UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
CAMPUS DE CHAPECÓ
CURSO DE CIÊNCIA DA COMPUTAÇÃO

MICHEL FELIPE WELTER

IDENTIFICAÇÃO DE PRÁTICAS PARA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS APLICADAS AO DESENVOLVIMENTO DE SOFTWARE

CHAPECÓ
2023

MICHEL FELIPE WELTER

IDENTIFICAÇÃO DE PRÁTICAS PARA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS APLICADAS AO DESENVOLVIMENTO DE SOFTWARE

Trabalho de conclusão de curso apresentado como requisito para obtenção do grau de Bacharel em Ciência da Computação da Universidade Federal da Fronteira Sul.
Orientador: Prof. Dra. Raquel Aparecida Pegoraro

CHAPECÓ
2023

Welter, Michel Felipe

Identificação de Práticas para Implementação da Lei Geral de Proteção de Dados Aplicadas ao Desenvolvimento de Software / Michel Felipe Welter. – 2023.
60 f.: il.

Orientador: Prof. Dra. Raquel Aparecida Pegoraro.
Trabalho de conclusão de curso (graduação) – Universidade Federal da Fronteira Sul, curso de Ciência da Computação, Chapecó, SC, 2023.

1. LGPD. 2. Desenvolvimento de software. 3. Segurança de dados. I. Pegoraro, Prof. Dra. Raquel Aparecida, orientador. II. Universidade Federal da Fronteira Sul. III. Título.

E-mail: michelfelipew@gmail.com

MICHEL FELIPE WELTER

IDENTIFICAÇÃO DE PRÁTICAS PARA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS APLICADAS AO DESENVOLVIMENTO DE SOFTWARE

Trabalho de conclusão de curso apresentado como requisito para obtenção do grau de Bacharel em Ciência da Computação da Universidade Federal da Fronteira Sul.

Orientador: Prof. Dra. Raquel Aparecida Pegoraro

Este trabalho de conclusão de curso foi defendido e aprovado pela banca avaliadora em: 11/2/2023.

BANCA AVALIADORA

Prof. Dra. Raquel Aparecida Pegoraro – UFFS

Prof. Dr. Braulio Adriano de Mello – UFFS

Profa. Me. Andressa Sebben – UFFS

RESUMO

Com o processo de globalização, o desenvolvimento de novas tecnologias e a fácil circulação dos dados na internet, a sociedade mundial culminou em diversos questionamentos éticos acerca dos dados compartilhados. No Brasil, criou-se em 2018 a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709) que dispõe sobre o tratamento de dados pessoais, inclusive por meios digitais, por pessoa natural ou jurídica. Ao longo do tempo, foram divulgados diversos casos de violação e da má preservação dos dados pessoais. A LGPD surge com o objetivo de assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais, impondo penalidades às empresas e instituições que não cumprem com seus requisitos. Entre as empresas mais afetadas estão as empresas de desenvolvimento de software que necessitam adequar os seus processos e alterar os seus softwares para se adequarem à lei . Neste contexto, esse trabalho teve como objetivo apresentar um conjunto de práticas por princípio que podem ser aplicadas em empresas de desenvolvimento de software para implementação da LGPD.

Palavras-chave: LGPD. Desenvolvimento de software. Segurança de dados.

ABSTRACT

With the globalization process, the development of new technologies and the easy circulation of data on the internet, world society culminated in several ethical questions about shared data. In Brazil, the General Law for the Protection of Personal Data (Law No. 13,709) was created in 2018, which provides for the processing of personal data, including by digital means, by natural or legal persons. Over time, several cases of violation and poor preservation of personal data have been reported. The LGPD arises with the objective of ensuring the right to privacy and protection of users' personal data, through transparent and safe practices, guaranteeing fundamental rights, imposing penalties on companies and institutions that do not comply with its requirements. Among the companies most affected are software development companies that need to adapt their processes and change their software to comply with the law. In this context, this work aimed to present a set of practices by principle that can be applied in software development companies for the implementation of the LGPD.

Keywords: LGPD. Software development. Data security

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

1.1 APRESENTAÇÃO

A privacidade digital é uma recente demanda da sociedade. Assim como a privacidade física, no lar ou em conversas reservadas, é um valor essencial, também a privacidade digital se tornou um desejo da sociedade moderna (22).

Para Pinheiro (39) A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

A lei, criada em 14 de agosto de 2018, tem 65 artigos e foi alterada pela Medida Provisória 869/2018 e pela Lei n. 13.853/2019. Por ser a lei mais específica e exclusiva sobre o tema é que a LGPD tem principal relevância e inova ao criar sanções direcionadas, além de uma governança que inclui um novo órgão da presidência da República. Qualquer empresa, organização, instituição pública ou privada que coleta ou que utiliza dados de pessoas físicas precisa se adaptar a ela (22).

A LGPD estabelece normas e regras rigorosas para a proteção de dados pessoais, regulamentando seu tratamento, definido como qualquer ação realizada desde a coleta, cópia, edição, armazenamento, publicação, impressão, transmissão, processamento e compartilhamento de dados pessoais (31).

Como principais objetivos, a LGPD visa fortalecer o direito à privacidade dos titulares de dados, protegendo os direitos fundamentais dos indivíduos, pelo fortalecimento da segurança da informação quanto a privacidade, transparência, desenvolvimento, padronização, proteção do mercado e livre concorrência (31).

Todas as empresas que realizam o processamento de dados pessoais, sejam próprios (de seus funcionários e colaboradores) ou de terceiros (clientes, fornecedores ou parceiros) serão impactadas nas relações comerciais e de consumo, relações de trabalho e emprego, adequações de tecnologia e processos, políticas corporativas de privacidade, ética e segurança de dados, bem como na capacitação e no treinamento de pessoal (público interno e externo) (31).

Segundo MARINHO (31) a LGPD impõe uma profunda transformação no sistema de gestão de dados no Brasil, regulamentando a forma pela qual as organizações passarão a utilizar esses dados, criando diretrizes e limitações para todas as empresas em território nacional ou empresas nacionais em território estrangeiro.

A lei não se aplica quando o tratamento dos dados é realizado por uma pessoa física, para fins exclusivamente particulares e não econômicos, para fins exclusivamente jornalísticos

e artísticos e para tratamentos realizados para fins de segurança pública e defesa nacional, conforme o art. 4°, I, II, III e IV (39).

1.2 PROBLEMÁTICA E JUSTIFICATIVA

Conforme Pinheiro (39) a necessidade de uma lei específica sobre proteção dos dados pessoais decorre da forma como está sustentado o modelo atual de negócios da sociedade digital, na qual a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências.

Dessa forma, a fim de evitar qualquer penalidade imposta pela LGPD, as atividades de tratamento legítimo, específico e explícito de dados pessoais devem ser informadas previamente ao titular e necessitam estar orientadas pelos seguintes princípios: da finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas, além do princípio da boa-fé (39).

Segundo a lei, algumas penalidades que podem ser aplicadas são:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- 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;
- multa diária, observado o limite total a que se refere o inciso II;
- publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- 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;
- 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;

Para a LGPD, são dois os personagens que podem ser apenados por suas sanções, ou seja, o controlador e operador, assim considerado o primeiro como “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” e o segundo como “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”, nos termos do artigo 5º, inciso VI e VII. Segundo o artigo 52, a delimitação é clara no sentido de que terceiros que não

participem do tratamento de dados pessoais não são destinatários das sanções, como poderia ser considerado, por exemplo, a empresa que licencia software, mas não tem acesso ou gestão sobre os dados nele imputados. No caso de vazamento de dados, se tal empresa não tratou os dados, poderá até ser penalizada de outra forma, mas não por meio das sanções previstas no artigo 52 (37).

Um dos grandes problemas encontrados pelas empresas de desenvolvimento de software foi o controle e gestão da hierarquia de acesso aos dados do titular, já que os dados passam por muitas fases dentro dessas empresas como por exemplo na coleta, no tratamento e no compartilhamento desses dados. Para evitar sanções e controlar o nível hierárquico de acesso aos dados do titular uma das alternativas desenvolvidas foi o Privacy by Design, que estudaremos mais adiante nesse trabalho.

Neste contexto, o presente trabalho irá contribuir para as empresas de desenvolvimento de software que necessitam se adequar a LGPD, identificando possíveis práticas para implementação da LGPD que podem ser aplicadas em empresas de desenvolvimento de software.

2 OBJETIVOS

2.1 OBJETIVOS GERAIS

Esse trabalho tem como objetivo identificar as práticas para implementação da LGPD que podem ser aplicadas em empresas de desenvolvimento de software.

2.2 OBJETIVOS ESPECÍFICOS

- Apresentar os principais fundamentos necessários para compreensão da lei e da sua adequação;
- Compreender as necessidades vivenciadas por empresas de desenvolvimento de software referente a adequação a LGPD, as práticas realizadas e os desafio enfrentados;
- Apresentar orientações para adequação a LGPD.
- Simplificar a compreensão de adequação das empresas de software à LGPD através de estruturação de práticas por princípio da lei.

3 REVISÃO BIBLIOGRÁFICA

3.1 CONTEXTUALIZAÇÃO

A Lei Geral de Proteção de Dados Pessoais - LGPD, Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (6).

Com a grande quantidade de dados circulando pela internet, surgiu a necessidade de criar e implementar uma lei que pudesse garantir a proteção e privacidade dos dados pessoais, de modo que o usuário tenha o controle sobre o uso, compartilhamento e armazenamento de suas informações. Além de assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, a LGPD tem como princípio fomentar o desenvolvimento econômico e tecnológico e estabelecer regras únicas e harmônicas sobre tratamento de dados pessoais, por todos os agentes e controladores que fazem tratamento e coleta de dados, além de fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo (6).

O que se busca, portanto, em primeiro plano, na balança de interesses correspondentes ao trinômio pessoa-mercado-dados, é proteger a pessoa humana, valor central do ordenamento jurídico brasileiro, dando guarida efetiva aos seus dados, para que, então, possa ser tutelado também o mercado (45).

De acordo com o Art. 2. da Lei , a LGPD tem como princípio assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais. Além disso, a lei impõe penalidades às empresas e instituições que não cumprem com seus requisitos. Para evitar qualquer problema de ordem jurídica, é fundamental estar de acordo com as bases legais da LGPD.

3.2 PRINCÍPIOS APLICADOS AO TRATAMENTO DE DADOS

As bases legais são condições determinadas pela lei para que seja possível fazer a coleta e o tratamento de dados pessoais, e a melhor forma de se entender a lei é pela análise dos princípios que norteiam a base legal. Nenhuma lei é capaz de prever todas as condições e circunstâncias pelas quais ela vai ser aplicada, por isso se torna fundamental conhecer os princípios que a regem. Os princípios funcionam como uma bússola que irão reger as interpretações dos juízes no caso de existir questões que os dispositivos não possam prever. A lei apresenta no art. 6º os dez princípios gerais, além do princípio da boa-fé, para a aplicação dos seus dispositivos, incluindo as práticas de tratamento de dados (18).

Nesse sentido serão abordados em seguida os conceitos e definições dos princípios

aplicados ao tratamento de dados.

3.2.1 Princípio da finalidade

O princípio da finalidade é definido no Art. 6 da lei 13.709/18 como:

> "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

Assim, para que o tratamento de dados esteja autorizado, não é suficiente o consentimento geral e irrestrito do titular para tratamento. Deverá sempre o controlador atender aos requisitos da LGPD no art. 8º: "O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas". Nesse sentido, FEIGELSON; SIQUEIRA (18) explica: Deverá o controlador buscar sempre descrever, de forma mais específica e detalhada possível, de maneira destacada das demais cláusulas contratuais: (a) o propósito/finalidade do tratamento; (b) os meios empregados para a realização do tratamento; (c) extensão e duração do tratamento, estabelecendo um marco temporal para o seu encerramento e eliminação dos dados; (d) informações de contrato do controlador, e (e) informações acerca do uso compartilhado de dados pelo controlador.

3.2.2 Princípio da adequação

Segundo o Art. 6 da lei 13.709/18, o princípio da adequação é descrito:

> "adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento".

É um princípio que complementa o princípio da finalidade, uma vez que estabelece que o tratamento de dados deve ser relacionado exclusivamente com as razões apresentadas ao titular. "Portanto, o tratamento de dados pessoais deve restringir-se aos meios especificamente informados pelo controlador ao titular no ato do consentimento, sendo vedada qualquer utilização que extrapole os limites utilizados pelo titular" (18).

3.2.3 Princípio da necessidade

A lei define no seu Art. 6 que:

> "necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

FEIGELSON; SIQUEIRA (18) aponta que este princípio veda o tratamento de dados que ultrapassa os limites do propósito desejado, o que impediria práticas como coleta de dados que não possuam nenhuma relação com a atividade fim da empresa.

Ou seja, o princípio da necessidade também complementa o princípio da finalidade e determina que os controladores devem usar somente as informações fundamentais para atingir as finalidades pretendidas, e, portanto, o tratamento de dados pessoais deve ser limitado ao mínimo. As startups e empresas em geral devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades (35).

3.2.4 Princípio do livre acesso

O princípio do livre acesso confere aos titulares o direito de consultar seus dados pessoais, o modo, a duração e a segurança do tratamento de forma simples e gratuita. Portanto, o controlador e o operador deverão oferecer meios de fácil acesso para que o titular possa obter informações exatas sobre o tratamento de seus dados.

Segundo a lei em seu Art. 9:

> "o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso".

Ressalta-se, por fim que, as informações sobre o tratamento de dados devem ser fornecidas de maneira adequada à linguagem e compreensão do usuário, podendo o consentimento ser revogado a qualquer momento. Este deve ser feito por escrito ou de qualquer outra forma que evidencie a livre manifestação de vontade do titular (39).

3.2.5 Princípio da qualidade de dados

Conforme o Art. 6 da Lei n. 13.709, de 14 de agosto de 2018:

> "qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento".

Este princípio tem o objetivo de assegurar aos titulares que as informações que os agentes de tratamento possuem sobre eles são verdadeiras e atualizadas. É importante ter atenção à exatidão, clareza, relevância e atualização dos dados, sempre respeitando a necessidade e a finalidade do tratamento. Conforme prescrito no §2º do art. 9º da LGPD, se o consentimento for requerido e houver mudança na finalidade do tratamento, não sendo compatível com o consentimento inicial, o controlador deverá comunicar de antemão o titular sobre as alterações

de finalidade, sendo possível a revogação do consentimento pelo titular, caso se oponha às alterações (18).

3.2.6 Princípio da transparência

Conforme o Art. 6 da lei:

> "transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

De acordo com FEIGELSON; SIQUEIRA (18): "Através desse princípio, os titulares dos dados têm direito a receber informações claras, precisas, verdadeiras e de simples acesso sobre o tratamento e seus respectivos agentes de tratamento. Isto é, aos titulares de dados deverá ser disponibilizado livre e ilimitado acesso às informações dos responsáveis pelo tratamento, assim como ao modo e à extensão da realização do tratamento de dados."

3.2.7 Princípio da segurança

No sentido da segurança da informação, “os processos e procedimentos devem assegurar a disponibilidade, integridade e confidencialidade de todas as formas de informação, ao longo de todo o ciclo de vida do dado” (39).

Segundo a lei em seu Art. 6:

> "segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".

Assim, pelo princípio da segurança, presente no artigo 46 da Lei em questão, os agentes de tratamento têm a responsabilidade de buscar métodos de segurança, tecnicidade e administração, para proteger as informações pessoais dos usuários de acessos não autorizados por terceiros, assim como imprevistos e ilicitudes que ocasionem destruição, perda, alteração, comunicação ou difusão de dados pessoais.

3.2.8 Princípio da prevenção

Ligado ao princípio da segurança, o princípio da prevenção “impõe aos agentes de tratamento a obrigação de adotar medidas preventivas contra a ocorrência de eventuais danos decorrentes do tratamento de dados” (18).

De acordo com a Lei n. 13.709, de 14 de agosto de 2018:

> "prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais". (BRASIL, 2018)";

Ou seja, os agentes de tratamento devem prevenir o dano, formulando regras de boas práticas e de governança, como normas de segurança, padrões técnicos, métodos internos de supervisão e de redução de riscos(18).

3.2.9 Princípio da não discriminação

Segundo FEIGELSON; SIQUEIRA (18), o princípio da não discriminação proíbe que o tratamento de dados pessoais seja realizado para fins discriminatórios, ilícitos ou abusivos. Ademais, refere que o art. 21 da LGPD proíbe que os dados pessoais dos titulares sejam utilizados em seu prejuízo. Os dados frequentemente utilizados para discriminação são os chamados dados pessoais sensíveis. Por exemplo, os que tratam sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, e dados genéticos ou biométricos conforme artigo 5º, da LGPD.

3.2.10 Princípio da responsabilização

De acordo com o Art. 6 da Lei:

> "responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas"

O último princípio é o da responsabilização, pelo qual o controlador e o operador deverão demonstrar que agiram de boa-fé e com dedicação no cumprimento das normas de proteção dos dados pessoais. Assim, os agentes de tratamento devem manter conduta adequada e, na hipótese de violação, serão responsabilizados individualmente (18).

3.3 BENEFÍCIOS

A partir da medida provisória n° 959/20 na lei n° 14.058/20 onde a LGPD entrou em vigor, é preciso entender a importância da compreensão da proteção dos dados pessoais, uma vez que as informações que possam nos identificar servem como estatísticas políticas, econômicas e sociais não apenas para órgãos governamentais, mas também para empresas da iniciativa privada, logo, é nosso dever saber a relevância dos nossos dados pessoais para com os coletores desses dados (47).

De acordo com Vasconcelos , Kleber (47), a LGPD em vigor trouxe uma excelente oportunidade principalmente para o setor empresarial. A empresa tem a chance de fidelizar

os clientes por meio da proteção de seus dados, bem como proteger o seu negócio de futuras sanções administrativas ou judiciais por algum descumprimento da lei .

Segundo Giarllarielli, Gustavo (23) alguns benefícios da LGPD são:

- Descobrir as vulnerabilidades: é fundamental detectar as vulnerabilidades (físicas e digitais) que existem, principalmente aquelas que estão ligadas à segurança da informação, à privacidade e à proteção de dados, visto que, durante o processo de adequação à LGPD poderão ser descobertas lacunas de segurança, bem como aprender a corrigi-las.

- Aumentar a consciência: a empresa vai aumentar a consciência sobre a segurança da informação, já que, para se adequar à lei, é necessário realizar treinamentos com a participação de todos os colaboradores.

- Identificar e proteger os dados essenciais: no decorrer do processo de adequação a empresa vai identificar quais são os dados vitais para que ela consiga exercer o seu negócio, bem como onde eles estão armazenados. Por exemplo: backup, pastas digitais ou físicas, armazenamento na nuvem etc;

- Credibilidade da empresa: os seus parceiros de negócio vão perceber que a sua empresa se preocupa com a segurança e a privacidade, portanto ela será mais valorizada e respeitada por isso e, consequentemente, irá gerar benefícios para a imagem da empresa.

- Mapeamento e inventário de dados: através dessas ferramentas a empresa irá conseguir descobrir quais tipos de informações tem em seu banco de dados. Por exemplo: dados sensíveis.

- Controle de acesso às informações: o controle de acesso é uma medida preventiva que define quais funcionários são autorizados a acessar determinadas informações, assim como, é uma ferramenta que ajuda a garantir que os direitos dos titulares dos dados sejam respeitados. Por exemplo: somente o chefe do RH, em razão de sua função, está autorizado a ter acesso aos dados relativos à rescisão do contrato de um empregado.

- Evitar multas: as empresas que se adequarem à LGPD, estarão mais preparadas para cooperar com os órgãos de fiscalização, pois terão mais ferramentas para evitar multas ou reduzi-las.

De acordo com Henriques , Pedro (27) para que a empresa possa se adequar a LGPD é interessante ressaltar a importância da segurança dos dados. A segurança da informação tem relação direta com a proteção de dados, com a segurança física e com a segurança ambiental de uma empresa. Toda essa proteção é adquirida por meio do alinhamento de tecnologias da informação que trabalham em prol de objetivos alinhados à missão, visão, valores e propósito da empresa.

3.4 FUNDAMENTOS SOBRE A LGPD

A LGPD regulamenta qualquer atividade que envolva utilização de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, no território nacional ou em países onde estejam localizados os dados (6). Portanto, estão definidos abaixo alguns conceitos presentes na lei e suas características.

3.4.1 Dados pessoais

Segundo o Art. 5. da Lei n. 13.709, de 14 de agosto de 2018, Dado pessoal é: "informação relacionada a pessoa natural identificada ou identificável".

Portanto, dados pessoais são todos aqueles que podem identificar uma pessoa – números, características pessoais, qualificação pessoal, dados genéticos.

3.4.2 Dados sensíveis

A lei n. 13.709, de 14 de agosto de 2018, também definiu alguns tipos de dados pessoais, como os dados sensíveis. Trata-se de informações que podem ser utilizadas de forma discriminatória e, portanto, carecem de proteção especial.

A lei define como: "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".

3.4.3 Dados pessoais de crianças e adolescentes

Conforme o Artigo 14 da LGPD, o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

Segundo FEIGELSON; SIQUEIRA (18), a expressão “melhor interesse” da criança e do adolescente deve ser compreendida como tudo o que não prejudica o menor, bem como aquilo que poderá lhe trazer benefícios.

3.4.4 Dado pessoal anonimizado

É o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (6).

Desta forma, estariam fora do escopo de aplicação da lei, à exceção se o processo de anonimização puder ser revertido ou se estes forem utilizados na formação de perfis comportamentais. Dados efetivamente anonimizados são essenciais para o funcionamento de tecnologias

no campo da Internet das Coisas, inteligência artificial, machine learning, smart cities e análise de grandes contextos comportamentais (41).

3.5 PAPÉIS DENTRO DA LGPD

A LGPD em seu Art. 5. da Lei n. 13.709, de 14 de agosto de 2018, institui as partes que são envolvidas pela Lei, são elas:

3.5.1 Titular

O titular é pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (BRASIL, 2018).

3.5.2 Controlador

Brasil (6) define o controlador como: "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

O controlador é aquele que tem o poder de decidir a forma de tratamento, a finalidade do tratamento de cada dado e os meios de tratamento destes dados.

3.5.3 Operador

Segundo a Brasil (6), o operador é: "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

3.5.4 Encarregado

Encarregado de acordo com a Brasil (6) é: "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)".

3.5.5 Agentes e controladores

De acordo com o Art. 37. da Brasil (6), "controlador e operador são os agentes de tratamento de dados pessoais, devendo manter registro das operações de tratamento que realizarem", especialmente quando baseadas em legítimo interesse. Conforme o Art. 39, o operador deve realizar o tratamento de dados de acordo com as instruções fornecidas pelo controlador. Além disso, o controlador deve indicar o encarregado (DPO – Data Protection Officer) pelo tratamento de dados pessoais.

Segundo o Art. 41. da Brasil (6), conforme inovação trazida pela redação da Medida Provisória n.º 869/2018, o DPO pode ser pessoa física ou jurídica (nacional ou internacional), que atue como canal de comunicação entre o controlador e a ANPD e os titulares. A identidade e as informações de contato do encarregado devem ser públicas, claras e objetivas, de preferência no site do controlador; e o encarregado deverá aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

3.5.6 Agência Nacional de Proteção de Dados - ANPD

A ANPD é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil (6).

A ANPD foi criada pela Medida Provisória n. 869, de 27 de dezembro de 2018, posteriormente convertida na Lei n. 13.853, de 14 de agosto de 2019.

De acordo com o Art. 55-K. da Brasil (7), de 14 de agosto de 2019, "A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.".

Ou seja, a ANPD deve se articular com outras entidades e órgãos públicos a fim de garantir o cumprimento de sua missão institucional, atuando como órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para a sua implementação. A LGPD determina, por exemplo, que a ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados. Da mesma forma, a LGPD determina que a ANPD deve comunicar às autoridades competentes as infrações penais das quais tiver conhecimento.

É importante observar que a aplicação das sanções previstas na LGPD compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

3.6 APLICAÇÃO E SANÇÕES DA LGPD

Na última década, uma grande indústria acumulou uma quantidade cada vez maior de dados pessoais. Um complexo ecossistema de sites, aplicativos, empresas de mídia social, corretores de dados e empresas de tecnologia de publicidade passaram a rastrear usuários on-line

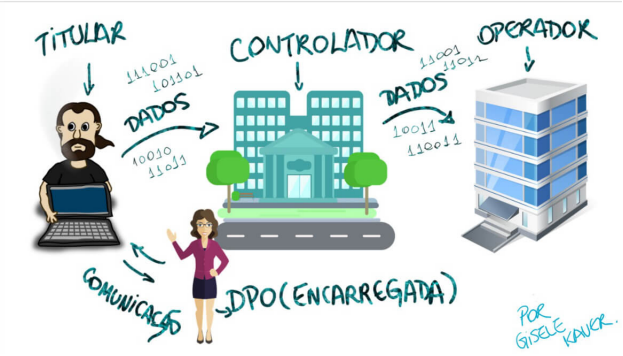

Figura 1 – Papéis na LGPD
(28)

e off-line, coletando seus dados pessoais. Esses dados são reunidos, compartilhados, agregados e monetizados, alimentando uma indústria de 227 bilhões de dólares por ano (25).

Isso ocorre todos os dias, conforme as pessoas vivem diariamente suas vidas, muitas vezes sem seu conhecimento ou permissão. Em razão disso, torna-se indispensável uma regulação para o tratamento de dados e sanções para estas condutas que lesam de maneira significativa os seus titulares. O art. 52 da lei 13.709/18 apresenta algumas das sanções que serão aplicadas pela Autoridade Nacional em hipótese de infração às normas previstas nesta lei. É interessante compreender que as sanções se aplicam à infração de qualquer norma prevista na LGPD. Isso quer dizer que se atentar aos princípios é tão relevante quanto observar dispositivos de caráter mais pragmático/objetivo.

Dentre estas sanções, a primeira penalidade estipulada pela lei é a advertência, considerada o tipo mais leve dentre as sanções administrativas. Embora pareça inofensiva, é importante enfatizar que a advertência indicará um prazo para adoção de medidas corretivas (14).

Caso ocorra inércia da advertida e a não adoção de medidas dentro do prazo especificado pode constituir uma nova infração e resultar em sanções mais severas para a empresa.

A segunda sanção a que se refere a lei são as multas simples. O valor da multa pode chegar em até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, no entanto, é limitada ao total de RS 50 milhões por infração (14).

Segundo Dias (14), além da multa simples, o art. 52 traz uma outra modalidade de multa: as multas diárias, observando o mesmo limite imposto na multa simples. Considerando que, ainda com esse limite máximo, a possibilidade de emprego de multas diárias podem causar prejuízos consideráveis ao infrator, podendo de fato, atingir de forma significante o faturamento de empresas que talvez RS 50 milhões, por si só, não represente um impacto econômico significativo.

Embora as multas se destaquem entre as infrações, é importante considerar que os danos indiretos podem ser maiores que os diretos: perda de valor da marca, impacto na confiança do

cliente e do investidor, desvalorização de ativos e perdas de contratos são apenas alguns deles. Em razão disso, dependendo da natureza da infração e do ramo de negócios, a publicidade talvez traga maior impacto que a multa. Ela está entre as sanções dispostas no art. 52, e só pode ser aplicada após a devida apuração do caso e confirmação da ocorrência. Por fim, temos duas outras formas de sanções que também afetam indiretamente o negócio e podem significar uma paralisação parcial das operações e perda de ativos: o bloqueio e a eliminação dos dados pessoais referentes à infração. No primeiro caso até a sua devida regularização. Todas as sanções mencionadas somente serão aplicadas após procedimento administrativo que assegure a ampla defesa do acusado (14).

Conforme Dias (14), desta forma, serão consideradas as particularidades de cada caso em específico, assim, a lei traz alguns parâmetros e critérios para a avaliação daquilo que será aplicado no caso concreto, tais como: a gravidade e a natureza das infrações e dos direitos pessoais afetados, boa-fé, reincidência, o grau do dano, cooperação do infrator, condição econômica, vantagem auferida ou pretendida pelo infrator, adoção de política de boas práticas e governança, adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, adoção de medidas corretivas e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

3.7 PROTEÇÃO E SEGURANÇA DOS DADOS

Segundo Barbieri (5), com o crescimento do volume de dados, há uma clara percepção de que as empresas já estão atrasadas com relação a um olhar mais cuidadoso em direção aos seus problemas potenciais de dados. A isso se acrescenta a amplificação dos riscos e das consequências tecnológicas e gerenciais que chegarão com o desembarque de outras tendências apontadas, como Big Data, IoT e Inteligência Artificial, que, para muitos tipos de negócios, mudarão a escala dos dados e as dimensões dos problemas e soluções por eles gerados.

Até um determinado momento histórico, a tutela jurisdicional sobre a privacidade, liberdade e igualdade foi suficiente. Novos desdobramentos da era moderna, reacenderam a necessidade de novos limites, já adaptados à realidade da era digital. Ao longo dos anos, aconteceram diversas situações que contribuiram para o surgimento de uma normativa que zela pela proteção dos dados (21).

Para Henriques , Pedro (27) a Segurança da Informação tem relação com a proteção de dados, com a segurança física e com a segurança ambiental de uma empresa. Toda essa proteção é adquirida por meio do alinhamento de Tecnologias da Informação que trabalham em prol de objetivos alinhados à missão, visão, valores e propósito da empresa. Se engana quem pensa que Segurança da Informação se resume a um software ou a uma prática isolada de segurança. Para que uma empresa pratique Segurança da Informação de maneira eficaz, são necessárias uma série de medidas, pensadas e implementadas em conjunto, que vão trabalhar em prol dos mesmos objetivos de negócio. (27)

A LGPD tem impacto direto sobre praticamente todas as empresas que atuam em território nacional coletando e tratando os dados pessoais. É comum que empresas solicitem dados como nome, endereço, telefone e idade para realizar cadastros. Se esses dados ficam armazenados, a empresa precisa se adequar à LGPD. Outra forma de atuação da Lei Geral de Proteção de Dados é sobre empresas que utilizam seus sites para coletar dados de forma automatizada. Dados de navegação, endereço de IP, cookies, e-mail, localização por GPS e similares também são considerados dados pessoais pela LGPD e também devem seguir as diretrizes da lei para coleta e tratamento. Dessa forma a Segurança da Informação se faz indispensável no dia a dia de empresas que lidam com dados pessoais. Não só pela LGPD, mas também por interesse próprio. (27)

Para Barbieri (5), organizar os dados de uma empresa é tarefa árdua e exige caminhos cuidadosos, alguns deles com obstáculos culturais fortes, a governança de dados e as suas gerências vieram justamente para tratar disso.

De forma simplificada, a governança de dados é um conjunto de práticas, dispostas em um framework, com o objetivo de organizar o uso e o controle adequado dos dados como um ativo organizacional. Seria, por assim dizer, uma forma de organizar a empresa em relação aos aspectos de dados, visando disponibilidade, integridade, consistência, usabilidade, segurança, controle (5).

A forma mais usual de se buscar entender qual a situação atual de uma empresa com relação aos seus dados é mediante processos de avaliação/diagnósticos em áreas de negócios. Isso pode ser feito por reuniões com técnicas de dinâmicas de dados em grupo ou por entrevistas e pesquisas sobre maturidade de dados na empresa (5).

Segundo Oliveira (37), com a finalidade de garantir a segurança do tratamento de dados pessoais, recomenda-se a implementação de Política de Segurança da Informação (PSI) para que se estabeleçam regras claras sobre a proteção de dados, inclusive os pessoais. A PSI é um documento interno, que pode ser criado pelo controlador ou operador, no qual serão regulados os procedimentos internos para que se preserve a segurança de dados no âmbito da empresa. A PSI poderá prever métodos, processos, tecnologias a serem aplicadas, direitos e deveres dos usuários, entre outras disposições.

Uma PSI adequada, apesar de não ser exigência expressa da LGPD, é uma medida administrativa que tem o intuito de garantir a proteção das informações e, neste caso específico, dos dados pessoais, ou seja, trata-se de um meio para que a empresa garanta a proteção dos dados pessoais conforme requerido pela lei (37).

3.7.1 Privacy by Design

Conforme FREITAS (20), a política de privacidade é um dos instrumentos de implementação do privacy by design faz parte da estrutura de documentos para a proteção de dados. A política objetiva dar visibilidade ao tratamento de dados pessoais em um determinado serviço,

atendendo princípios da Lei Geral de Proteção de Dados Pessoais.

Cavoukian et al. (11) articula que a PbD pode ser alcançada seguindo-se sete princípios básicos. Estes princípios refletem uma filosofia de ação e não uma abordagem computacional de Engenharia de Sistemas, de Processos ou de Engenharia de Software. Sobre esses princípios, podem ser aplicados vários modelos específicos para desenvolvimento de processos, bem como arquiteturas computacionais e praticamente qualquer infraestrutura de rede de comunicação. (29)

Vejamos quais são estes sete princípios da PbD apontados por Cavoukian et al. (11):

- Proatividade e Prevenção: prefira a proatividade à reatividade, como também a prevenção à remediação. Esse princípio sugere a prevenção contra eventos de invasão de privacidade. PbD não espera pela materialização dos riscos de privacidade. PbD deve se antecipar ao fato e não sucedê-lo. Esse princípio prevê a prevenção até mesmo para eventuais ataques provocados por membros internos da equipe do software. As atitudes que levam à proatividade e prevenção passam por:

  a. Comprometimento para implementar padrões sofisticados e que alcancem graus elevados de privacidade, geralmente maiores que os sugeridos por normas ou leis;

  b. Comprometimento com um padrão de privacidade que possa oferecer garantias claras à comunidade de usuários e aos responsáveis pela organização em que é implementada;

  c. Esteja pronto para corrigir qualquer ação negativa que possa ocorrer.

- Privacidade como configuração padrão: É um princípio que pode ser chamado como Privacy-by-Default. Entende-se como privacidade por padrão os seguintes princípios: Apresentação do propósito - O usuário deve estar ciente da motivação da organização para coletar aquele dado de caráter pessoal que pode ser usado para reidendificá-lo. Do mesmo modo, ele deve saber como o dado será usado, como será armazenado e, eventualmente, descartado. O propósito deve estar claro, deve ser limitado e relevante para as tarefas a serem realizadas;

  a. Limitação dos dados: os dados obtidos dos usuários devem estar cobertos por uma previsão legal e devem ser limitados ao mínimo necessário para as tarefas a serem executadas;

  b. Minimização dos dados: a minimização do contato com dados pessoais deve ocorrer em toda cadeia de fluxo de dados da organização. Desde a primeira interação do usuário com o sistema, incluindo todas as demais transações, devem ser não identificáveis. Deve ser observado também o mínimo de ligação entre os dados pessoais;

  c. Minimização do uso, armazenamento e divulgação: o uso, o armazenamento e a divulgação dos dados pessoais deve ser limitada e relevante para os propósitos de identificação pessoal. É também imprescindível que haja um termo de consentimento livre e esclarecido

(TCLE). O armazenamento dos dados pessoais deve se restringir ao tempo de execução da tarefa e posteriormente devem ser descartados com segurança.

- Privacidade incorporada no projeto: este é um tema intrinsecamente ligado ao projeto de software. Este princípio sugere que o projeto e a arquitetura de software do sistema de TI devem ter o requisito não funcional de privacidade incorporado ao sistema computacional. Deste modo, a privacidade será um componente não funcional integrante no cerne do sistema, sem comprometer nenhuma funcionalidade do sistema. Neste princípio não devemos esquecer que a avaliação de riscos e impacto deve ser publicada, bem como as medidas de mitigação do impacto de eventuais violações de privacidade.

- Funcionalidade completa. Soma positiva: todos os objetivos funcionais da organização devem estar contemplados no sistema de software. Não deve haver nenhuma perda de funcionalidade dada a adoção de PbD. PbD deve evitar falsas dicotomias como "privacidade versus segurança" no sistema, ou seja, todas as demais demandas do sistema, sejam elas não funcionais ou funcionais não devem "competir" com a demanda pela privacidade. A soma de requisitos funcionais e não funcionais deve ser sempre positiva.

- Segurança de ponta a ponta: todo dado que entra num sistema tem um ciclo de vida, ou seja, ele é coletado, processado e descartado. A abordagem PbD deve prever a proteção dos dados logo na fase de coleta, de entrada, e essa proteção deve prevalecer por todo ciclo de vida do dado. Isso garante que todas as informações retidas no sistema estão seguras. Segurança nesta abordagem significa manter a privacidade. Sem uma metodologia forte para a segurança de dados não há garantia de privacidade. As organizações devem assumir esta responsabilidade pela segurança que acompanhará os dados por todo ciclo de vida. Adicionalmente, a segurança deve possibilitar confidencialidade, integridade e disponibilidade dos dados pessoais em todo ciclo de vida. São também esperados, métodos seguros para descarte dos dados, criptografia apropriada e a autenticação das operações;

- Visibilidade e Transparência: PbD deve assegurar à todas as partes envolvidas no sistema que está operando de acordo com os objetivos e com a garantia de respeito às premissas legais de proteção dos dados pessoais. Todas as operações com dados pessoais poderão ser verificadas por um agente independente. Paralelamente, todos os componentes de software e suas operações devem ser transparentes aos usuários. Visibilidade e transparência são essenciais para garantir a confiança e a demonstração de responsabilidade sobre os resultados, ou accountability. Estes princípios também resgatam os seguintes princípios da FIP:

  a. Accountability: as responsabilidades por todos os procedimentos que proporcionam segurança na privacidade, bem como as políticas de privacidade adotadas, devem estar documentadas e devem ser comunicadas apropriadamente;

b. Abertura: abertura e transparência são a chave para accountability. Informações sobre o gerenciamento das informações privadas devem estar disponíveis aos usuários;

c. Aderência: compliance às normas de privacidade deve ser monitorada, avaliada e verificada frequentemente. Mecanismos de reparação para violação de privacidade devem ser estabelecidos e os indivíduos afetados devem ser notificados.

- Respeito à privacidade do usuário: acima de todos os requisitos de software, da arquitetura do sistema e das necessidades dos implementadores, devem prevalecer as soluções para implantação e manutenção da privacidade individual. O papel dos usuários neste tipo de solução que busca a privacidade na concepção do projeto deve ser priorizado. Este princípio também abarca os seguintes princípios FIP:

  a. Consentimento: o TCLE na coleta, uso e descarte dos dados pessoais. Quanto mais sensível o dado, mais clareza o TCLE deve transmitir ao usuário;

  b. Acurácia: as informações pessoais armazenadas devem ser acuradas, completas e atualizadas;

  c. Acesso: todos os usuários devem ter acesso às informações pessoais mantidas pelo sistema, como também devem poder atualizá-las, corrigi-las ou apagá-las.

Embora esta proposta de PbD seja bastante abrangente, para Gürses; Troncoso; Diaz (26), não é claro como estes princípios podem ser traduzidos para operações ou tarefas práticas computacionais, ou seja, são princípios que não correspondem diretamente a uma metodologia de projeto de software. Sendo assim, os engenheiros de software devem procurar adaptar esses requisitos não funcionais à metodologia de projeto e desenvolvimento escolhida.

3.8 ETAPAS PARA A ADEQUAÇÃO DA LGPD

As empresas que possuem diversos cadastros em sua base, sejam estes de cunho pessoal sensível ou não, precisam aprimorar seus processos de gestão da segurança da informação e privacidade, além de governança de dados pessoais, não apenas para cumprir a Lei, mas também para melhorar o tratamento de dados pessoais e assim elevar a qualidade dos seus serviços mantendo a proteção dos direitos e liberdades dos titulares (3).

Nesse sentido, a ANPPD (3) estabeleceu algumas fases para adequação da LGPD. Essas fases tem como objetivo a realização de um diagnóstico de privacidade, identificação de riscos associados ao tratamento de dados pessoais, construção de um plano de ação, implementação das medidas necessárias, revisão e monitoramento da Política de Privacidade e Proteção de Dados. Serão elencadas abaixo as cinco fases bem como sua definição e exemplo prático de aplicação.

3.8.1 Fase 01 - Preparação

O objetivo da fase de preparação é realizar um diagnóstico de privacidade por meio de análise dos requisitos e necessidades de proteção de dados e privacidade, identificar leis, regulamentos e normas relevantes e estabelecer um plano de ação. (3)

Segundo a ANPPD (3) algumas atividades a serem desenvolvidas nessa primeira fase são:

- Realizar análise de privacidade;
- Identificar leis de privacidade e outras normas aplicáveis ao segmento de atuação;
- Analisar o impacto da privacidade;
- Realizar auditorias e avaliações dos dados iniciais;
- Estabelecer organização de governança de dados;
- Estabelecer fluxos de dados e inventário de dados pessoais;
- Estabelecer programa proteção de dados e privacidade;
- Esboçar planos de implementação de ações de proteção de dados e privacidade.

Como resultado dessas atividades é possível identificar algumas práticas a serem adotadas nessa etapa. São elas:

- Relatório de análises de proteção de dados e privacidade;
- Manual de leis de privacidade;
- Relatório de auditoria de dados pessoais;
- Sistema de fluxo de dados;
- Inventário de dados pessoais;
- Política de proteção de dados;
- Plano de treinamento em privacidade;
- Programa de proteção de dados e privacidade;
- Relatório e listagem das aquisições e materiais necessários para proteção dos dados;
- Planos de implementação de ações de proteção de dados e privacidade.

Portanto, o resultado da Fase 1 é identificar os departamentos impactados, mapear os dados e definir o cronograma do projeto a ser seguido nas próximas etapas.

3.8.2 Fase 02 - Organização

Nessa segunda etapa o objetivo consiste em desenhar e organizar o programa de proteção de dados e privacidade, designar um DPO, envolver e obter o compromisso de todas as partes interessadas relevantes.

Assim sendo, algumas atividades propostas são:

- Manter programa, políticas e controles de governança de privacidade de dados;
- Atribuir e manter responsabilidades na Proteção de Dados e Privacidade;
- Manter o compromisso na organização com Proteção de Dados e Privacidade;
- Manter comunicações regulares para questões de Proteção de Dados e Privacidade;
- Manter o envolvimento das partes interessadas em questões de Proteção de Dados e Privacidade;
- Implementar e operar sistemas computadorizados para Proteção de Dados e Privacidade.

Como resultado dessas atividades é possível identificar algumas práticas a serem adotadas nessa etapa. São elas:

- Estratégia de Proteção de Dados e Privacidade atualizada;
- Programa de Proteção de Dados e Privacidade atualizado;
- Controles de governança de dados atualizados;
- Anúncio da nomeação do DPO/Encarregado;
- Comunicações relativas a todas as questões relacionadas a Proteção de Dados e Privacidade;
- Garantias da Rede dos Agentes de Tratamento, com medidas de Proteção de Dados e Privacidade;
- Papel de Proteção de Dados e Privacidade nas descrições de trabalho;
- Plano de treinamento, comunicação e conscientização de privacidade atualizado;
- Sistemas e processamentos automatizados com medidas para Proteção de Dados e Privacidade.

Dessa forma, na fase de organização pretende-se obter estruturas organizacionais para facilitar a implementação de Proteção de Dados e Privacidade, e a conscientização das áreas funcionais impactadas a respeito da Legislação, realização do inventário de dados pessoais.

3.8.3 Fase 03 - Implementação

A fase de implementação consiste em projetar um sistema de classificação de dados, desenvolver e implementar políticas, procedimentos e controles para cumprir leis de privacidade e requisitos da organização.

Algumas atividades apresentadas são:

- Desenvolver e implementar estratégias, planos e políticas de Proteção de Dados e Privacidade;
- Implementar o procedimento de aprovação para processamento de dados pessoais;
- Registrar bancos de dados para dados pessoais;
- Desenvolver e implementar um sistema de transferência internacional de dados;
- Executar atividades de integração de proteção de dados e privacidade;
- Executar o plano de treinamento de proteção de dados e privacidade;
- Implementar controles de segurança de dados.

Como resultado dessas atividades é possível identificar algumas práticas a serem adotadas nessa etapa. São elas:

- Sistema de classificação de dados pessoais;
- Procedimento para aprovar o processamento;
- Documento de registro de bancos de dados de dados pessoais;
- Sistema de transferência internacional de dados;
- Atividades de integração de proteção de dados e privacidade concluídas;
- Atividades de treinamento de proteção de dados e privacidade concluídas;
- Controles de segurança de dados implementados.

Como resultado da aplicação das atividades e práticas, a empresa terá medidas implementadas para governar dados pessoais com mais efetividade.

3.8.4 Fase 04 - Governança

Nessa fase os objetivos principais são desenhar e configurar estruturas de governança, Ex.: Programa de proteção e privacidade, DPO, etc., envolver e obter o comprometimento de todas as partes interessadas relevantes, relatar todas as questões de privacidade (processo contínuo).

- Implementar práticas para gerenciar o uso de dados pessoais;
- Manter avisos de privacidade sobre dados pessoais;
- Executar um plano de solicitações, reclamações e retificações;
- Executar uma avaliação de riscos de proteção de dados;
- Emitir relatórios de proteção de dados e privacidade;
- Estabelecer e manter um plano de resposta de violação de privacidade.

Como resultado dessas atividades é possível identificar algumas práticas a serem adotadas nessa etapa. São elas:

- Estratégia de proteção de dados e privacidade atualizada;
- Política de proteção de dados;
- Procedimentos para manter avisos de privacidade de dados;
- Plano de para tratar solicitações, reclamações e retificação;
- Processo de avaliação de riscos de proteção de dados e privacidade;
- Plano de gerenciamento de riscos de terceiros;
- Relatório proteção de dados e privacidade;
- Documentação de privacidade de dados;
- Plano de resposta à violação de privacidade de dados.

Portanto, nessa fase são implementadas estruturas de governança para proteção de dados, programa de governança em proteção de dados e sistema de gestão da privacidade da informação (SGPI).

3.8.5 Fase 05 - Avaliação e Melhoria

A última fase tem como objetivo monitorar a operação e a resolução de todas as questões relacionadas à privacidade, avaliar regularmente a conformidade com processos e políticas internas, melhorar a proteção de dados e as medidas de privacidade.

Com base nisso, algumas atividades propostas são:

- Realizar auditoria interna de proteção de dados e privacidade;
- Envolver uma parte externa para avaliações proteção de dados e privacidade;
- Realizar avaliações e estabelecer comparações com entidades similares;
- Executar avaliações de riscos de proteção de dados;
- Resolver riscos de proteção de dados e privacidade;
- Relatar análise de riscos de proteção de dados e privacidade e resultados;
- Monitorar as leis e regulamentos de proteção de dados e privacidade.

Como resultado dessas atividades é possível identificar algumas práticas a serem adotadas nessa etapa. São elas:

- Relatório de auditoria interna de proteção de dados e privacidade;
- Relatório de auditoria externa proteção de dados e privacidade;
- Relatórios de avaliação desestruturados;
- Relatório de auto avaliação de privacidade;
- Relatório comparativo de privacidade com outras entidades similares à do controlador;
- Relatório de avaliação de impacto sobre proteção de dados;
- Relatório de riscos de privacidade e proteção de dados resolvidos;
- Análise de riscos de privacidade e proteção de dados e relatório de resultados;
- Relatório de monitoramento de leis de privacidade.

Os resultados dessa fase são relatórios de monitoramento de leis de privacidade, identificação dos riscos associados ao tratamento de dados pessoais e lista de compras dos materiais necessários para tratamento dos riscos identificados.

3.9 DESAFIOS PARA EMPRESAS DESENVOLVEDORAS DE SOFTWARE:

Para as empresas desenvolvedoras de software, a implementação das normas da LGPD, acima de tudo, para não sofrer as consequências que ela prevê, irá gerar uma reformulação na forma como a empresa lida com a coleta e o tratamento de dados dos seus clientes, funcionários e colaboradores.

Segundo Lima (30), em um projeto que tem como premissa alterar a estrutura e a forma como os processos são conduzidos em uma empresa, a maior dificuldade será em relação à mudança cultural da empresa. A complexidade da implantação de novos processos em organizações que já possuem uma cultura rígida por parte de seus colaboradores pode dificultar a adesão.

Para Lima (30), existe a necessidade da revisão constante dos processos internos e externos da empresa, em alguns casos será necessário ajustes simples, em outros casos ajustes de grande impacto. Na etapa de mapeamento se torna de fundamental importância a categorização dos dados, através do mapeamento será possível a identificação quais são os dados que a empresa possui acesso, quem são os responsáveis por determinados dados, se a empresa está coletando e armazenando somente os dados necessários ao qual foi indicado no consentimento de coleta dos dados.

A nomeação de um encarregado de proteção de dados é um ponto bastante discutido em um processo de implementação da LGPD, a nomeação de um encarregado implicará geração de novos custos para as empresas, pois ele será o responsável por prestar assistência interna para os colabores da empresa, aos titulares de dados, sobre a práticas de tratamento de dados, verificar se está práticas estão em conformidade com a legislação e a política interna da empresa. Investimento em cursos de capacitação, certificações serão essenciais. (30)

De acordo com a lei, empresas que não possuem um encarregado definido e efetuam algum tipo de tratamento de dados, deverão eleger um colaborador ou uma equipe capacitada para que possa atender essa função.

É necessário que a cultura de proteção de dados pessoais esteja presente em todas as fases do desenvolvimento de seus sistemas, pois quando a LGPD efetivamente entrar em vigor, qualquer usuário vai poder perguntar quais dados estão sendo utilizados, para quais motivos e com quem eles foram compartilhados. Caso haja qualquer vazamento de dados, a empresa terá de notificar quais dados foram vazados e quais as providências tomadas para evitar um novo vazamento, além de precisar estar preparada para responder esses questionamentos de maneira rápida e precisa. (46)

Segundo SOUZA (46), a Tecnologia está cada vez mais presente em todas as áreas das nossas vidas, e as empresas que não se adequarem corretamente a esse mundo digital, além de perder dinheiro e clientes, vão se tornar cada vez mais obsoletas e ultrapassadas. Além de todas as sanções e multas que podem ser causadas pela não conformidade com a LGPD, uma empresa que não consegue garantir a transparência e a segurança no uso dos dados de seus clientes, vai

perder totalmente sua credibilidade, e por consequência, seus clientes.

4 RESULTADOS

4.1 METODOLOGIA

Esse trabalho tem como objetivo geral identificar as práticas para implementação da LGPD que podem ser aplicadas em empresas de desenvolvimento de software. Para atingir este objetivo foi estruturada uma metodologia conforme apresentado abaixo.

4.1.1 Revisão da literatura

Esta primeira etapa visa identificar práticas de implementação da LGPD, para isso foi desenvolvida uma pesquisa em trabalhos na literatura que demonstravam estudos de casos práticos.

Segundo Gil (24), a revisão da literatura consiste na identificação, localização e análise de publicações que contêm informações relacionadas ao tema da investigação e busca identificar contribuições teóricas aplicáveis ao estudo.

4.1.2 Pesquisa qualitativa

Neste segundo momento, foi realizada entrevista com um especialista que atuou como DPO na implementação da LGPD numa empresa de desenvolvimento de software da cidade de Chapecó no oeste do estado de Santa Catarina. Esta etapa procurou identificar as práticas utilizadas para adequação e os principais desafios enfrentados por ele. Devido ao tempo disponível para desenvolvimento deste trabalho, delimitou-se esta etapa da pesquisa para investigar as práticas relacionadas ao princípio de segurança.

A entrevista é uma técnica eficiente para obtenção de dados em profundidade acerca dos aspectos que estão sendo estudados (24). Para isso, primeiramente foi criado um questionário semi-estruturado que são entrevistas guiadas onde o pesquisador define uma sequência de perguntas, mas podendo se adequar com as características do entrevistado.

4.1.3 Estruturação de orientações de adequação

A terceira e última etapa visa condensar em uma tabela todo o aprendizado e resultados obtidos pelas etapas anteriores. Nessa tabela constam diversas práticas e ações por princípio da lei que norteiam a adequação à LGPD em uma empresa de desenvolvimento de software.

Para cada princípio é apresentado o dever do controlador e as práticas que podem ser adotadas pelas empresas de software para se adequar à LGPD.

4.2 DESENVOLVIMENTO DA PESQUISA

4.2.1 Práticas para adequação

Nessa etapa do trabalho foram identificadas práticas de implementação da LGPD, para isso foi desenvolvida uma pesquisa em trabalhos na literatura que demonstravam estudos de casos práticos.

Abaixo serão apresentadas as práticas identificadas.

4.2.1.1 Princípio da finalidade

Para atender o Princípio de finalidade, é necessário fazer a coleta precisa dos dados e informar ao titular a finalidade com que os dados serão utilizados. Para atender esse princípio, as práticas identificadas foram:

- Mapeamento dos dados: deverá ser mapeado todos os dados sensíveis e qual a finalidade dos dados identificados em cada atividade, isso irá facilitar a etapa de levantamento de riscos. Além disso, é necessário mapear onde estão armazenados esses dados, por quanto tempo e indicar se existe alguma lei ou consentimento que permita a sua captura (42).

- Categorização dos dados: segundo Sabino (42), categorizar os dados, para que posteriormente possam ser identificados os responsáveis e os propósitos do armazenamento dessas informações. Esse trabalho é feito para entender quais dados são necessários para cada atividade, como estão sendo usados, quem tem acesso a eles e de quem são.

- Termos de uso: é um documento que estabelece as regras e condições de uso de determinado serviço. Caso o Termo de Uso seja aceito pelo usuário, a utilização do serviço será vinculada às cláusulas dispostas nele (8).

- Levantamento do mapa de finalidades de dados: levantamento das finalidades de dados através de um mapeamento realizado junto aos setores chaves da instituição, setores esses que de alguma forma utilizam-se de dados pessoais dentro de qualquer uma das fases que a lei propõe, ou seja, coleta, retenção, processamento, compartilhamento e eliminação (13).

4.2.1.2 Princípio da adequação

Para atender o Princípio da adequação, é necessário tratar os dados visando a compatibilidade com as finalidades informadas ao titular. Para atender esse princípio, as práticas identificadas foram:

- Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

  Segundo Buchain (9), as exigências legais de adequação e necessidade exigem do controlador limitar as características de seu tratamento única e exclusivamente ao que for minimamente indispensável para atingir as suas finalidades. A escolha dos dados tratados é justificada pela finalidade do tratamento, ou seja, deverá haver uma adequação entre a finalidade informada e os dados tratados.

- Norma de Uso Aceitável de Ativos da Informação: segundo Ferreira (19), ativos da informação podem ser compreendidos como o conjunto que envolve as pessoas, tecnologia e processos, sendo estes responsáveis por alguma etapa do ciclo de vida da informação. Já Sêmola (44) conceitua ativo como todo elemento que faz parte do processo de manipulação e processamento da informação, os meios em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

  Para assegurar que a informação receba um nível adequado de proteção, os ativos precisam ser mapeados durante o planejamento da segurança da informação, sendo de extrema relevância a realização da sua classificação a qual irá determinar o grau de sigilo às informações neles contidas (10).

4.2.1.3 Princípio da necessidade

Para atender ao princípio da necessidade, é necessário ponderar entre o que é realmente essencial para o seu negócio. Para atender esse princípio, as práticas identificadas foram:

- Minimização dos dados: em decorrência da minimização dos dados, os dados pessoais devem ser pertinentes e limitados ao que seja necessário para atingir às finalidades para os quais são tratados. O controlador deverá limitar a coleta de dados pessoais ao que seja necessário para alcançar seu propósito, retendo-os apenas o tempo necessário para o atingimento desse desiderato (9).

- Política de retenção de dados: por quanto tempo a empresa guarda os dados pessoais (38).

  Para Buchain (9) os dados tratados deverão ser eliminados após o término de seu tratamento no âmbito e nos limites técnicos das atividades, como previsto no art 16 da LGPD, ou seja, os dados só poderão ser utilizados durante o período não excedente aquele necessário para atender a(s) finalidade(s) para as quais foram tratados.

- Cronograma de retenção de dados: quando os dados serão apagados a partir do momento em que não forem mais necessários (38).

4.2.1.4 Princípio da livre acesso

Para atender ao princípio do livre acesso, é necessário assegurar a facilidade e gratuidade sobre a forma e a duração do tratamento, além de garantir a integridade dos dados. Para atender esse princípio, as práticas identificadas foram:

- Consulta aos dados pessoais: garantir, aos titulares, consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais Brasil (6).
- Acesso aos dados pessoais: conceder, gratuitamente, o acesso aos dados, mediante requisição do titular ou de seu representante; Brasil (6)
- Formato de armazenamento dos dados pessoais: armazenar os dados pessoais em formato que favoreça o livre acesso pelo titular de dados pessoais Brasil (6).
- Criar e manter canal de comunicação exclusivo LGPD: fornecer informações e dados solicitados por meio eletrônico ou na forma impressa, a critério do titular de dados pessoais Brasil (6).

4.2.1.5 Princípio da qualidade dos dados

Para atender ao princípio da qualidade dos dados, é necessário garantir aos titulares, a exatidão, clareza, relevância e atualização dos dados. Para atender esse princípio, as práticas identificadas foram:

- Atualização dos dados: Realizar consultas frequentes para atualização dos dados do titular;
- Implantação de sistema para controle de fluxo de dados pessoais: de acordo com Daniel et al. (13), deve-se utilizar tecnologias de controle de fluxo de dados objetivando os registros das informações de saída e entrada, como também o bloqueio das mesmas em caso de não cumprimento dos papéis relacionados a Política de Proteção de Dados.
- Auditorias internas em sistemas que tratam dados pessoais: em conjunto a implementação de uma Política de Proteção de Dados, vem a necessidade de assegurar o cumprimento das diretrizes impostas na mesma. Para esse fim foram definidos períodos de análises de auditoria interna na instituição, a fim de encontrar possíveis apontamentos que de alguma forma estejam em desacordo com a Política proposta, e consequentemente em desconformidade com a Lei Geral de Proteção de Dados (13).

  Em razão desses deveres, observando o caso concreto, o controlador deverá corrigir e atualizar os dados do titular de dados, gratuitamente e mediante requerimento formulado pelo titular ou por seu representante. E, caso não possa adotar tais providências, cabe ao devedor informar ao titular (2).

4.2.1.6 Princípio da transparência

Para atender ao princípio da transparência, é necessário garantir a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação. Para atender esse princípio, as práticas identificadas foram:

- Declaração contendo a discriminação dos dados e de seus tratamentos: declaração clara e completa na qual indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial (33).

- Política Geral de Segurança da Informação: a Política de Segurança da Informação é um documento extremamente importante pois indica a toda organização quais são as diretrizes da empresa, em se tratando exclusivamente de Segurança da Informação. A elaboração e publicação desse documento é imprescindível, pois a partir dele diversos outros guias, normas e documentos podem ser criados (34).

  Uma vez implantada a política de segurança da informação, o aumento da transparência e a elevação da eficiência do negócio surgem como consequências naturais. Essa política deve ser mais clara possível, para que os colaboradores entendam como organizar a informação seguindo um padrão para facilitar os fluxos de processos em todas as escalas (15).

- Políticas de privacidade : é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário (8).

4.2.1.7 Princípio da segurança

Para atender ao princípio da segurança, é necessário manter os dados da pessoa física que está sendo tratada em um ambiente seguro. Para atender esse princípio, as práticas identificadas foram:

- Anonimização dos dados: segundo OLIVEIRA; MADEIRA; MONTEIRO (36), a anonimização consiste em utilizar técnicas visando impossibilitar a associação de um dado com o sujeito, com objetivo de proteger a identidade do titular e torná-lo não identificável.

  Segundo Fabio Correa Xavier (17) a anonimização seria mais adequada caso o controlador não precise mais fazer o tratamento de dados pessoais, mas tenha interesse em fazer análises nas atividades dos titulares, de forma genérica, sem trabalhar com qualquer dado que possa identificar o titular. Ou seja, se o controlador deveria eliminar os dados dos titulares mas por alguma razão tem interesse em manter alguns dados, a anonimização seria a opção.

- Criptografia: A criptografia em si não é um mecanismo mencionado na LGPD, contudo é uma técnica viável para garantir a segurança das informações. (36).

  De acordo com OLIVEIRA; MADEIRA; MONTEIRO (36), existem duas formas de criptografia:

  - Simétrica: método mais antigo, o remetente e o destinatário utilizam de uma única chave para codificar e decodificar a mensagem ou dado.

  Segundo ARNAUD (4) é recomendada quando desejar enviar uma mensagem criptografada rápida.

  - Assimétrica: é considerado o meio mais seguro, porém é mais lento e requer maior capacidade de processamento. Utiliza-se de duas chaves, uma pública que é utilizada para criptografar a mensagem ou dado, e uma chave privada que serve para decodificação.

  De acordo com ARNAUD (4) a criptografia assimétrica pode ser usada quando você tiver a chave pública OpenPGP verificada do seu destinatário.

- Controle de Acesso: a política de controle de acesso é tipicamente baseada no privilégio e direito de cada usuário autorizado, mas o acesso a todas as informações pode não ser necessário para todos os tipos de usuários. Por exemplo, um médico em questão pode recuperar os dados de seu paciente, mas nenhuma outra informação do paciente (43).

- Política de Backup: para Couto et al. (12) é recomendada a criação de uma política com detalhamento dos procedimentos de backup, armazenamento, cópia na nuvem e os responsáveis pela execução.

- Privacy by default: segundo PARO; SILVA (38), Privacy by default é uma decorrência do Privacy by Design, conforme informado por Henrique Dantas no blog Advogatech (2019), significa que ao ser lançado no mercado, um produto ou serviço, deve vir por padrão, com as configurações de privacidade no modo mais restrito possível, ou seja, todas as medidas de proteção da privacidade que foram formadas desde o início do projeto, considerando o princípio do Privacy by Design.

  São coletados apenas os dados essenciais para entregar produto ou prestar um serviço, mesmo assim o usuário ainda deve saber para qual finalidade está sendo utilizada, para quem estão sendo compartilhadas as suas informações e com qual propósito.

- Implantação de sistema para registro e tratamento de logs: o tratamento de logs surgiu da importância da rastreabilidade imposta pela Lei Geral de Proteção de Dados, tanto para atendimento direto a ANPD quanto a solicitação de Titulares de Dados. Nesse quesito foi importante a implantação de sistema próprio para esse tipo de guarda e amostragem de informação (13).

- Privacy by Design: o Privacy by Design fornece uma visão holística e uma perspectiva preventiva da proteção de dados. Sua aplicação atravessa toda a estrutura do negócio, de

ponta a ponta, incluindo informações, práticas e processos de negócios, design físico e em rede, e sua infraestrutura, com o objetivo de atingir uma soma positiva na interação, mutuamente benéfica, entre privacidade como padrão de negócio e tecnologia (32).

A Lei Geral de Proteção de Dados prevê em seu artigo 46, artigo 2º, que os agentes de tratamento devem adotar medidas de segurança técnicas e administrativas desde a concepção, ou seja, refere-se à ideia de privacy by design.

Acima de tudo, Privacy by Design exige que controladores e operadores mantenham os interesses do titular, oferecendo medidas como fortes padrões de privacidade e notificação apropriada (48).

4.2.1.8 Princípio da prevenção

Para atender ao princípio da prevenção, é necessário adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Para atender esse princípio, as práticas identificadas foram:

- Fomentar o desenvolvimento de estratégias de segurança da informação: segundo Albuquerque; Ribeiro (1) há três princípios básicos para garantir a segurança da informação:
  - Confidencialidade. a informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso.
  - Disponibilidade. a informação deve estar disponível no momento em que a mesma for necessária.
  - Integridade. a informação deve ser recuperada em sua forma original (no momento em que foi armazenada). É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

- Perfis comportamentais: para PARO; SILVA (38), é importante traçar os perfis comportamentais dos riscos, listando os possíveis *gaps* de uso dos dados sensíveis, por exemplo, finalidade de uso dos dados, necessidade, compartilhamento, transparência, qualidade dos dados e medidas de segurança.

- Relatórios de impacto de privacidade: relatórios de impacto de privacidade devem conter a descrição do risco, uma nota para a probabilidade e uma nota para o impacto. Estas notas serão de 1 até 5, onde 1 é o cenário menos preocupante e 5 o cenário mais preocupante. Após dadas as notas para cada risco, ele será identificado como Risco Extremo, Elevado, Moderado e Baixo. Com base nessa análise de riscos, deve-se priorizar as correções para os itens conforme o nível de urgência (42).

- Análise de risco e de impactos relacionados a dados pessoais: de acordo com Daniel et al. (13), a realização da análise de risco em privacidade de dados veio com o objetivo de fazer uma análise dos impactos relacionados a manipulação dos dados e garantia da privacidade diante da nova lei. Essa análise levou em consideração as vulnerabilidades e ameaças encontradas, gerando assim os possíveis impactos para a instituição em caso da não atendimento correto à lei.

4.2.1.9 Princípio da não discriminação

Para atender ao princípio da não discriminação, é necessário garantir que o tratamento de dados não pode ser realizado para fins discriminatórios ilícitos ou abusivos. Para atender esse princípio, as práticas identificadas foram:

- Orientar os colaboradores e os responsáveis pelo tratamento dos dados: a Lei de Proteção de Dados prevê, como uma obrigatoriedade: "orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais" (6).

- Criação de um material de divulgação interno para os colaboradores: material de divulgação interno para os colaboradores, descrevendo como a empresa se comporta em relação aos tratamentos dos dados e informações, e esclarecendo os papéis e responsabilidades, inclusive sobre a discriminação (42).

4.2.1.10 Princípio da responsabilização

Para atender ao princípio da responsabilização, é necessário ser responsável por todas as medidas que forem adotadas com o objetivo de atender as exigências legais e princípios nela estabelecidos e que acima de tudo sejam eficazes. Para atender esse princípio, as práticas identificadas foram:

- Prestação de contas: trata-se de um balanço financeiro fundamental para instituições que dão importância máxima à transparência operacional. Devem estar descritas num documento as despesas detalhadas, entradas de dinheiro, com origem e o total de ativos e passivos, além de patrimônio líquido e bruto. Ou seja, é um relatório detalhado que contém todas as transações financeiras da empresa (16).

- Nomeação do encarregado: segundo Quispe; Custodio (40), a nomeação do DPO é uma obrigação imposta pela lei, esse encarregado deve obter conhecimento técnico jurídico e regulatório em proteção de dados suficiente para conduzir as definições pela empresa. Ademais, o profissional que vai atuar dentro do cenário de proteção de dados, será o intermediador entre os titulares dos dados, as organizações e os órgãos de fiscalização, a

partir disso, a empresa vai poder aplicar uma série de outras políticas de proteção de dados e privacidade, como por exemplo: treinamento de equipes da área de compliance,e o mais importante, a criação de uma cultura de proteção de dados em todos os seguimentos da empresa, trazendo assim, mais confiabilidade e credibilidade à organização.

- Plano de Continuidade de Negócios: deve-se elaborar um Plano de Continuidade de Negócios, que possa fornecer respostas aos eventuais incidentes que possam ocorrer na empresa, e que contemple as obrigações da empresa como custodiante dos dados e o zelo pela operação do negócio (42).

- Revisão jurídica: Sabino (42) diz que deve ser feita a revisão jurídica e atualização das cláusulas de contratos com parceiros e fornecedores que realizam algum tipo de tratamento de dados, principalmente fornecedores de soluções em nuvem, email marketing e mídias sociais.

4.2.2 Estruturação de orientações de adequação

Com o objetivo de apresentar orientações para adequação à LGPD, foi elaborado um conjunto de recomendações através de práticas e ações a serem implementadas para cada princípio da lei. Visando sintetizar as informações encontradas e para facilitar a compreensão das mesmas foi elaborado pelo autor a tabela 1 contendo as necessidades de adaptação da LGPD separadas por princípio.

Princípio	**Dever do controlador**	**Práticas adotadas**
Princípio da finalidade	Fazer a coleta precisa dos dados e informar ao titular a finalidade com que os dados serão utilizados	- Mapeamento dos dados - Categorização dos dados - Termos de uso - Levantamento do mapa de finalidades de dados
Princípio da adequação	Tratar os dados visando a compatibilidade com as finalidades informadas ao titular	- Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento - Norma de Uso Aceitável de Ativos da Informação
Princípio da necessidade	Ponderar entre o que é realmente essencial para o seu negócio	- Minimização dos dados - Política de retenção de dados - Cronograma de retenção de dados
Princípio do livre acesso	Assegurar a facilidade e gratuidade sobre a forma e a duração do tratamento, além de garantir a integridade dos dados	- Consulta aos dados pessoais - Acesso aos dados pessoais - Formato de armazenamento dos dados pessoais - Criar e manter canal de comunicação exclusivo LGPD

Princípio	**Dever do controlador**	**Práticas adotadas**
Princípio da qualidade dos dados	Deve garantir aos titulares, a exatidão, clareza, relevância e atualização dos dados	- Atualização dos dados - Implantação de sistema para controle de fluxo de dados pessoais - Auditorias internas em sistemas que tratam dados pessoais
Princípio da transparência	Garantir a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação	- Declaração contendo a discriminação dos dados e de seus tratamentos - Política Geral de Segurança da Informação - Políticas de privacidade
Princípio da segurança	Manter os dados da pessoa física que está sendo tratada em um ambiente seguro	- Anonimização dos dados - Criptografia - Controle de Acesso - Política de Backup - Privacy by default - Implantação de sistema para registro e tratamento de logs - Privacy by Design
Princípio da prevenção	Adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais	- Fomentar o desenvolvimento de estratégias de segurança da informação - Perfis comportamentais - Relatórios de impacto de privacidade - Análise de risco e de impactos relacionados a dados pessoais

Princípio	Dever do controlador	Práticas adotadas
Princípio da não discriminação	O tratamento de dados não pode ser realizado para fins discriminatórios ilícitos ou abusivos	- Orientar os colaboradores e os responsáveis pelo tratamento dos dados - Criação de um material de divulgação interno para os colaboradores
Princípio da responsabilização	Ser responsável por todas as medidas que forem adotadas com o objetivo de atender as exigências legais e princípios nela estabelecidos e que acima de tudo sejam eficazes	- Prestação de contas - Nomeação do encarregado - Plano de Continuidade de Negócios - Revisão jurídica

Tabela 1 - Necessidades de adaptação por princípio da LGPD

4.2.3 Entrevista com especialista

Nesta seção é descrita a entrevista realizada com o especialista com a finalidade de validar as práticas identificadas e descritas na etapa 1 da pesquisa.

A entrevista com o especialista teve como objetivo entender o contexto da empresa, identificar as práticas utilizadas para adequação e desafios enfrentados naquele contexto específico. A pesquisa foi realizada com um especialista que atuou como DPO na implementação da LGPD numa empresa de desenvolvimento de software situada no estado de Santa Catarina.

A empresa armazena no seu sistema dados pessoais de clientes, empregados, fornecedores, contratados, entre outros. A segurança dos dados sempre foi um tema de grande preocupação, mesmo antes da LGPD. Porém, a Lei Geral de Proteção de Dados trouxe orientações claras do que deve ser implementado sobre segurança dos dados. A empresa procurava seguir os padrões de segurança, porém sempre encontrava dificuldades em estabelecer práticas e medir a sua aderência, sendo esta dificuldade sanada com a LGPD.

A empresa na primeira fase de implementação de ações e práticas para se adequar a LGPD, a empresa atacou os pontos que ela considerava mais críticos em relação a LGPD, com planos para num segundo momento conseguir se adequar de maneira mais ampla. Esta escolha se deu pelo impacto da segurança do negócio e questões financeiras, como multas. Durante a entrevista os pontos abordados foram sobre segurança e quais as práticas que a empresa adotou nessa primeira etapa que foram:

- Mapeamento e categorização dos dados: A empresa começou o processo de mapeamento dos dados fazendo uma triagem de todos os dados que precisavam do consentimento do

usuário, principalmente nos dados que são compartilhados com terceiros.

- Controle de acesso: Foi implementado no software funcionalidades que permitem o cliente definir múltiplos níveis de acesso, personalizando de acordo com cada necessidade. Isso permitiu autonomia para o cliente que atua como controlador dos dados. Em vez de anonimizar dados, apenas o usuário com perfil criado terá acesso as informações que são da finalidade do seu perfil.

- Medidas socioeducativas: Sempre que um novo colaborador entra na empresa é realizado treinamento para conscientização sobre a LGPD e disponibilizado material digital e impresso.

- Criptografia: A empresa não utiliza nenhum método de criptografia, contudo, no que se refere a segurança ao acesso dos dados existe uma preocupação muito grande, estando estes em um ambiente de servidor seguro com múltiplos níveis e com um design de infraestrutura muito forte.

- Privacy by default: Atualmente a empresa utiliza de forma parcial o privacy by default. Ao fazer o primeiro acesso são divulgados os termos de uso e a política de privacidade ao usuário. A partir disso o default da aplicação é sobre o negócio, deixando a responsabilidade do não vazamento de dados pessoais por conta do usuário.

Além das práticas citadas acima, a empresa já possuía, antes da LGPD, um sistema de registro e tratamento de log e uma política de backup. Outras práticas estão em vias de implementação com a ajuda de uma consultoria especializada, sendo elas: política de segurança interna e anonimização de parte dos dados.

Para a empresa o grande desafio para atender os requisitos de segurança impostos pela LGPD foi a refatoração da aplicação, pois esta, quando desenvolvida, não foi pensada para suprir os termos que a lei impôs. Além disso, descobrir, elencar, priorizar os problemas e definir a melhor estratégia para sua resolução foram questões importantes que apareceram no percurso de adequação a lei.

Se pudesse começar do zero a adequação à LGPD, a empresa optaria por uma estratégia diferente, anonimizaria todos os dados pessoais possíveis e planejaria uma arquitetura de software utilizando privacy by design para construir desde o princípio uma aplicação pensando nas questões de segurança.

5 CONSIDERAÇÕES FINAIS

O problema da privacidade de dados e da fraude de sistemas de informação é latente e precisa ser uma preocupação constante dos profissionais de tecnologias da informação que lidam com dados pessoais. A LGPD apresentou um impacto significativo para empresas de desenvolvimento de software, tanto na parte organizacional como na parte técnica na estruturação de um software compatível com as novas exigências da lei.

Este trabalho teve como objetivo principal identificar algumas práticas para implementação da LGPD que podem ser aplicadas em empresas de desenvolvimento de software. Baseado numa vasta pesquisa na literatura foram identificados trabalhos de estudo de caso de aplicação da lei, sendo possível extrair as práticas que são compatíveis a empresas de software. Finalizamos com uma tabela com as práticas que podem ser utilizadas para atender cada princípio da lei, sendo este uma compilação final deste trabalho. O objetivo é tornar simplificada a compreensão da adequação das empresas de software à LGPD.

Para validação adicional foi realizada entrevista com um especialista que atuou como DPO na implementação da LGPD numa empresa de desenvolvimento de software. Esta etapa procurou identificar as práticas utilizadas para adequação ao princípio de segurança e os principais desafios enfrentados por ele, consolidando as práticas encontradas no referencial teórico e que serviram de base para a estrutura do trabalho.

5.1 TRABALHOS FUTUROS

Com o objetivo de dar continuidade neste trabalho recomenda-se os seguintes trabalhos futuros:

- Fazer pesquisa com mais profissionais que atuaram como DPO em empresas de desenvolvimento de software, com a finalidade de identificar os desafios enfrentados e aprendizados.
- Realizar entrevista com empresas que desenvolvem software para outras áreas, como por exemplo área financeira e de recursos humanos, para identificar outras necessidades de adequação à LGPD que não foi possível identificar neste pesquisa.

REFERÊNCIAS

1 ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no desenvolvimento de software**. [S.l.]: Elsevier Brasil, 2002.

2 ANCHIETA, Luıza Jalil. **Os deveres do controlador de dados pessoais**. 2022. B.S. thesis – Universidade Federal do Rio Grande do Norte.

3 ANPPD. Proposta com os elementos necessários para uso em licitações de Projetos de Adequação à Lei 13.709/2018 – LGPD nas câmaras e prefeituras brasileiras. In.

4 ARNAUD. **Criptografia simétrica x assimétrica: qual é a diferença?** [S.l.: s.n.], 2021. Disponível em: https://blog.mailfence.com/pt/criptografia-simetrica-x-assimetrica-qual-e-a-diferenca/#:~:text=Qual%20criptografia%20voc%C3%AA%20deve%20usar,OpenPGP%20verificada%20do%20seu%20destinat%C3%A1rio.. Acesso em: 22 janeiro 2023.

5 BARBIERI, Carlos. **Governança de Dados: Práticas, conceitos e novos caminhos**. [S.l.]: Alta Books, 2020.

6 BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. In.

7 _____. LEI Nº 13.853, DE 8 DE JULHO DE 2019. In.

8 _____. Oficina Termo de Uso e Política de Privacidade. In.

9 BUCHAIN, Luiz Carlos. Minimização e proporcionalidade na coleta de dados. **Direitos Democráticos & Estado Moderno**, v. 2, n. 5, p. 51–68, 2022.

10 CAMPOS, André. Sistema de segurança da informação: controlando os riscos. **Santa Catarina: Visual Books**, 2007.

11 CAVOUKIAN, Ann et al. Privacy by design: The 7 foundational principles. **Information and privacy commissioner of Ontario, Canada**, v. 5, p. 12, 2009.

12 COUTO, Karlla Soares et al. A Adequação de uma Associação Comercial à LGPD: Um Estudo de Caso. **Journal of Technology & Information (JTnI)**, v. 2, n. 3, 2022.

13 DANIEL, Maycon Antônio et al. A evolução e aplicação da segurança da informação por meio da lei geral de proteção de dados pessoais (lgpd): um estudo de caso em uma instituição financeira. Araranguá, SC, 2022.

14 DIAS, José Lucas Costa. As sanções administrativas da lgpd, responsabilidade e ressarcimento de danos: uma ótica a partir da violação aos dados pessoais pelo compartilhamento irregular e falta de segurança da informação. Pontifıcia Universidade Católica de Goiás, 2021.

15 DOCUSIGN. **Política de segurança da informação: saiba como e por que desenvolvê-la**. [S.l.: s.n.], 2018. Disponível em: https://www.docusign.com.br/blog/politica-de-seguranca-da-informacao-saiba-como-e-por-que-desenvolve-la. Acesso em: 18 janeiro 2023.

16 EXPENSEON. **10 benefícios da adequação à LGPD**. [S.l.: s.n.], 2021. Disponível em: https://expenseon.com/gestao-de-despesas/prestacao-de-contas/. Acesso em: 26 novembro 2022.

17 FABIO CORREA XAVIER. **O uso dos processos de anonimização e pseudonimização no contexto da LGPD**. [S.l.: s.n.], 2021. Disponível em: https://www.migalhas.com.br/depeso/342896/o-uso-dos-processos-de-anonimizacao-e-pseudonimizacao-da-lgpd. Acesso em: 22 janeiro 2023.

18 FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani. Comentários à lei geral de proteção de dados: Lei 13.709/2018. **São Paulo: Revista dos Tribunais**, 2019.

19 FERREIRA, Fernando Nicolau Freitas. **Polıtica de segurança da informação: guia prático para elaboração e implementação**. [S.l.]: Ciência Moderna, 2008.

20 FREITAS, Carla. **Como elaborar uma polıtica de privacidade aderente à LGPD**. [S.l.: s.n.], 2021.

21 FROIS, Rebecca de Araujo. LGPD: mecanismos de segurança, da invasão à proteção de dados.

22 GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados (LGPD): guia de implantação**. [S.l.]: Editora Blucher, 2020.

23 GIARLLARIELLI, GUSTAVO. **10 benefícios da adequação à LGPD**. [S.l.: s.n.], 2021. Disponível em: https://giarllarielli.jusbrasil.com.br/artigos/1193028119/10-beneficios-da-adequacao-a-lgpd. Acesso em: 15 janeiro 2022.

24 GIL, Antonio Carlos. **Estudo de caso**. [S.l.]: Atlas, 2009.

25 GRÖNE, FLORIAN AND PÉLADEAU, PIERRE AND SAMAD, RAWIA ABDEL. **Tomorrow's data heroes**. [S.l.: s.n.], 2019. Disponível em: https://www.strategy-business.com/article/Tomorrows-Data-Heroes. Acesso em: 19 dezembro 2021.

26 GÜRSES, Seda; TRONCOSO, Carmela; DIAZ, Claudia. Engineering privacy by design. **Computers, Privacy & Data Protection**, v. 14, n. 3, p. 25, 2011.

27 HENRIQUES , PEDRO. **A importância da Segurança da Informação com a LGPD em vigor**. [S.l.: s.n.], 2021. Disponível em: https://indicca.com.br/seguranca-da-informacao-3/#:~:text=A%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%20tem,valores%20e%20prop%C3%B3sito%20da%20empresa.. Acesso em: 03 fevereiro 2022.

28 KAUER, Gisele. **Controlador, operador e encarregado: Quem é quem na LGPD**. [S.l.: s.n.]. https://infranewstelecom.com.br/controlador-operador-encarregado-quem-e-quem-na-lgpd/.

29 LIMA, Cıntia Rosa Pereira de. **ANPD e LGPD: Desafios e perspectivas**. [S.l.]: Digitaliza Conteudo, 2021.

30 LIMA, Victtor Henrique. LGPD Análise dos impactos da implementação em ambientes corporativos: Estudo de caso. Pontificia Universidade Católica de Goiás, 2020.

31 MARINHO, Fernando. **Os 10 Mandamentos da LGPD - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos.** [S.l.]: Grupo GEN, 2020.

32 MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princıpio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. **Revista Eletrônica Direito e Polıtica**, v. 15, n. 3, p. 955–984, 2020.

33 MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, v. 1009, 2019.

34 NARDELLI, Cleber. Segurança da Informação e LGPD Aplicado no Desenvolvimento de Software. In: SBC. ANAIS da V Escola Regional de Engenharia de Software. [S.l.: s.n.], 2021. p. 169–178.

35 NUNES, Natália Martins. **princıpios da LGPD para o tratamento de dados pessoais. 2019**. [S.l.: s.n.], 10.

36 OLIVEIRA, Erick de; MADEIRA, Humberto dos Santos; MONTEIRO, Pedro Augusto Migliari. A lei geral de proteção de dados pessoais e a anonimização de dados: uma aplicação da técnica em uma base de dados real. 168, 2020.

37 OLIVEIRA, Ricardo. **LGPD: Como evitar as sanções administrativas**. [S.l.]: Saraiva Educação SA, 2021.

38 PARO, Patrıcia Cristina Azevedo; SILVA, Vitor Luiz Santiago da. Inıcio de adequação à lei geral de proteção de dados: estudo de caso da empresa multinacional alemã de engenharia e eletrônica. 004, 2020.

39 PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD**. [S.l.]: Saraiva Educação SA, 2020.

40 QUISPE, Lizeth Daniela Villcacuti; CUSTODIO, Lucas Roberto. Um Estudo de Caso no Âmbito da LGPD em Empresas de Pequeno Porte na Região de Arthur Nogueira. In: FATECSEG-CONGRESSO de Segurança da Informação. [S.l.: s.n.], 2021. v. 1.

41 RPP TECNOLOGIA. **POLÍTICA DE PRIVACIDADE DO USUÁRIO DOS SISTEMAS**. [S.l.: s.n.], 2021. Disponível em: https://www.ereceita.net.br/download/LGPD/LGPD_RPP_politica_privacidade_sistemas.pdf. Acesso em: 15 fevereiro 2022.

42 SABINO, Richard. Gestão da segurança da informação orientado a LGPD: impactos da implantação das mormas LGPD nos processos da ADM Sistemas LTDA. **Tecnologia em Gestão da Tecnologia da Informação-Unisul Virtual**, 2020.

43 SANTOS, Allan CN et al. Aplicações em redes de sensores na área da saúde e gerenciamento de dados médicos: tecnologias em ascensão. **Sociedade Brasileira de Computação**, 2020.

44 SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva. Rio de Janeiro: Ed**. [S.l.]: Campus, 2003.

45 SILVA REGIS, Erick da. LINHAS GERAIS SOBRE A LEI 13.709/2018 (A LGPD): OBJETIVOS, FUNDAMENTOS E AXIOLOGIA DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA E A TUTELA DE PERSONALIDADE/PRIVACIDADE. **matéria**, v. 8, p. 9.

46 SOUZA, Thiago de Almeida. Um estudo da LGPD para nortear o desenvolvimento de novos sistemas e a manutenção de sistemas legados. 002, 2021.

47 VASCONCELOS , KLEBER. **Os benefícios da implementação da LGPD**. [S.l.: s.n.], 2020. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/beneficios-riscos-lgpd-empresas. Acesso em: 12 dezembro 2021.

48 WAGNER BARCELOS. **Privacy By Design: conceito e aplicação na prática**. [S.l.: s.n.], 2020. Disponível em: https://www.securityreport.com.br/colunas-blogs/privacy-by-design-conceito-e-aplicacao-na-pratica/#.ZAEqInbMKUk. Acesso em: 28 janeiro 2023.