FACULDADE DE TECNOLOGIA DE SÃO PAULO
THIAGO DE ALMEIDA SOUZA

Um estudo da LGPD para nortear o Desenvolvimento de Novos Sistemas e a manutenção de Sistemas Legados

SÃO PAULO
2021

FACULDADE DE TECNOLOGIA DE SÃO PAULO
THIAGO DE ALMEIDA SOUZA

Um estudo da LGPD para nortear o Desenvolvimento de Novos Sistemas e a manutenção de Sistemas Legados

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.
Orientador: Professor Me. Valter Yogui

SÃO PAULO
2021

FACULDADE DE TECNOLOGIA DE SÃO PAULO
THIAGO DE ALMEIDA SOUZA

Um estudo da LGPD para nortear o Desenvolvimento de Novos Sistemas e a manutenção de Sistemas Legados

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Parecer do Professor Orientador
aprovado

Conceito/Nota Final: 9,0

Atesto o conteúdo contido na postagem do ambiente TEAMS pelo aluno e assinada por mim para avaliação do TCC.

Orientador: Professor Me. Valter Yogui

SÃO PAULO, 21 de junho de 2021.

Assinatura do Orientador

Assinatura do aluno

AGRADECIMENTOS

A todos os professores que pavimentaram o caminho para que eu pudesse chegar até aqui. E principalmente ao Professor Valter Yogui por aceitar ser meu orientador nesse projeto, suas aulas foram uma grande inspiração para o tema e sua ajuda foi o diferencial a esse trabalho.

À Professora Grace Anne Ponte Borges, por todo incentivo e pelas várias aulas em matérias diferentes. Por permitir ajudar com o trabalho no Projeto das Fatech Girls e por nos apoiar nos momentos que mais precisamos.

À Professora Neide Itocazu, por me aconselhar no tema e por me ajudar a focar e não querer abraçar o mundo todo de uma vez. Suas aulas sempre foram atrativas e fora da caixa, ajudando a aprender sem ficar preso a amarras.

A todos os amigos do RPG, Amaral, Déra, Elet, Melmer, Momo, Pitre, Rafaelfo, Red, Reik e Zimbro, por fazer dessa pandemia um pouco mais aturável e me impedir de surtar de vez, ao me fazer viajar por histórias incríveis e momentos memoráveis ao longo desse ano.

À Camila Gamino, por além de me aturar no RPG, me ajudar a enfrentar esse boss final, com dicas, sugestões e por estabelecer prazos para que eu funcionasse melhor. Rumo à Odisseia e a vigésima masmorra.

À minha equipe do trabalho, a melhor equipe de WFM que existe, que conseguiu planejar maneiras de me deixar trabalhar nesse projeto para poder me formar.

Aos amigos da faculdade, Rafael Galo e Vagner Cruz, que além de formar a melhor equipe para todos os trabalhos, ainda vão ser os melhores padrinhos de casamento do mundo.

À Dra Roberta Ruedas, por me ajudar nesse trabalho e por todos os eventos que fomos juntos, e por ser uma excelente madrinha de casamento.

Ao meu amigo de sempre, irmão da época da escola que me atura há mais de 20 anos, Marcos Felipe, obrigado por nunca desistir de mim e da nossa amizade, mesmo eu muitas vezes não merecendo.

Ao meu irmão, Victor Souza que me ajudou nos momentos que eu mais precisei, me apoiou em todas as transições da vida e que sempre que eu puder, vou manter perto de mim, para me aturar.

À minha mãe Marcia e minha vó Leny, que cuidaram de mim e são totalmente responsáveis pelo ser humano que me tornei hoje, e que se sou capaz de fazer ou alcançar qualquer objetivo, é porque vocês trabalharam duro para que eu pudesse trilhar esse caminho.

E por último, mas não menos importante, para minha noiva Michelli que literalmente mudou minha vida, me fazendo mudar de estado. Só entrei na faculdade por causa dela, e não teria aguentado passar por tudo isso sem seu apoio, literal, já que fizemos o curso juntos, e espero que essa parceria continue por toda eternidade. Uma caixinha de bombom e um buquê de flores. Obrigado, te amo, mais do que amanhã, menos do que ontem, e só a gente entende isso.

“Se não existe um meio de vencer o inimigo, crie um meio! Se não há chance de vitória, encontre uma”.

Mestre Arsenal.

RESUMO

A Lei Geral de Proteção de Dados (LGPD), 13.709/2018 regulamenta o acesso, gestão, armazenamento e compartilhamento dos dados pessoais de usuários por todo e qualquer serviço digital em funcionamento no território nacional. Dado pessoal é todo aquele relacionado à pessoa natural identificada ou identificável, tais como números, características pessoais, qualificação pessoal, dados genéticos. Alguns dados são considerados sensíveis, trata-se de informações que podem ser utilizadas de forma discriminatória, e carecem de proteção especial. Essa lei tem grande impacto nas relações comerciais e de consumo, já que a coleta de dados se tornou um padrão no desenvolvimento de sistemas para o tratamento de dados pessoais com a finalidade de traçar perfis de consumo, condições financeiras e de crédito e até mesmo opiniões pessoais. Uma empresa estando em não conformidade com a lei pode gerar consequências severas, desde advertências e multas, até mesmo a proibição do tratamento de dados como um todo.

Palavras-Chave: LGPD, Dados, Conformidade, Desenvolvimento.

ABSTRACT

The General Data Protection Law (LGPD), 13.709/2018 regulates the access, management, storage and sharing of users personal data by all digital services operating in the national territory. Personal data is any data related to an identified or identifiable natural person, such as ID numbers, personal characteristics, personal qualification, genetic data. Some data is considered sensitive, it is information that can be used in a discriminatory way, and it needs special protection. This law has a great impact on commercial and consumer relations, as data collection has become a standard in the development of systems for the processing of personal data to trace consumption profiles, financial and credit conditions, and even personal opinions. A company not complying with the law can generate severe consequences, from warnings and fines, even the prohibition of data processing as a whole.

Keywords: LGPD; Data; Compliance; Development

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABES – Agência Brasileira das Empresas de Software

ANPD – Autoridade Nacional de Proteção de Dados

DFD – Diagrama de Fluxo de Dados

DPO – Data Protection Officer

GDPR - General Data Protection Regulation

IDC – International Data Corporation

LGPD – Lei Geral de Proteção de Dados

RIPD – Relatório de Impacto à Proteção de Dados Pessoais

SUMÁRIO

1 INTRODUÇÃO

Com o desenvolvimento de novas tecnologias, dados tem se tornado cada vez mais a mercadoria importante e desejada da era digital, pois quanto maior o volume de dados tratados por determinada empresa ou pessoa, maior o poder que ela exercerá, podendo afetar desde o mercado de consumo até mesmo o destino eleitoral de algum país. E é justamente o olhar nesse poder, que uma legislação específica foi criada para tratar sobre a privacidade de dados e regras para a sua utilização. O mundo já está atento para isso com mais cuidado, e vários países já estão criando Leis para cuidar dessas questões, como a General Data Protection Regulation (GDPR) da União Europeia, e em partes pelo Marco Civil no Brasil. A Lei Geral de Proteção de Dados (LGPD), ou Lei Nº 13.709, de 14 de agosto de 2018, regulamenta o tratamento de dados pessoais, inclusive por meios não digitais, por qualquer pessoa ou serviço digital em funcionamento no Brasil, ela entraria em vigor em agosto de 2020, mas devido ao contexto da Pandemia, foi adiada para maio de 2021.

As empresas deverão passar por várias transformações, passando por treinamentos e até mesmo aderindo a uma nova cultura de tratamento de dados e de cibersegurança, e pensar em privacidade e proteção destes, em todas as etapas do trabalho, desde o início do desenvolvimento dos sistemas até a execução. As sanções pelo descumprimento da lei são bem pesadas, podendo variar de multa e podendo chegar até mesmo à proibição de fazer qualquer tipo de tratamento de dados no Brasil. Segundo um levantamento da Associação Brasileira das Empresas de Software, 56% das empresas de tecnologia ainda precisam se adequar a nova Lei (ITFORUM, 2020). É necessário a elaboração de processos claros e extensos e da disponibilização de recursos adequados para evitar vazamentos de informações e da mitigação dos riscos de usos inadequados dos dados, gerando a necessidade de profissionais especializados no estudo da lei, de tecnologia e dos processos internos da empresa, como o data protection officer (DPO).

Nesta monografia serão explicados os principais pontos da Lei Geral de Proteção de dados, os principais passos para a sua implementação e suas aplicações e nortear o desenvolvimento de novos sistemas, se estendendo também aos sistemas já em funcionamento.

2 A LEI GERAL DE PROTEÇÃO DE DADOS

2.1 A IMPORTÂNCIA DOS DADOS

Com os constantes avanços tecnológicos nos últimos anos, a criação de dados tem praticamente dobrado a cada dois anos, segundo pesquisa divulgada recentemente pelo International Data Corporation (IDC) tornando dados pessoais uma das mercadorias mais valiosas e disputadas dos próximos anos (IDC 2020).

Com uma quantidade cada vez maior de dados pessoais sendo comercializada e até mesmo distribuída sem permissão, tornou-se imperativo o debate sobre leis específicas para tratar e proteger a privacidade dos dados e as regras para a utilização deles. Vários países já começaram a debater sobre isso, tendo como exemplo mais recente e importante a GDPR, concebido pela União Europeia para proteger os dados e a identidade dos seus cidadãos, concebido em 2012 e aprovado em 2016. Mesmo já existindo algumas leis relacionadas à privacidade desde 1995, simplesmente atualizar não seria suficiente para colocar de acordo com a situação técnica atual. A partir daí, tomou-se a decisão de uma nova regulamentação, que foi aplicada em maio de 2018.

Com o advento do GDPR, o Brasil se viu na necessidade de discutir extensivamente uma lei específica de proteção de dados, que acabou culminando na Lei nº 13709/2018, conhecida como a LGPD, que foi lançada em setembro de 2020, mas devido ao cenário de Pandemia, foi postergada para agosto de 2021.

2.1.1 Apresentando a lei

A LGPD dispõe sobre o tratamento de dados pessoais, em meios digitais ou não, por pessoa natural ou jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, e determina como os dados dos cidadãos podem ser coletados, tratados e prevê as punições caso haja transgressões. Com o regramento para o uso de dados pessoais no Brasil, tanto no âmbito online quanto offline, nos setores públicos ou privados, o país tenta complementar as leis já existentes que tratam da proteção à privacidade e dados pessoais e tornar o país mais competitivo numa sociedade cada vez mais movida a dados.

Um dos principais objetivos da lei é deixar claro aos usuários como seus dados estão sendo tratados. No momento em que são coletados, é necessário expor a forma que esses dados podem ou não serem utilizados, e para isso é necessário o consentimento do usuário, dando assim a ele a opção de aceitar ou não essas condições.

2.1.2 Sobre Os Tipos De Dados

Entende-se como dados pessoais qualquer informação relacionada a pessoa natural identificada ou identificável, tal como nome, RG, CPF ou e-mail. Tratamento de dados pessoais é toda operação realizada com dados pessoais que se referem a coleta, produção, classificação, recepção, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, eliminação, avaliação ou controle da informação, modificação comunicação, transferência, difusão ou extração.

Os dados pessoais também podem ser classificados como dados pessoais sensíveis, que podem gerar algum tipo de discriminação, por exemplo os dados sobre origem cultural, racial ou étnica, crenças religiosas e opiniões políticas, dados referentes a saúde ou a vida sexual e dados genéticos ou biométricos.

2.2 TRATAMENTO DE DADOS

Após o usuário fornecer os dados de forma consciente e voluntária, as empresas, por sua vez, podem utilizá-los de maneira que seja interessante para o seu negócio, ainda precisando respeitar as normas da lei para serem tratados de maneira correta, A lei reforça a necessidade de deixar claro e transparente a utilização dos dados para cada coleta, armazenamento, utilização, transmissão, modificação ou eliminação, assim, caso haja algum vazamento de dados ou qualquer tipo de problema, será possível resolver ou contornar o acontecido e garantir ao usuário que tudo está sob controle. Segundo Holzner e Holzner (2006) transparência é o fluxo aberto de informações, dependendo do acesso à informação que é tida como verdadeira e detida pelas autoridades.

Esse controle também é necessário, pois o usuário tem o direito de pedir os dados e as informações que a empresa tem sob ele sempre que achar necessário.

Assim, é importante que os controladores desses dados tenham as ferramentas certas para atender a demanda de acesso ou correção dessas informações. Garantindo assim a transparência total dos no tratamento dos dados.

2.2.1 Princípios no Tratamento de Dados

As atividades definidas no art. 6º da LGPD trazem os principais termos sobre o tratamento de dados. Ele afeta todas as atividades que envolvam utilização de dados pessoais, sejam pela internet ou fora dela, de consumidores, empregados ou qualquer tipo de pessoa.

> I - Finalidade: realização do tratamento para propósitos informados ao titular, sem possibilidade de tratamento posterior;
>
> II – Adequação: compatibilidade do tratamento com as finalidades informadas ao titular;
>
> III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades;
>
> IV - Livre Acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - Qualidade dos dados: garantia de exatidão, clareza, relevância e atualização dos dados;
>
> VI - Transparência: garantia de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;
>
> VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas;
>
> VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - Responsabilização e prestação de contas: demonstração 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. (BRASIL, 2018).

Seguindo esses princípios estabelecidos, é possível obter uma padronização de normas únicas e harmônicas por todos os agentes controladores que fazem parte do tratamento e da coleta de dados.

2.3 PRINCIPAIS MUDANÇAS

Com o advento da lei, as empresas desenvolvedoras de sistemas deverão se ajustar a novas práticas e condutas para seu modelo de desenvolvimento, armazenamento e captura de dados. Os principais afetados por essas mudanças podem ser separados em Operadores e Controladores.

De acordo com o Art. 37, os Controladores e os Operadores são os agentes que processam os dados pessoais e devem registar as operações de tratamento que realizam, especialmente quando se baseiam em interesses legítimos (BRASIL, 2018). O Controlador é o usuário final do Software, que utiliza o tratamento dos dados e toma decisões com eles, também é responsável por indicar um carregado, normalmente um DPO, pelo tratamento dos dados pessoais, podendo ele ser pessoa física ou jurídica e vai atuar como ponte de comunicação entre o Controlador e a Autoridade Nacional de Proteção de Dados (ANPD), ele deverá supervisionar todas as práticas de tratamento de dados sensíveis e garantir que eles estão em conformidade com a Lei de Proteção de dados.

O Operador é a empresa que desenvolve o Software, que efetivamente vai realizar o tratamento dos dados em nome do Controlador. Esse tratamento deve ser feito conforme as instruções repassadas pelo Controlador.

Segundo o Art. 41, a identidade e os dados de contato do responsável devem ser públicos, claros e objetivos, preferencialmente no site do responsável pelo tratamento; o responsável deve aceitar reclamações e cartas do titular da licença, dar explicações e tomar providências; aceitar informações das autoridades e ações nacionais; instruir os empregados e contratados da entidade a adotarem práticas relacionadas à proteção de dados pessoais; e implementar outras atribuições determinadas pelo responsável pelo tratamento ou nas normas complementares (Brasil, 2018).

O titular dos dados pode ser o cliente, fornecedor ou pessoa natural que tem os dados inseridos no sistema do controlador, e que terá seus dados tratados de alguma forma. Atualmente, uma parte relevante das atividades econômicas e sistemas desenvolvidos gira em torno da coleta, processamento e venda de dados pessoais. De acordo com o artigo 7º da LGPD, no item 1 é estipulado que “o tratamento de dados pessoais poderá ser realizado mediante o fornecimento de

consentimento pelo titular por escrito ou por outro meio que demonstre a manifestação de vontade do titular". Com isso, é necessário o consentimento do titular para o tratamento de determinados dados após ser informado quais as condições de tratamento, se há comercialização dos dados ou qual o acesso de terceiros, podendo assim formar sua opinião e decidir se vai fornecer os dados ou não. Em caso de Alteração de informação, é necessário que o controlador informe ao titular o teor dessas mudanças de forma clara e específica, podendo o titular revogar o consentimento aos dados, caso não concorde com as alterações; podendo assim o consentimento ser revogado a qualquer momento mediante a manifestação expressa do titular, por processo gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (Art. 8º).

2.3.1 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Segundo o artigo 5º, inciso XVII, da LGPD, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é a documentação que contém a descrição de todos os processos de tratamento de dados pessoais que podem gerar algum tipo de risco aos direitos dos titulares, além das medidas, mecanismos e salvaguardas além das medidas e mecanismos que possam ser empregados para mitigar esses riscos (BRASIL, 2018). O relatório deverá avaliar todo o ciclo de tratamento de dados, desde a coleta até a exclusão. A LGPD dispõe, em seu artigo 38, que a ANPD (Autoridade Nacional de Proteção de Dados) poderá determinar a elaboração do relatório referente as suas operações de tratamento de dados, observando os segredos comerciais e industriais. A ANPD também pode solicitar ao controlador a elaboração do RIPD quando o tratamento for baseado em seu legítimo interesse ou para agentes de poder público, conforme o artigo 32 da LGPD.

O Relatório deverá conter a descrição dos dados coletados, bem como a metodologia para garantir a segurança das informações e a análise do controlador com relação as medidas de proteção e mitigação de riscos utilizadas. É de responsabilidade do Controlador a elaboração do RPID, devendo o encarregado pelo tratamento de dados pessoais (DPO) avaliar o relatório e dar um parecer. O RIPD deve ser elaborado o mais cedo possível no ciclo de vida de um projeto, assim suas avaliações podem ser adaptadas à operação. O treinamento constante das

equipes responsáveis pela elaboração do RIPD é fundamental para que se incorpore corretamente as descobertas nos projetos em andamento, e garantir o conhecimento sobre todas as justificativas da elaboração do relatório, trazendo benefícios a proteção de privacidade como problemas que não foram identificados nos estágios iniciais, maior conformidade às leis e as normas e a conscientização sobre privacidade e proteção de dados em toda a empresa.

2.4 SANÇÕES E MULTAS.

A LGPD prevê multa sanções para quem não se adequar as boas práticas, apesar da já estar em vigor desde setembro de 2020, as sanções administrativas só poderão ser aplicadas a partir de agosto de 2021. Entretanto, de acordo com a revista eletrônica Conjur (CONJUR, 2020), algumas empresas já foram multadas com base na LGPD e no código civil, mesmo com suspensão temporária da imposição da Multa (CONJUR, 2020). As Sanções englobam desde simples advertências, com prazos curtos para a regularização dos dados, multas no valor de 2% do faturamento, tendo como teto o valor de R$50.000.000,00 ou até mesmo a proibição total ou parcial de atividades relacionadas ao tratamento de dados (BRASIL, 2018). A Lei também prevê a divulgação pública da infração, após ser devidamente apurada e confirmada, o bloqueio dos dados envolvidos na infração, a exclusão permanente dos dados envolvidos na infração e a inversão de ônus da prova a favor do titular dos dados.

Tanto pessoas físicas quanto jurídicas de direito público e privado poderão ser multadas pelo descumprimento da Lei, ressaltando que ela não se aplica a pessoas físicas que usam dados pessoais sem fins econômicos, como redes sociais ou listas de contatos. A lei ressalta que as sanções serão aplicadas após um procedimento administrativo que permita oportunidade de defesa e serão analisados os critérios da gravidade e natureza das infrações e dos direitos pessoais afetados, a boa-fé da empresa envolvida na infração, as vantagens visadas pela empresa no tratamento dos dados, o grau dos danos gerados, a adoção de boas práticas de governança e medidas rápidas de correção, a proporcionalidade entre a gravidade da infração e intensidade da sanção. Caberá a ANPD a fiscalização do cumprimento da Lei, e a determinação da necessidade da aplicação de multas.

2.5 PRIMEIROS PASSOS

Inicialmente, é necessário procurar um consultor com conhecimentos aprofundados na LGPD, tecnologias e na cultura empresarial, desenvolvimento, arquitetura e gestão de softwares, comumente chamado de DPO, ele vai ser responsável pela comunicação com a ANPD e vai precisar entrar em contato e da ajuda de todas as áreas da empresa, para a conscientização dos membros da organização sobre a nova cultura de proteção de dados que será implementada bem como será responsável pela manutenção do projeto de adequação e treinamento dos colaboradores.

Com as ferramentas corretas, é necessário começar do zero, ajustando as relações contratuais entre os desenvolvedores e os clientes, já que caso aconteça algum problema, todos responderão solidariamente. É necessário fazer o Due Diligence sobre os dados pessoais. Due Diligence é um processo que envolve o estudo, a análise e a avaliação detalhada de informações de uma determinada sociedade empresária (BLB Brasil, 2017), nesse caso, mapear todos os dados identificando os tipos de dados (pessoal, sensível criança, público, anonimizado), em quais tabelas do banco de dados estão, em quais relatórios são exibidos, em quais formulários são inseridos e em quais integrações são transmitidos ou compartilhados.

Uma Auditoria sobre o tratamento dos dados é necessária, verificando a aderência as atividades de tratamento de dados contidas no Artigo 5º da LGPD, e uma revisão dos contratos e políticas e termos de uso, ou até mesmo a criação deles, garantindo a documentação de todos os pontos sensíveis em tratamento de dados.

A Segurança da Informação é um dos pontos mais importantes, pois conforme previsto na Lei, será necessária a adoção de medidas de segurança adequadas a proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas, alteração, perda ou qualquer forma de tratamento não autorizado. A empresa deve pensar na privacidade e proteção de dados desde o princípio, no momento da concepção dos sistemas e serviços até a execução final. Assim, a revisão das políticas e soluções em TI, tais como backups, antivírus, gerenciamento de permissões entre outros, se tornam vitais para a proteção tanto das empresas quanto dos dados dos clientes.

Com as políticas decididas, os procedimentos estabelecidos, é necessário o treinamento da equipe, boa parte das ameaças e vazamentos de dados não ocorrem por invasões externas, grande parte das falhas de segurança são causadas por falhas humanas, assim garantir o treinamento em normas de segurança e ações educativas, garantindo assim a mitigação dos riscos no tratamento dos dados pessoais.

Entrar em conformidade com todos os pontos da Lei vai gerar uma grande transformação na empresa, em todos os setores, focando na implementação da nova cultura de privacidade e proteção de dados pessoais, sendo necessário pensar na privacidade e proteção de dados em todas as etapas de criação de seus produtos, assumindo uma postura no tratamento da volumosa quantidade de dados sensíveis que vão ser utilizadas pelos diferentes setores da empresa. Para Jorge Sukarie, sócio fundador e presidente da Brasoftware e vice-presidente do conselho da ABES, “Muito ainda precisa ser feito por parte das empresas para que elas estejam plenamente estruturadas para atender às expectativas trazidas pela LGPD no que tange a privacidade, segurança e transparência, e caberá à ANPD criar os instrumentos normativos que garantam um ambiente de segurança jurídica nesta jornada de adaptação à Lei por parte das empresas” (TI INSIDE, 2021). Apenas com grande ênfase nos processos e muito treinamento será possível garantir total conformidade e governança para se adequar corretamente e evitar qualquer tipo de sanção ou penalidade.

2.5.1 Implementação

A adequação a LGPD demanda vários procedimentos que vão precisar da colaboração de todos os níveis da empresa, e podem ser implementados de maneira simultânea independente de outros processos, dependendo de como for implementada. Assim, para garantir a qualidade de uma implementação correta, é necessário adotar metodologias de gestão, que deve ser selecionada dentro do contexto exclusivo de cada empresa. Garcia (GARCIA et al., 2020) define a necessidade do uso de uma metodologia eficiente:

> Para que uma Organização consiga atender continuamente e de maneira sustentável aos requisitos da LGPD, será preciso implementar um sistema de gestão que permeie todas as áreas de negócio, constituído por

> processos, pessoas e tecnologias. A experiência que o mundo tem vivido desde os anos 1990, com a implantação dos sistemas de gestão da qualidade, mostra um caminho que já foi trilhado com sucesso. A implantação desse sistema de gestão abrange o desenvolvimento de um projeto de transformação, orientado por uma das muitas metodologias de gestão de projetos encontradas no mercado (GARCIA et al., 2020, p25).

Metodologias ágeis já são comuns em ambientes de desenvolvimento de software, se utilizam de iterações, ciclos curtos de procedimentos, e normalmente duram poucas semanas, garantindo assim o recebimento de feedbacks e respostas rápidas às alterações. As metodologias ágeis vão variar conforme a necessidade da empresa, Scrum, BEST (Business Engaged Security Transformation), Crystal Clear e Extreme Programing (XP) são as mais comummente usadas. Após escolhido o tipo de metodologia, a empresa deve fornecer as melhores ferramentas disponíveis para ajudar a equipe de implementação no trabalho colaborativo.

Uma outra metodologia interessante, é a Roadmap ou mapa da estrada (Trello, 2017), que é responsável por apontar o caminho para que a empresa possa sair de um ponto inicial e passar por todas as etapas de construção e entrega até o ponto final do projeto. O objetivo é uma bússola para guiar a equipe em sincronia até a finalização do um projeto.

Com essas decisões tomadas, é necessário escolher quem vai ser o Encarregado da proteção de dados (DPO), conforme previsto pelo inciso VIII do art. 5 da LGPD (Brasil, 2020), ele pode ser tanto alguém já da empresa, quanto um funcionário terceirizado, mas é de extrema importância que ele tenha conhecimento dos processos da empresa e conhecimento do fluxo de informações dos dados pessoais, para que possa fazer corretamente o mapeamento das principais ameaças e riscos no momento de adequação a lei. As principais funções do DPO são treinar e orientar os funcionários sobre os requisitos de conformidade da LGPD, realizar auditorias constantes para garantir que as regulamentações estão sendo cumpridas, servir de elo entre a empresa e a ANPD, responder e informar aos titulares de dados pessoais quaisquer questionamentos sobre como seus dados estão sendo tratados e quais medidas estão sendo tomadas para melhorar a proteção e garantir que todos os pedidos de acessos ou remoção de dados feitos pelos titulares sejam atendidos conforme necessários. Por essa razão, é de extrema importância que o DPO tenha o conhecimento sobre a Legislação e tecnologia, para desempenhar

bem sua função. Existem várias certificações que podem qualificar o profissional para as atribuições de um DPO.

Com a metodologia e o Encarregado decidido, uma outra boa prática é começar a pensar no Gap Analysis, ou análise de Lacunas (Privacy tools, 2021), que é o processo para acompanhar o nível de conformidade que os procedimentos que estão sendo adotados estão alcançando em função dos requisitos da LGPD. Essa análise visa identificar as principais diferenças e lacunas entre o estado atual de adequação da sua empresa e do seu sistema e o estado que a organização planejou estar. É uma excelente ferramenta de conformidade para diagnosticar a aderência da organização a LGPD. O Gap Analysis para a LGPD baseia-se nos princípios previstos na legislação. É importante também se atentar ao nível de maturidade (UX Collective, 2019) para conseguir mensurar em interfaces digitais, realizado por meio de questionários de conformidade, normalmente separados em seis indicadores principais: consentimento, níveis de consentimento, retirada de consentimento, transparência, direito do usuário e políticas de privacidade. Apesar de cada empresa ser única e precisar de uma variação de indicadores, esses normalmente são cruciais para medir a conformidade dos sistemas. Existem vários softwares e sites onde é possível fazer o Gap Analysis, como por exemplo o Diagnóstico LGPD, da ABES, onde respondendo a um questionário de aproximadamente 20 minutos, é possível verificar o seu nível de conformidade e atuar corretamente para que a aplicação siga o planejamento.

Após essas etapas de preparação, é necessário um intenso treinamento com os colaboradores e terceirizados da organização, com o objetivo de explicar o trabalho desenvolvido até agora e a necessidade na mudança da cultura da organização em relação ao tratamento de dados pessoais, e explicar as etapas decididas no *roadmap* garantindo assim o sucesso da implementação.

2.5.2 Metodologias Ágeis

Devido a uma necessidade de urgência na implementação da LGPD, uma metodologia ágil de gestão pode servir para que a adequação permeie por todas as áreas da empresa e seus sistemas.

> Os métodos ágeis são uma alternativa à gestão tradicional de projetos, eles nasceram nos braços do desenvolvimento de software, mas hoje podem ser aplicados a qualquer tipo de projeto (inclusive os que não se remetem ao software). Os métodos ágeis vêm ajudando muitas equipes a encarar a imprevisibilidades dentro de um projeto através de entregas incrementais e ciclos iterativos. As metodologias ágeis passaram a ser uma alternativa aos métodos tradicionais, também conhecidos como métodos pesados ou clássicos. (BERNARDO, 2015)

A utilização de métodos ágeis é interessante para a implementação da LGPD pois ao contrário dos métodos tradicionais, onde normalmente é um processo em que a implementação é realizada uma única vez e em sequência, uma metodologia ágil pode trabalhar de forma concomitante. Ele é adotado para permitir que o DPO tenha um contato rápido com todos os colaboradores e terceiros, basicamente particionando o projeto de implementação em pequenas etapas, normalmente denominadas *Sprints*, com tempo de duração médio de 15 dias corridos (Garcia, 2020, p28). Utilizando ciclos curtos de procedimentos, chamados de iterações, é possível separar todas as etapas necessárias para a adequação à LGPD: planejamento, análise, sistematização, testes e documentação. Seguindo então as principais diretrizes do método ágil, segundo GARCIA (2020, p28):

- Pessoas e interações, ao contrário de processos e ferramentas;
- Processo executável, ao contrário de documentação extensa e confusa;
- Engajamento do colaborador, ao contrário de pressões pelo cumprimento de prazos e cláusulas contratuais;
- Respostas rápidas para mudanças que geram valor, ao contrário de seguir planos previamente definidos, com longas cadeias de tomada de decisão para incorporação da mudança positiva (GARCIA, 2020).

Com isso é possível formar as equipes responsáveis pela implementação, composta por um Agente de Transformação, normalmente denominado *Project Owner*, externo, um colaborador que assume o papel de líder da equipe e os demais membros. Ao início das etapas, cada equipe deve identificar os programas que serão necessários para a implementação, os requisitos de segurança e proteção de dados que serão exigidos, qual vai ser a estratégia para essa implementação, os recursos necessários, sejam eles de pessoas, financeiros ou tecnológicos, a estimativa do esforço de implementação e validação (GARCIA, 2020) e as estimativas de valores que serão gerados ao concluir essas atividades.

Durante as próximas etapas, o líder da equipe é responsável por interagir todos os dias com os membros da equipe, em reuniões de em média 10 minutos, onde serão tratados os assuntos formais referentes ao que foi feito e o planejamento do dia, e em momentos informais para acompanhar o desenvolvimento e ajudar na solução de eventuais problemas. O líder do projeto também é responsável por interagir com o Agente de Transformação para tomar as decisões necessárias, consolidar e verificar os resultados atingidos, avaliar como a equipe está lidando com os processos, solucionar eventuais conflitos internos e se necessário, ajustar a estratégia, podendo também desenvolver as próprias atividades se for preciso (GARCIA, 2020).

Cada metodologia ágil traz uma abordagem diferente, com valores, princípios e reuniões, algumas trazem uma abordagem mais voltada para a gestão, com maior foco em reuniões e planejamento, enquanto outras são mais voltadas para as práticas técnicas. Cada empresa vai precisar analisar o que se encaixa melhor em seus projetos e em suas necessidades, mas os métodos ágeis são muito adaptativos, e com isso incentivam a melhoria contínua através dos ciclos de inspeção e adaptação, acarretando uma constante de mudanças e transformação, sempre tentando melhorar (Prikladnicki, 2014, p5).

2.5.3 Mapeamento de dados e Implantação de Políticas.

A revisão ou implantação de políticas de segurança da informação envolvem políticas de proteção de dados pessoais, a política de privacidade e por consequência a avaliação de risco dessas políticas. Ela pode ser desenvolvida posteriormente ao mapeamento de dados, pois é mais seguro revisar ou implantar a política de segurança da informação depois que todos os dados pessoas forem devidamente mapeados. Sendo assim mais interessante e prático começar pelo mapeamento dos dados pessoais, que segundo as palavras de Mariana Sbaite Gonçalves é advogada e especialista em LGPD, o mapeamento de dados é o coração do projeto.

> Dito isso, o intuito é discorrer sobre a importância do mapeamento de dados pessoais (data mapping) que, apesar de algumas vezes ser colocado em segundo plano, quando comparado com outros trabalhos, é o coração do projeto. E por que o coração? Por definição, o coração tem como função primordial garantir que o sangue seja enviado para todas as partes do nosso corpo, ou seja, é o que nos mantém vivos. Aqui, o paralelo cai como uma luva: sem um mapeamento correto, a tendência é que o projeto esteja fadado ao insucesso, não sobrevivendo à mais simples auditoria, por insuficiência da profundidade do entendimento sobre o cotidiano do tratamento dos dados pessoais e deixando a organização à mercê de problemas de privacidade e proteção de dados pessoais, por consequência. (Gonçalves, 2021)

Nessa etapa os dados pessoais são devidamente inventariados e para cada processo será criado um fluxo de todo o ciclo de vida do dado, a sua origem e sua finalidade. Sendo necessário quatro ações importantes, levantar dados pessoais, utilizar o diagrama de fluxo de dado para o mapeamento, realizar o mapeamento dos dados e elaborar o registro das operações de tratamento de dados pessoais. Essa etapa deve estar em constante revisão, para refinar com precisão o mapeamento dos dados pessoais para que eles sejam devidamente inventariados de forma segura. O levantamento dos dados pessoais é feito através de questionários e análises documentais, com questionários enviados a todos os setores da instituição e serão confrontadas e tabuladas no próximo procedimento.

Para fazer o mapeamento de dados, é importante a utilização de ferramentas para representar graficamente o fluxo de dados do sistema, o diagrama de fluxo de dados (DFD), ele descreve os processos envolvidos em um sistema para transferir dados de entrada para o armazenamento de arquivos e criação de relatórios. Após a elaboração do DFD geral do sistema, será iniciado o mapeamento dos dados propriamente dito, todos os processos relacionados a dados são identificados e mapeados, com o objetivo de saber como esse dado é utilizado e tratado pelo sistema. Após a conclusão do mapeamento, é necessário a elaboração do registro das operações de tratamento de dados pessoais (LGPD Brasil, 2020), que é uma estrutura de controle para gerenciar e auditar todos os acessos e manipulações das bases de dados, com a finalidade de garantir sua integridade. A LGPD prevê no seu artigo 37 que os agentes de tratamento de dados devem manter um registro de todas as operações de tratamento de dados pessoais que realizarem, especialmente quando esses tratamentos são baseados em legítimo interesse. Cada departamento ou setor é responsável pelo mapeamento de dados e o registro das operações de tratamento de dados que serão tratadas pelos seus sistemas, e muitas vezes esses

dados vão se comunicar pelos sistemas entre si. Mas o importante nesse caso é registrar cada dado que passa por cada setor e cada sistema e a finalidade do seu tratamento.

Com o mapeamento devidamente concluído, é possível começar a pensar nas políticas de segurança da informação, que são conjuntos de ações, medidas e práticas, que são responsáveis por gerar a proteção dos dados contra diferentes tipos de ameaças, tanto internas quanto externas, e com a intenção de prevenir e mitigar os riscos (Certifiquei, 2020). A LGPD torna a adoção de políticas de segurança da informação uma disciplina obrigatória, que garante a efetividade das ações. Para elaborar e implementar uma política de segurança alguns passos devem ser observados: Planejamento, definição de responsáveis por escrever a política de segurança da informação, definir níveis de acesso de dados e definir consequências caso haja violação das regras.

Outra política importante é a Política de privacidade, conceito que pensa na privacidade desde a concepção do sistema. O objetivo principal é exibir o tratamento de dados pessoais atendendo aos princípios da LGPD, normalmente disponibilizadas em forma de documento público endereçado aos usuários que são titulares de dados. A política também deve trazer avisos sobre o uso de Cookies (Legal Cloud, 2020), identificando quais são e quais suas finalidades, que precisam ser bastante claras e passar as informações precisas para o tipo do usuário, normalmente apontando a existência de cookies necessários, de desempenho, de funcionalidade e de publicidade. Também é necessário ensinar o usuário como ele pode gerenciar esses cookies, permitindo que ele tenha maior controle sobre as informações que está fornecendo ao sistema.

O Aviso de Privacidade é um documento dedicado a proteger a privacidade do titular e a proteção dos dados pessoais. Ele deve estar disponível aos usuários do sistema em uma linguagem objetiva e clara, descrevendo os tipos de dados pessoais que serão coletados, com quem são compartilhados e em que hipóteses isso pode acontecer e eventuais medidas de proteção que podem ser adotadas.

2.5.4 Direito dos titulares

A LGPD estabelece uma estrutura que confere poder aos titulares de dados pessoais, concedendo direitos a serem exercidos perante os controladores desses

dados (Get Privacy, 2020). A empresa precisa se preparar para lidar com possíveis requisições de confirmação de existência de tratamento, de acesso aos dados, de correção de dados incompletos ou inexatos e de revogação de consentimento. Considerando que esses direitos podem ser exercidos pelo titular dos dados a qualquer momento durante a vigência do tratamento dos dados e mediante a exigência ao controlador, é de extrema importância que a empresa esteja preparada para responder a todas as possíveis solicitações que podem ser recebidas a partir do momento da vigência da Lei. Elaborar um processo de recebimento e resposta de solicitações ajudara a organizar o cumprimento das solicitações. A criação de uma política interna de requisição dos titulares de dados serve para guiar o fluxo e o tratamento de todas as possíveis requisições que a empresa pode receber, amparadas nos direitos citados.

O DPO tem um papel fundamental nesse fluxo de tratamento, deixando claro quem é o responsável pelo processo de recebimento, tratamento e resposta das requisições e o respectivo prazo legal para que elas sejam respondidas, garantindo que a empresa não seja exposta de forma negativa e garantindo que os dados serão tratados de forma adequada sem oferecer riscos a organização.

Com as regras internas devidamente definidas, é preciso decidir como será implementado o processo de atendimento as requisições dos titulares. Como a LGPD ainda não está completamente em vigor, a ANPD ainda não fixou procedimentos para auxiliar na criação desses processos, mas é possível seguir as boas práticas de outras leis similares, como a GDPR. Após ter as regras definidas, é necessário desenvolver e ministrar treinamentos específicos sobre as respostas das requisições de titulares, para que todos os colaboradores responsáveis por essas respostas estejam alinhados e em conformidade com as políticas e os procedimentos. Esse treinamento deve ser ministrado preferencialmente pelo DPO e devem ser constantemente repetidos e atualizados, seja por meios de videoaulas, oficinas, ações em grupo, garantindo assim o alcance de todos os colaboradores que tenham acesso ao tratamento de dados pessoais.

2.5.5 Transferência internacional de dados

Em um mundo cada vez mais conectado, a circulação de serviços e dados entre países é algo constante, sendo necessário que se regularize a forma do

tratamento de dados pessoais de forma internacional também. LEITE (Leite et al, 2019) cita em seu livro:

> O tema transferência internacional de dados pessoais é hoje um tema essencial a ser discutido. Diversos tratamentos, em si, já pressupõe a transferência internacional dos dados pessoais tratados, muitas vezes o próprio titular desconhece essa informação. Por exemplo uma empresa que coleta os dados pessoais de um indivíduo dentro do território brasileiro, porém, armazena esse dado em seu servidor, localizado nos Estados Unidos. Ou uma agência de viagens que manda os dados de seus clientes para um hotel localizado na Alemanha. (Leite et al, 2019, p45)

A lei brasileira foi fortemente inspirada na lei da União Europeia, a GDPR, e traz uma escrita bem específica para a transferência internacional de dados, demonstrando as bases legais para que esses dados sejam transferidos de forma legal e segura e delimitando as transferências de dados para países que não ofereçam uma proteção de dados pessoais adequadas a LGPD. Essas limitações se aplicam a todos os tipos de transferências internacionais, inclusive as decorrentes de serviços de armazenamento em nuvem e centros de dados localizados em outros países. Então antes de se fazer qualquer transferência internacional de dados pessoais, é necessário analisar cuidadosamente se ela é permitida e quais dos mecanismos legais permitidos pela lei serão utilizados para justificá-la. Essas regras se aplicam a todas as empresas, sejam elas nacionais ou estrangeiras que pretenda tratar dados pessoais de pessoas localizadas em território brasileiro, inclusive o oferecimento de produtos ou serviços, então é importante que todos os setores da empresa que tenham eventuais parceiros internacionais se atentem que estarão sujeitos a LGPD se efetuarem qualquer tratamento de dados pessoais.

Além de proteger os direitos a privacidade, a LGPD também segue o padrão guiado pela GDPR na proteção de dados também no referente a transferência internacional de dados, seguindo os padrões que estão sendo adotados não só pela Europa, como por vários outros países no mundo.

2.5.6 Ajustes Contratuais

Essas alterações não se limitam apenas as questões tecnológicas, mas também exigem ajustes nos contratos com os clientes e usuários, com a necessidade de elaboração de novos contratos visando atender os requisitos legais (Eximia Co, 2019). Além das adequações físicas e sistémicas e de procedimentos

internos de treinamento para proteção e segurança dos dados pessoais, será necessário alterar e preparar cláusulas padrões e novas minutas contratuais que precisam ser formalizadas.

Devido aos diversos requisitos da LGPD, não será possível uma simples comunicação direta com o usuário final titular dos dados, a lei passa a exigir que novas disposições contratuais sejam implementadas para garantir que o titular de dados esteja completamente ciente de todos os procedimentos relativos à coleta de dados, tais como a forma, duração e finalidade, informando também seus direitos e deveres e as responsabilidades dos controladores. Para que essa alteração e criação de novos contratos seja feito da maneira mais segura possível e consiga atender todos os requisitos da lei, é interessante observar alguns pontos de destaque. O primeiro é que a LGPD estabelece que o titular precisa consentir com o uso e o tratamento de seus dados pessoais, sempre apresentado por cláusula clara e transparente sobre como será feito o uso desses dados, por quanto tempo e com qual finalidade. A empresa também deve estar preparada para uma auditoria completa de todos os contratos já em vigor, firmados com clientes, usuários e até com os próprios colaboradores, identificando aqueles que implicam em coleta e tratamento de dados, para que eles possam ser adequados e implementados atendendo as previsões legais. Por fim, a empresa precisa garantir que todos os contratos firmados ou que possam vir a ser formalizados estejam totalmente adequados e em conformidade com a LGPD, de preferência elaborando um processo interno para otimização do processo de classificação dos riscos relacionados a privacidade.

2.5.6 Gerenciamento de violação de dados.

Os agentes de tratamento de dados são responsáveis por adotar medidas de segurança técnicas e administrativas preparadas para proteger os dados pessoais de acessos não autorizados, perda, alteração ou qualquer forma de tratamento não autorizado ou ilícito (Oliveira, 2019). Qualquer situação dessas deve ser tratada como um incidente de segurança por violação de dados pessoais. Diante disso é de extrema importância que a empresa esteja preparada para atuar de maneira preventiva e reativa a qualquer incidente que possa acontecer, e saber como agir em caso de violação de segurança. O plano de resposta a incidentes é planejado

para que a empresa possa responder rapidamente e adequadamente a qualquer incidente de segurança, mitigando os danos ao negócio e reduzindo o tempo e os custos de recuperação. Gonçalves (GONÇALEVS, 2021) explica como se deve atuar em casos de incidentes com dados pessoais:

> Ao ter ciência sobre qualquer incidente com dados, é preciso comunicar imediatamente o Comitê de Privacidade (ou qualquer outra equipe correspondente) e o Encarregado pelo Tratamento de Dados Pessoais (DPO), que deverão acionar o Departamento de Tecnologia da Informação e o Departamento Jurídico. O colaborador deve seguir as orientações dos responsáveis, pois a adoção de medidas por conta própria pode agravar o problema ou danificar evidências do Incidente com Dados Pessoais. Ainda, é importante manter sigilo sobre a comunicação recebida, pois tornar a informação pública pode prejudicar a investigação do suposto Incidente com Dados Pessoais e a identificação do autor da comunicação (Gonçalves, 2021).

Um plano de resposta a incidentes bem planejado permite a coordenação de ações que envolvam vários departamentos da empresa, tornando-o absolutamente necessário para a empresa garantir que a reposta a qualquer incidente seja feito da maneira mais rápida e apropriada possível e em conformidade com a legislação. O plano deve ser elaborado previamente, pois é necessário que ele exista antes da ocorrência de qualquer incidente, com todas suas fases devidamente mapeadas e tarefas distribuídas a cada departamento específico. E mesmo com a adoção de medidas preventivas extremamente planejadas, incidentes de segurança podem ocorrer e é necessário que a empresa esteja preparada para responder o mais rápido possível.

O primeiro passo para a elaboração de um bom plano é a existência de uma equipe previamente definida com funções determinadas para atuar na contenção do incidente assim que ele ocorrer. É importante essa equipe ser formada por pelo menos um integrante das áreas jurídica, de Conformidade, TI e de comunicação, todos sob o comando do DPO, sendo importante isso ser definido já nas fases iniciais de implementação. Outra etapa importante consiste no planejamento das repostas necessárias, seguindo uma ordem interna de validação. A Empresa deve comunicar aos titulares dos dados sobre qualquer incidente relacionado aos dados, caso possam acarretar danos ou riscos a eles. É crucial que essas respostas sejam rápidas e alinhadas, para que todos os riscos existentes sejam cobertos. A repostas a um incidente deve ser rápida e não pode conter falhas, para minimizar os danos e conter o mais rápido possível para impedir que o incidente continue causando

danos, as medidas podem variar entre indisponibilizar os dados até a interrupção do sistema que os fornece.

Após a equipe responsável concluir todos os procedimentos do plano de resposta, caberá ao DPO elaborar um relatório do incidente, identificando o evento, os integrantes da equipe responsável pela contenção, os dados atingidos, os impactos e as consequências, para quem o incidente foi reportado e as medidas de contenção adotadas. A elaboração desse relatório é importante não só para a comprovação da atuação da equipe, como também para que tudo fique documentado e sirva de referência para possíveis revisões dos procedimentos internos e a melhoria da atuação da equipe e evolução do próprio Plano de respostas a Incidentes.

2.5.7 Cultura de Cibersegurança.

A empresa precisará passar por uma grande mudança na sua postura, adotando novas normas de segurança e pensando em privacidade de dados e segurança em todos os momentos da concepção de seus produtos. Adotando a cultura de Cibersegurança. Garcia (GARCIA et al., 2020) define cultura de cibersegurança:

> A Cultura de Cibersegurança é um aspecto particular da Cultura Organizacional da Empresa. A cultura como um todo, seja ela organizacional ou de cibersegurança, é composta de regras formais ou informações que influenciam colaboradores e terceirizados a tomar determinada decisões e executar ações do dia a dia que com elas estão alinhadas. Regras culturais são suficientes para impedir a consecução de muitos tipos de ataques e cobrir os casos omissos não abrangidos por políticas e controles de segurança (GARCIA et al., 2020, p27).

O fortalecimento das aplicações dessas regras no dia a dia baseia-se em vários aspectos importantes, como na Liderança, ao definir princípios claros e valorizar comportamentos seguros definidos pelos líderes e gestores de segurança, a Ética ao estabelecer que cumprir as obrigações de segurança de tratamento de dados pessoais é o caminho correto a ser feito, visando sempre a proteção dos sistemas desenvolvidos, e a Responsabilidade ao determinar que a garantia da segurança e privacidade é um dever de todos os setores da empresa, devendo empenhar-se ao máximo para cumprir as obrigações de cibersegurança e políticas de privacidade em todas as etapas de desenvolvimento. Outro aspecto de extrema importância é a Capacitação, para garantir o empenho máximo de todos os

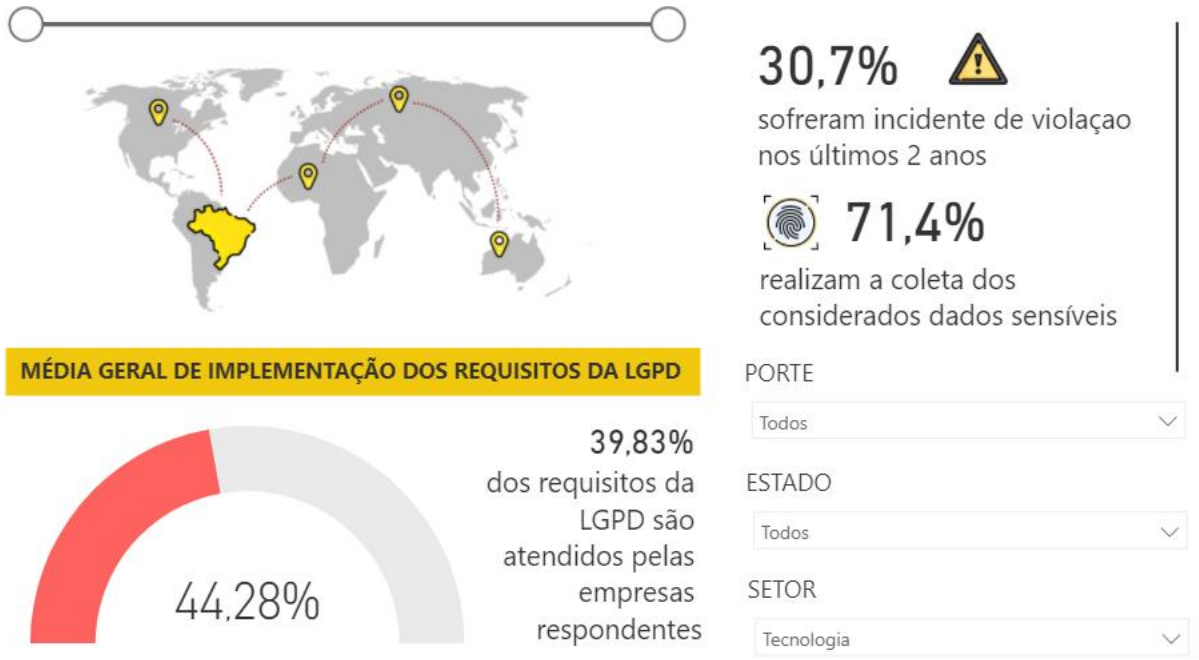
funcionários que possam estar envolvidos em processos de tratamento de dados nos treinamentos disponibilizados, garantindo que todas as decisões tomadas sejam baseadas nos princípios de segurança. A Governança é a orientação para que todos estejam harmonizados para alcançar os objetivos de maneira consciente e alinhados com a missão da empresa, particularmente nas atividades que envolvam tratamento de dados e segurança da informação. E por último a Comunicação aberta sobre questões e dúvidas a respeito da segurança de dados, desenvolvimento de novos projetos e formação de equipes multidisciplinares, bem como o fortalecimento do trabalho em equipe para sempre pedir orientação aos companheiros ou superiores em caso de dúvida sobre algum processo.

2.6 CENÁRIO ATUAL

A Agência Associação Brasileira das Empresas de Software (ABES) em conjunto com a empresa EY, desenvolveu uma ferramenta de autoavaliação de conformidade com a LGPD, compilando respostas de centenas de empresas de diversos setores para acompanhar como está a jornada de preparação do mercado brasileiro.

De acordo com a Figura 1, aproximadamente 56% das empresas de tecnologia ainda precisam se adequar à LGPD (ABES, 2020). Apesar do Setor de Tecnologia estar liderando a iniciativa, ainda está longe de um cenário aceitável. Segundo Rodolfo Fücher, presidente da ABES, “Nos dias atuais, não podemos debater estratégias para o desenvolvimento econômico e social de uma nação sem mencionar Inteligência Artificial, big data, blockchain, computação quântica e realidade aumentada, por exemplo. A tecnologia está presente em todos os âmbitos sociais, então, companhias do setor que não estão em conformidade com a LGPD podem facilmente perder a credibilidade” (ABES, 2020).

Figura 1: Média geral de implementação dos requisitos da LGPD.



Fonte: ABES SOFTWARE, 2021

Para uma empresa, não estar de acordo com a LGPD pode gerar prejuízos não só pelas possíveis multas, mas também pela perda da confiança dos seus clientes e parceiros.

2.6.1 Vazamentos de dados e cibercrime

Em janeiro de 2021, um mega vazamento de dados expôs mais de 223 milhões de números de CPF e outros dados sensíveis, muitos deles colocados à venda em fóruns usados por criminosos digitais (G1, 2021). Isso é quase a totalidade da população brasileira, significando então que estejam incluídos dados de pessoas falecidas. Não apenas dados cadastrais como CPF e RG foram divulgados, mas também dados como endereço, telefone, salário foram expostos. Uma pesquisa recente do Instituto de Tecnologia de Massachusetts publicada no Journal of Data and Information Quality da Association for Computing Machinery aponta um aumento de 493% no vazamento de dados no Brasil (ACM, 2021), colocando o Brasil entre os países mais vulneráveis a ataques cibernéticos, a maioria desses dados está sendo disponibilizada de forma criminosa. (PSafe, 2021). Esses dados normalmente são utilizados para contrair dívidas ou cometer crimes sem que o titular saiba.

Um fator crucial nesses vazamentos é que as empresas têm demorado muito tempo para notar que seu banco de dados foi comprometido, podendo a média desse intervalo ser próxima de 250 dias para identificar o vazamento e 69 dias para a contenção, tornando difícil saber exatamente quem foi o responsável por esse vazamento. As empresas gastam cerca de US$740 mil apenas para notificar seus clientes a respeito do incidente (LB2, 2021). É necessário identificar os responsáveis para que seja possível criar um plano de contenção e mitigar futuros novos vazamentos, por mais que as empresas sejam igualmente vítimas de ataques de hackers, tentativas de phishing e tentativas de invasão por força bruta, ainda é necessário que as empresas estejam preparadas para se defender desse tipo de invasão, seja por softwares mais recentes ou por treinamentos para identificação e conscientização de suas ferramentas.

Apesar da LGPD concretizar o princípio da segurança, condicionando a responsabilidade e o ressarcimento de danos pelo tratamento irregular de dados, ou seja, deixar de garantir os parâmetros de segurança por ela estabelecidos no artigo 46(Brasil, 2020), muitas das vezes não existem maneiras de identificar de a origem do vazamento de dados, e assim não é possível atribuir a responsabilidade desse vazamento a um controlador ou operador específico.

No caso do vazamento de mais de 220 milhões de dados pessoais de cidadãos brasileiros, a empresa Serasa Experian chegou até a ser notificada pelo Procon-SP (Procon, 2021), mas ela encaminhou uma resposta informando que nada indicava que houve vazamento em suas bases de dados, mas ainda estava investigando para apurar o incidente. A empresa apresentou um parecer técnico de uma empresa especializada demonstrando que os sistemas eram seguros, mas de acordo com o Procon-SP, a empresa não conseguiu implementar as medidas de segurança necessárias para o cumprimento da LGPD. Também foram questionados quais eram as medidas de contenção do incidente e mitigação dos riscos dos danos causados pelo vazamento e o que seria feito para evitar falhas. Apesar da empresa citar que mantém um “abrangente programa de segurança de informação, não chegou a detalhar quais seriam essas políticas. Cabe a Agência Nacional de Proteção de Dados a fiscalização e aplicação de multas previstas na lei.

Segundo o Relatório sobre o prejuízo de um vazamento de dados (IBM, 2020), a maioria dos vazamentos são causados por ataques mal-intencionados, que também tendem a ser os mais caros. Esses ataques aumentaram de forma

constante no último ano, sendo a violação de credenciais a mais prejudicial as empresas. Cerca de 52% dos vazamentos foram causados por ataques mal-intencionados, e outros 27% causados por erro humano e 23 por falhas em sistemas. Os dois últimos podendo ser evitados por um interesse maior das empresas em treinamentos e investimentos em uma melhor infraestrutura de Tecnologia. Esse mesmo relatório mostra que a pandemia aumentou o risco e o prejuízo de vazamento de dados. Com o aumento do trabalho remoto para a segurança dos colaboradores devido à disseminação da COVID-19, 70% dos entrevistados disseram que o trabalho remoto aumentaria o prejuízo de um vazamento de dados, devido a flexibilização da segurança para que o trabalho remoto fosse possível e pela diminuição da fiscalização facilitando vazamentos por funcionários mal-intencionados ou não treinados contra tentativas de engenharia social.

3 CONCLUSÃO

A Coleta e o tratamento de dados têm se tornado um padrão cada vez maior no desenvolvimento de sistemas, expandindo o alcance de produtos e direcionando serviços para o tipo certo de consumidor de uma maneira precisa e rápida, e com uma injeção de dados crescendo exponencialmente, algo tão valioso assim precisaria ser regulado para garantir a segurança e privacidade dos dados gerados. A Lei ainda não entrou em vigor totalmente, mas percebemos que mesmo com avanços consideráveis, ainda existe um longo caminho pela frente e muitas empresas ainda não estão em conformidade com as novas regras.

A LGPD não é um Software ou um sistema que pode ser instalado e nem um curso ou treinamento que pode ser dado em um dia e já ficar tudo correto dentro dos termos da Lei. Torna-se necessária toda uma transformação na cultura da empresa e no modo como ela lida com os dados pessoais. Estar em conformidade com a lei é algo que vai demandar tempo e dinheiro, o que a curto prazo pode parecer desperdício, ou que a lei nunca vai entrar completamente em vigor e não será totalmente cobrada como outras leis. Mas os riscos, e os prejuízos, por não estar de acordo com a regulamentação podem ser catastróficos e em algumas situações até mesmo irreversíveis, pois não é uma questão apenas de prejuízo financeiro, mas é algo que também pode afetar a imagem da empresa e a confiança dos clientes e

parceiros comerciais. Ninguém quer ter sua imagem vinculada a uma empresa envolvida com vazamentos de dados ou que passe a ser conhecida por não se importar com essas questões. E essa é uma tendência Global, que está sendo adotada em cada vez mais países. A GDPR foi a primeira, mas em breve cada país ou região vai ter a sua própria lei de tratamento de dados, podendo até se negar a oferecer serviços e fechar negócios com países que não levem a sério a segurança de dados pessoais.

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.

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 REFERÊNCIAS

ABESSOFTWARE. Índice LGPD ABES aponta que 60% das empresas não estão em conformidade com a lei. 2020. Disponível em: https://abessoftware.com.br/indice-lgpd-abes-aponta-que-60-das-empresas-nao-estao-em-conformidade-com-a-lei/. Acesso em: 2 jun. 2021

ANGELO, Tiago. **Juíza aplica LGPD e condena construtora que não protegeu dados de cliente**. ConJur, 2020. Disponível em: https://www.conjur.com.br/2020-

set-30/compartilhar-dados-consumidor-terceiros-gera-indenizacao. Acesso em: 16 jun. 2021.

BASTOW, Janna. **Roadmap ágil: pense grande, entregue rápido e se mantenha sempre em movimento**. Trello, 2017. Disponível em: https://blog.trello.com/br/roadmap-agil. Acesso em: 11 jun. 2021

BHAGESHPUR**,** Kiran **Data Is the New Oil -- And That's A Good Thing** Forbes, 2019. Disponível em: https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=45aa535f7304. Acesso em 1 jun. 2021.

BLB BRASIL. O que é Due Diligence? Entenda o conceito e sua aplicação em empresas. 2017. Disponível em: https://www.blbbrasil.com.br/blog/due-diligence/. Acesso em: 5 jun. 2021

BRITO, Priscilla. **Escala de maturidade para compliance de Interfaces Digitais com a LGPD**. UX Colletctive, 2019. Disponível em: https://brasil.uxdesign.cc/escala-de-maturidade-para-compliance-de-interfaces-digitais-com-a-lgpd-ffbc5e282dfb. Acesso em: 10 jun. 2021.

COMUNICAÇÃO, Assessoria de. **Serasa complementa resposta sobre vazamento de dados**. Procon-SP, 2021. Disponível em: https://www.procon.sp.gov.br/serasa-complementa-resposta-sobre-vazamento-de-dados/. Acesso em: 16 jun. 2021

DIAGNÓSTICO LGPD. ABES. Disponível em: https://diagnosticolgpd.abes.org.br/. Acesso em: 10 jun. 2021.

EXIMIA CO. LGPD: não basta revisar o software, é necessário revisar seus contratos. 2019. Disponível em: https://eximia.co/lgpd-nao-basta-revisar-o-software-e-necessario-revisar-seus-contratos/. Acesso em: 17 jun. 2021.

GARCIA, Lara Rocha. et. Tal. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. São Paulo: Blucher, 2020

GONÇALVES, Mariana Sbaite. **LGPD e o Registro das Operações de Tratamento de Dados Pessoais – ROPA**. LGPD Brasil, 2020. Disponível em: https://www.lgpdbrasil.com.br/lgpd-e-o-registro-das-operacoes-de-tratamento-de-dados-pessoais-ropa/. Acesso em: 11 jun. 2021.

GONÇALVES, Mariana Sbaite. **Mapeamento de dados pessoais: o coração do projeto!** ConJur, 2021. Disponível em: https://www.conjur.com.br/2021-fev-22/sbaite-mapeamento-dados-pessoais-coracao-projeto. Acesso em: 2 jun. 2021

GONÇALVES, Mariana Sbaite. **Ocorreu um incidente de segurança com dados pessoais. E agora?** LGPD Brasil, 2021. Disponível em: https://www.lgpdbrasil.com.br/ocorreu-um-incidente-de-seguranca-com-dados-pessoais-e-agora/. Acesso em: 17 jun. 2021.

HOLZNER, Burkart., **HOLZNER**, Leslie. **Transparency in Global Change: The Vanguard of the Open Society**. 1ª edição. Pittsburgh: Universidade de Pittsburgh, 2006

LEGAL CLOUD. Política de Cookies na LGPD: Como criar em 3 passos. 2020. Disponível em: https://legalcloud.com.br/politica-cookies-passo-passo/. Acesso em: 15 jun. 2021.

LEITE, Luciano Vasconcelos; LAMBOY, C. K. d; ANDRADE, M. H. L. A.; **Manual de Implementação da Lei Geral de Proteção de Dados**; 1ª edição. São Paulo: Via Ética, 2019. p. 45-46.

LGPD BRASIL. Disponível em https://www.lgpdbrasil.com.br. Acesso em 4 jun. 2021.

LUZ, Jean Carlo Jacichen. **A operacionalização da resposta à requisição do titular de dados na LGPD**. Get Privacy. Disponível em:

https://getprivacy.com.br/artigo-operacionalizacao-da-resposta-a-requisicao-do-titular-de-dados-na-lgpd/. Acesso em: 15 jun. 2021.

NEEDHAM, Mass. **Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts.** IDC, 2021. Disponível em https://www.idc.com/getdoc.jsp?containerId=prUS47560321. Acesso em 1 jun. 2021.

PECSEN, Thaisy. **Vazamento em massa expõe número de CPF de milhões de brasileiros, alerta PSafe**. PSafe, 2021. Disponível em: https://www.psafe.com/blog/vazamento-expoe-numero-de-cpf-de-milhoes-de-brasileiros-alerta-psafe/. Acesso em: 16 jun. 2021

PLANALTO. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 jun. 2021.

PLANALTO. **Lei n° 13. 709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais**. Brasília: 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 11 jun. 2021.

PRIKLADNICKI, Rafael; WILLI, Renato; MILANI, Fabiano; **Métodos Ágeis para Desenvolvimento de Software**. 1. ed. Porto Alegre: Bookman, 2014. p. 5.

PRIVACYTOLLS. Gap Analysis: o que é e como cumprir essa etapa de adequação. Disponível em: https://www.privacytools.com.br/gap-analysis/. Acesso em: 10 jun. 2021.

SÁ, Marcelo Dias de. **Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas.: Aplicações mobile do governo.** Repositório UFMG, 2019. Disponível em https://repositorio.ufmg.br/bitstream/1843/32040/1/MarceloDiasDeSa.pdf. Acesso em 3 jun. 2021.

SUKARIE, Jorge. **Os desafios da implementação da LGPD.** tiinside, 2021. Disponível em: https://tiinside.com.br/22/02/2021/os-desafios-da-implementacao-da-lgpd/. Acesso em: 5 jun. 2021.

ZEFERINO, Denis. **Política de segurança da informação: como criar corretamente?** Certifiquei, 2020. Disponível em: https://www.certifiquei.com.br/politica-seguranca-informacao/. Acesso em: 2 jun. 2021.