança de seus clientes e até mesmo enfrentar processos judiciais. (REIS, 2023)

Em aspectos gerais, a falta de conscientização, ainda hoje, é um dos maiores desafios em relação à implantação da LGPD. Muitos desconhecem as implicações da lei e os riscos de não realizar as conformidades da lei.

A falta de conscientização vai ao encontro da ausência de treinamentos aos colaboradores por parte dos empregadores aderentes à LGPD. De nada adianta a

aderência à LGPD se a cultura empresarial não for revisada periodicamente. Sem treinamentos adequados, torna-se praticamente nula a compreensão dos colaboradores em relação à proteção de dados.

Segundo Kiyohara (2019), o processo de adequação à LGPD começa com um diagnóstico: “é fundamental entender qual o estágio atual da organização em termos de gestão da privacidade, mapear quais os dados pessoais utilizados e onde eles estão. A avaliação deve considerar três pilares: legal, tecnologia da informação e gestão de processos”.

Outro fato identificado como um desafio é a falta de investimento em cibersegurança, pois uma empresa que não dispõe das ferramentas adequadas para a proteção fica suscetível a violações da privacidade e vazamentos de dados.

Quando tratamos de desafios, intrinsecamente os custos entram nesse escopo. Uma vez que a adequação à lei exige investimento em tecnologias, pessoas qualificadas, treinamentos, etc. Dependendo da quantidade de dados coletados e tratados, os custos podem ser exponenciais para garantir conformidade junto à LGPD.

Algumas abordagens que impactam diretamente o setor de tecnologia da informação estão relacionadas à produção de informações e à construção de infraestruturas robustas, escaláveis e seguras, uma vez que há necessidade de garantia da segurança dos dados; transparência no processo de coleta e consumo dos dados; confiabilidade das informações; definição das ferramentas a serem utilizadas; capacitação de profissionais para o desenvolvimento de habilidades; mudança na captura, armazenamento e análise de dados.

Além de adotar novas práticas, reestruturar as políticas internas e por vezes criar setores, é essencial que a empresa também revise e mantenha seus equipamentos de tecnologia atualizados, pois isso é crucial para assegurar o bom funcionamento e proporcionar segurança aos dados, uma vez que é por meio da tecnologia que as informações são armazenadas, processadas e transmitidas.

É crucial também dedicar recursos ao aprimoramento dos profissionais envolvidos na adequação, pois serão responsáveis por uma área sujeita à fiscalização das autoridades. É fundamental que estejam plenamente conscientes das mudanças que ocorrerão em suas atividades rotineiras, a fim de prevenir erros e possíveis contratempos futuros.

Lisboa e Takano, no estudo realizado pela Logicalis, o tradicional *IT Trends Snapshot*, apuraram o retrato atual das movimentações do mercado de TI no Brasil, além da antecipação de tendências. Segundo o estudo, o tema de LGPD como prioridade das

áreas de TI caiu de 51% para 8% entre as edições de 2021 e 2023. Entretanto, apenas 36% dos respondentes indicaram total aderência à LGPD.

> As questões relacionadas à privacidade e à gestão de dados vêm amadurecendo gradualmente. Prova disso é a redução da proporção de respondentes que afirmam que não têm iniciativas específicas. Em 2019 este índice era de 41%, em 2021 esse número cai para 12% e, neste ano, chega a 6%. Além disso, o índice de empresas que já estão totalmente aderentes à LGPD deu um salto expressivo de 11% em 2021 para 36% em 2022. Ainda assim, grande parcela das empresas (43%) continua na fase de adoção, com iniciativas concretas de implementação. (LISBOA; TAKANO, 2023, p. 15)

Ainda sobre o estudo, os entrevistados apontaram três desafios principais na adaptação à LGPD: a adequação de processos e sistemas (26%), o engajamento de usuários e colaboradores (18%) e a segurança de dados (17%).

Ao realizar a implementação de toda nova estrutura no modelo de negócio, caberá ao Encarregado de Proteção de Dados ou DPO (*Data Protection Officer*) realizar a gestão, controle e manutenção dos fluxos e processos da empresa. Pois o importante não é apenas aplicar os métodos necessários para o cumprimento das exigências legais, mas também manter toda a operação em conformidade.

3 METODOLOGIA

A metodologia empregada para alcançar os objetivos propostos neste trabalho baseia-se na abordagem indutiva, por meio de um levantamento bibliográfico que se fundamenta nas legislações e doutrinas vigentes. Isso permitirá a produção de conteúdo com base nos padrões observados e nas melhores práticas identificadas no contexto da conformidade com a LGPD e na proteção da privacidade dos dados.

4 CONCLUSÃO

Nesse artigo, exploraram-se os desafios enfrentados pela área de Tecnologia da Informação na implementação da Lei Geral de Proteção de Dados (LGPD). Analisamos a importância da conformidade com a LGPD para empresas de tecnologia, uma vez que são as principais responsáveis por lidar com uma vasta quantidade de dados sensíveis diariamente, cujo potencial de crescimento é exponencial nesse mundo cada vez mais digitalizado.

O objetivo do artigo foi examinar de forma abrangente a LGPD, apontando explicitamente seus princípios, fundamentos, referências, legislações antecessoras e

autoridades reguladoras. Relatou-se que a LGPD foi um marco para o Brasil, uma vez que passou a ser uma lei centralizadora do contexto de coleta, armazenamento e tratamento de dados no país, definindo regras, boas práticas e sanções por descumprimento.

Destacou-se o conceito de dados e seus tipos. Diferenciar e entender que dado pessoal é diferente de dado pessoal sensível, mas que por vezes esse dado pessoal poderá se tornar um dado pessoal sensível dependendo do cenário de consumo é imprescindível para se trabalhar com esta lei.

Quando se busca técnicas para o tratamento de dados, muitas são encontradas, contudo, para o artigo apontamos as mais comuns no âmbito de tratamento de dados para a conformidade da LGPD e que comumente geram dúvidas nos envolvidos. Trata-se da anonimização e pseudonimização, palavras estas que fogem do comum, mas que geralmente fazem parte da política de segurança da informação de uma determinada empresa.

Identificou-se que a conformidade com a LGPD na área de TI é uma tarefa complexa devido à natureza heterogênea e distribuída das infraestruturas tecnológicas, exigindo do profissional envolvido uma gama elevada de conhecimento para que se consiga trabalhar com os dados utilizando sempre medidas de segurança aprimoradas para a proteção de dados sensíveis, além de toda documentação e política de segurança associada.

A conscientização e treinamento de colaboradores na área de TI são essenciais. De nada adiantará a construção de políticas rigorosas de segurança, sistemas computacionais incríveis se a cultura empresarial não estiver alinhada com os objetivos da LGPD. Neste ponto, foi evidenciada a necessidade de constante conscientização e treinamentos contínuos dos profissionais de TI, além das revisões e atualizações periódicas das infraestruturas tecnológicas, para só assim, garantir a segurança e eficácia da gestão dos dados pessoais.

A análise ofereceu uma visão dos desafios da TI na conformidade com a LGPD e apresentou os primeiros passos para adequação à lei, fornecendo insumos para o leitor, independentemente de sua ocupação profissional. É importante ressaltar que a complexidade e a dinâmica do cenário tecnológico apresentam variações específicas para cada organização.

Ao superar os obstáculos com determinação e implementar melhores práticas, a TI não apenas atende às exigências legais, mas também contribui para a construção de um ambiente digital mais seguro e confiável para todos os envolvidos.

Nota-se um amadurecimento no cenário brasileiro perante uma lei considerada “nova” por muitas interpretações. Fica evidente que para a adequação satisfatória à Lei, as empresas de TI devem estabelecer áreas de tecnologia bem estruturadas. É imperativo que equipes técnicas assumam a responsabilidade pelo gerenciamento da infraestrutura, pelos processos técnicos de tratamento de dados e pela constante busca por novas soluções, sempre com foco na segurança da informação.

Em última análise, a LGPD é um passo essencial em direção a um futuro digital mais ético e responsável. À medida que enfrentam os desafios com resiliência e inovação, as empresas de tecnologia não apenas cumprem um dever legal, mas também se destacam como pilares de confiança e integridade na era da informação.

REFERÊNCIAS

AGENCIA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS (ANPD). **Guia Orientativo: Tratamento de Dados Pessoais pelo Poder Público**. Versão 01, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 10 set. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO 27005:2019:** Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação da informação. Rio de Janeiro: ABNT, 2019. Disponível em: https://dokumen.pub/abnt-nbr-iso-iec-270052019-tecnologia-da-informaao-tecnicas-de-segurana-gestao-de-riscos-de-segurana-da-informaao-abnt-nbr-iso-iec-270052019-3nbsped-9788507082958.html. Acesso em: 15 out. 2023.

BRASIL, Autoridade Nacional de Proteção de Dados (ANPD). **Política de comunicação Social**. 1. ed. Brasília, Distrito Federal: 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/anpd-pol-comunicacao-2023-1.pdf. Acesso em: 8 out. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Emendas Constitucionais de Revisão. Brasília, 5 de outubro de 1988. Disponível em: http://www.planal-to.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 out. 2023.

BRASIL, HSC. **O que é GDPR e o que muda para as empresas e os brasileiros?** Abril, 2019. Disponível em: https://www.hscbrasil.com.br/gdpr. Acesso em: 8 out. 2023.

BRASIL. **Lei nº 9.613, de 3 de março de 1998.** Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Brasília, 3 de março de 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 31 de ago. de 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, 18 de novembro de 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 31 de ago. de 2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, 30 de novembro de 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 31 de ago. de 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e

deveres para o uso da Internet no Brasil. Brasília, 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 de ago. de 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 de ago. de 2023.

BRASIL. **Lei nº 14.010, de 10 de junho de 2020.** Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14010.htm#view. Acesso em: 31 de ago. de 2023.

BRASIL. Ministério Público Federal. **Lei Geral de Proteção de Dados:** Fundamentos e princípios. Disponível em: https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd/fundamentos-e-principios. Acesso em: 16 set. 2023.

COMPUGRAF. **Guia de implementação da LGPD:** Passo a passo para adequar sua empresa. São Paulo/SP: 2019. Disponível em: http://. Acesso em: 3 nov. 2023.

CRUZ, Uniran Lemos da; PASSAROTO, Matheus; JUNIOR, Nauro Thomaz. O Impacto da Lei Geral de Proteção de Dados Pessoais (LGPD) nos Escritórios de Contabilidade. **ConTexto,** Porto Alegre, v. 21, n. 49, p. 30-39, set./dez. 2021.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. **Reuters,** San Francisco, out., 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G. Acesso em: 16 set. 2023.

DONDA, Daniel. **Guia prático de implementação da LGPD**. 1 ed. São Paulo: Labrador, 2020. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 01 nov. 2023.

GUILHEN, Bruno Anselmo. **Como implementar a LGPD:** bases, mecanismos e processos. Fundação Escola Nacional de Administração Público. Brasília: Enap, 2022.

KIYOHARA, J. **A importância do PMO na adequação a LGPD**. Disponível em: https://lexprime.com.br/2019/09/a-importancia-do-pmo-na-adequacao-a-lgpd. Acesso em: 18 out. 2023.

LISBOA, Sofia; TAKANO, Yassuki. **IT Trends Snapshot 2023:** Um panorama da adoção de tecnologia no mercado brasileiro. Logicalis: 2023. Disponível em: https://imagine.la.logicalis.com/hubfs/IT%20Snapshot%202023/it-trends-snapshot-2023_logicalis.pdf. Acesso em: 06 nov. 2023.

MACHADO, Ulysses Alves de Levy; LEÃO, Paulo Roberto Correa. **Fundamentos da LGPD.** 2020. Curso desenvolvido pelo Serpro - Serviço Federal de Processamento de Dados em parceria com a Escola Nacional de Administração Pública - Enap. Disponível em: https://www.escolavirtual.gov.br. Acesso em: 30 out. 2023.

PIAZZA, Maurício R. **Norma ABNT NBR ISO/IEC 27.005:** Gestão de Riscos da Segurança da Informação como base para a Gestão de Riscos Corporativos. 2015. Disponível em: https://prevenirperdas.com.br/portal/meus-videos/item/download/171_b1a0fc962ecf7f4472decb7effc4df66. Acesso em: 05 out. 2023.

REIS, Beatriz de Felippe; GRAMINHO, Vivian Maria Caxambu. **A inteligência artificial no recrutamento de trabalhadores:** o caso Amazon analisado sob a ótica dos direitos fundamentais. XVI Seminário Internacional: Demandas sociais e políticas públicas na sociedade contemporânea - XII Mostra Internacional de Trabalhos Científicos, 2019. Disponível em: https://online.unisc.br/acadnet/anais/index.php/sidspp/article/download/19599/1192612314. Acesso em: 16 set. 2023.

REIS, Rafael. **Os desafios da implementação da LGPD em empresas brasileiras**. Maio, 2023. Disponível em: https://www.direitoempresarial.com.br/os-desafios-da-implementacao-da-lgpd-em-empresas-brasileiras. Acesso em: 05 nov. 2023.