CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA

CURSO DE GRADUAÇÃO TECNOLÓGICA EM

REDES DE COMPUTADORES

CLEYDSON RIBEIRO DE LIMA

JEFFERSON MATHEUS FERREIRA DA SILVA ANDRADE

JEREMIAS BARBOSA SOUZA

LUDOVICA PEREIRA DA SILVA

A LEI GERAL DE PROTEÇÃO DE DADOS IMPLEMENTADA PELOS SETORES DE TI DAS CORPORAÇÕES BRASILEIRAS

RECIFE

2019

CLEYDSON RIBEIRO DE LIMA

JEFFERSON MATHEUS FERREIRA DA SILVA ANDRADE

JEREMIAS BARBOSA SOUZA

LUDOVICA PEREIRA DA SILVA

A LEI GERAL DE PROTEÇÃO DE DADOS IMPLEMENTADA PELOS SETORES DE TI DAS CORPORAÇÕES BRASILEIRAS

Trabalho de Conclusão de Curso apresentado ao Centro Universitário Brasileiro – UNIBRA como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores.

Orientadora: Prof.ª Ameliara Freire Santos de Miranda.

RECIFE

2019

L732c Lima, Cleydson Ribeiro de

A lei geral de proteção de dados implementada pelos setores de ti das corporações brasileiras. / Cleydson Ribeiro de Lima; Jefferson Matheus Ferreira da Silva Andrade; Jeremias Barbosa Souza; Ludovica Pereira da Silva. - Recife: O Autor, 2019.

29 p.

Orientador(a): Ameliara Freire Santos de Miranda

Trabalho De Conclusão De Curso (Graduação) Centro Universitário Brasileiro – UNIBRA. Graduação Tecnológica em Redes de Computadores, 2019.

1. Lei Geral de Proteção de Dados. 2. Segurança da Informação. 3.Tecnologia da Informação. Centro Universitário Brasileiro - UNIBRA. II. Título

CDU: 004.7

Dedicamos este trabalho a todos os nossos amigos e familiares.

AGRADECIMENTOS

Primeiramente gostaríamos de agradecer a Deus por ter nos ajudado ao longo desses semestres.

Agradecemos a nossa orientadora: Ameliara Freire Santos de Miranda por aceitar a conduzir o nosso trabalho de pesquisa.

A todos os nossos professores do curso de Redes de Computadores, que foram importantes para nossa formação, pelo Centro Universitário Brasileiro - UNIBRA.

Aos nossos pais que sempre estiveram ao nosso lado nos apoiando ao longo de toda a nossa trajetória acadêmica, e a todos os amigos que contribuíram de forma direta e indiretamente nos dando apoio para continuar nessa caminhada.

SUMÁRIO

1 INTRODUÇÃO 8
2 DELINEAMENTO METODOLÓGICO 10
3 SEGURANÇA DA INFORMAÇÃO 11
3.1 CONTEXTO HISTÓRICO DA INFORMAÇÃO 11
3.2 COMPOSIÇÃO DE UM SISTEMA DE INFORMAÇÃO 12
3.3 A IMPORTÂNCIA DO SISTEMA DE INFORMAÇÃO 13
3.4 CRIMES VIRTUAIS 13
3.5 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO 15
3.6 CONCEITOS AVALIATIVOS DA SEGURANÇA DA INFORMAÇÃO 16
3.7 POLÍTICAS DE SEGURANÇA 16
4 LEI GERAL DE PROTEÇÃO DE DADOS 17
4.1 AGENTES DE TRATAMENTO DE DADOS PESSOAIS 19
4.2 SEGURANÇA 19
4.3 SANÇÕES ADMINISTRATIVAS 20
4.4 ÓRGÃO FISCALIZADOR 20
4.5 ADEQUAÇÃO DAS CORPORAÇÕES BRASILEIRAS À LGPD 20
5 A DIFERENÇA ENTRE LGPD E GDPR 21
6 RESULTADOS E DISCUSSÕES 24
6.1 APLICAÇÃO DA PESQUISA 25
6.2 COLETA DE DADOS 25
7 CONSIDERAÇÕES FINAIS 26
REFERÊNCIAS 28

A LEI GERAL DE PROTEÇÃO DE DADOS IMPLEMENTADA PELOS SETORES DE TI DAS CORPORAÇÕES BRASILEIRAS

Cleydson Ribeiro de Lima
Jefferson Matheus Ferreira da Silva Andrade
Jeremias Barbosa Souza
Ludovica Pereira da Silva

Msc. Ameliara Freire Santos de Miranda.[1]

RESUMO:

O presente trabalho teve como objetivo apresentar alguns tópicos importantes sobre a Lei Geral de Proteção de Dados, sancionada no ano de 2018, um tema que passou a ser muito discutido nos últimos meses nas corporações brasileiras e que vai integrar a área de Tecnologia da Informação com os outros departamentos das empresas. Está prevista para entrar em vigor no segundo semestre no ano de 2020, com a finalidade de intensificar o controle e o manuseio das informações que hoje circulam sem uma devida atenção em diversas organizações de direito público ou privado.

Palavras-Chave: Lei Geral de Proteção de Dados, Segurança da Informação, Tecnologia da Informação.

[1] Professora do Centro Universitário Brasileiro - UNIBRA. Mestre em Informática Aplicada. E-mail para contato: ameliara.unibra@gmail.com.

1 INTRODUÇÃO

Em pleno século XXI vemos que com a globalização e com todos os avanços científicos e tecnológicos no mundo, a necessidade humana de comunicação tem aumentado cada vez mais, a busca constante por informação leva muitas das vezes as pessoas a uma exposição na internet de forma incorreta sem a devida preocupação pela privacidade, isso tem aumentado exponencialmente o número de roubos de dados, tornando as pessoas vulneráveis a ações de criminosos, esse tipo de crime tem se espalhado globalmente, o impacto maior desse tipo de crime está voltado para as corporações pois o volume de dados e muito maior comparado a um única pessoa.

As empresas estão cada vez mais vulneráveis ao roubo de dados, pois muitas não levam a sério a segurança da informação, dentre os mais comuns ataques estão os realizados por Hackers, pessoas que utilizam suas habilidades para praticar crimes, muitas vezes visando as informações contidas dentro das corporações, hoje em dia a venda de dados e muito grande, pois a comercialização desses dados gera informações para terceiros, informações essas que são de grande importância para a corporação.

Na União Europa, no dia 25 de maio de 2018, foi sancionada a GDPR - (General Data Protection Regulation), após escândalos de espionagem e divulgação de dados de clientes envolvendo a Cambridge Analytica e o Facebook em 2016 utilizou vários dados de cidadãos para criar perfis eleitorais influenciando de forma direta nas eleições presidenciais nos Estados Unidos e em outros países também, com tudo isso foi gerado uma grande discussão que culminou na criação da GDPR, que tem seu regulamento aplicado na União Europeia com o maior objetivo de manter as informações das pessoas integras, dando uma aplicação mais aprimorada ao direito da privacidade, e regulamentando as empresas que fazem o uso das informações de terceiros e as responsabilidades que são impostas as mesmas.

Essa questão foi fundamental para termos escolhido esse tema, pois no Brasil até o presente momento não tínhamos uma Lei com vários pontos de responsabilidade, a questão da tratativa dos dados e muito importante, pois as responsabilidades vão muito além do que pensamos a mesma e estabelece que empresas que tenham um tratamento centralizado das informações alocadas dentro do sistema.

Refletindo sobre o tema determinamos o problema de pesquisa:

Quais são as dificuldades que os setores de TI das corporações brasileiras estão encontrando ao implementar a Lei Geral de Proteção de Dados?

Delimitando o problema chegamos aos seguintes objetivos:

Objetivo Geral

Analisar as dificuldades encontradas pelos setores de TI das Corporações brasileiras ao implementar a Lei Geral de Proteção de Dados.

Objetivos Específicos:

a) Apresentar a Lei Geral de Proteção de Dados;

b) Conceituar pontos importantes referente a Lei Geral de Proteção de Dados;

c) Descrever as dificuldades encontradas pelos setores de TI com a implementação da Lei Geral de Proteção de Dados;

d) Identificar a área de atuação dos profissionais de TI em relação a aplicabilidade da Lei Geral de Proteção de Dados.

2 DELINEAMENTO METODOLÓGICO

O nosso trabalho é de natureza bibliográfica e qualitativa. “A pesquisa bibliográfica é desenvolvida com base em materiais já elaborados, constituídos principalmente livros e artigos científicos” (GIL, 2002).

E segundo Fonseca (2002, p. 32),

> A pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto.

A pesquisa qualitativa não está atrelada à representatividade numérica, mas ao examinar o entendimento de um contexto, grupo social, de uma organização e outros (GOLDENBERG, 1997).

Usamos como instrumento de coleta de dados um questionário, com nove perguntas abertas. Na elaboração das perguntas, procuramos investigar o conhecimento dos gestores de TI sobre a LGPD, o entendimento deles sobre a lei e de que formar os mesmos estão implementação em suas empresas.

O questionário foi aplicado a sete gestores de TI que trabalham na empresa Um Telecom no ano de 2019. Eles responderam o questionário nas dependências das empresas onde trabalham.

3 SEGURANÇA DA INFORMAÇÃO

As informações se referem a qualquer conteúdo ou conjunto de dados valiosos para uma organização ou indivíduo específico, é um recurso extremamente valioso na sociedade atual. Ao usar conexões entre redes e sistemas computadorizados, as informações transmitidas em sua grande maioria ficam vulneráveis a ameaças podendo comprometer a integridade dos dados transmitidos, para não comprometer a consistência dos sistemas e garantir que o risco de fraude, erros, vazamentos, roubo, e o uso indevido de informações. Se faz necessário o uso de políticas de segurança interna, pois essas violações afetam diretamente o comportamento dos usuários, do ambiente ou de indivíduos mal-intencionados para roubar, destruir ou alterar informações (DIAS, 2000).

Com a crescente quantidade de informações que circulam constantemente pelas redes, A informação se torna um dos maiores bens das organizações modernas, sendo um produto vital para as mesmas. Portanto, essas informações devem ser protegidas e gerenciadas com eficiência e segurança da informação é usada no contexto atual para proteger sistemas, dados e informações valiosos evitando a perda ou roubo dessas informações, pois se casos essas informações forem violadas elas podem causar grandes danos às empresas (DIAS, 2000).

Vários outros níveis de segurança podem ser definidos e aplicados pelas corporações, uma política de segurança visa sempre garantir que o nível de segurança necessário seja mantido. Há vários fatores que devem ser considerados ao estabelecer uma política de segurança, em muitas empresas ainda insistem em não seguir ou em adotar uma política de segurança (DIAS, 2000).

3.1 CONTEXTO HISTÓRICO DA INFORMAÇÃO

Décadas de 1960 e 1970

Em 1960, os computadores começaram a aparecer logo após as grandes empresas aplicarem suas estruturas, e eles eram raros, contendo principalmente problemas de aplicativos e compatibilidade; em 1970, por permitir o acesso às linhas telefônicas, muitas organizações usavam o acesso remoto às informações. Terminal de computador. É processado por um computador central que gera relatórios e os

passa para computadores que precisam de flexibilidade, mesmo quando o desenvolvimento de sistemas de informação na época estimulou uma série de inovações no ambiente Técnico (DIAS, 2000).

Décadas de 1980 e 1990

Em 1980, com o surgimento dos microcomputadores e a expansão da tecnologia da informação, seguida pelo surgimento de bancos de dados de gerenciamento, sofreram muito porque não possuíam um sistema de armazenamento de informações. Em 1990, o surgimento de sistemas abertos começou no meio do hardware, encerrando assim a questão da compatibilidade de dispositivos (DIAS, 2000).

Após Década de 1990

Com o desenvolvimento contínuo da Internet, várias transformações ocorreram porque a acessibilidade ao compartilhamento de informações e ao armazenamento de dados pode ser alcançada. No mundo globalizado de hoje, uma grande quantidade de informações está sendo transmitida entre as pessoas na velocidade do processamento, transmissão e compartilhamento de informações, e o que acontece a milhares de quilômetros de distância podem ser espalhados (DIAS, 2000).

3.2 COMPOSIÇÃO DE UM SISTEMA DE INFORMAÇÃO

Devido à grande quantidade de dados gerados ao longo do tempo, tivemos que procurar maneiras de transformar esses dados em informações. Daí houve a junção com os sistemas de informação que chegaram a partir dessa necessidade, com base em três estruturas diferentes: Dados, Informações, Conhecimento. Os dados são elementos brutos que não têm significado. As informações são dados que se encontram organizados e que tem um significado. O conhecimento é a informação interpretada.

De acordo com Mitnick (2017, p.15),

> A Privacidade é complexa. Não é uma proposição única para todos. Todos nós temos diferentes razões para compartilhar algumas informações sobre nós mesmos livremente com estranhos e mantendo outras partes de nossas vidas em sigilo. Talvez você simplesmente não queira outro significativo lendo suas coisas pessoais. Talvez você não queira o seu empregador para saber sobre sua vida privada.

Os conceitos são interconectados e interdependentes, porque sem os dados que representam a entidade inicial, não teríamos o conjunto de informações e não teríamos interpretação dos dados, apenas o conteúdo solto não teria sentido. Para um sistema bem organizado, todos os conceitos devem estar sincronizados. Colaborando para fornecer as informações finais.

3.3 A IMPORTÂNCIA DO SISTEMA DE INFORMAÇÃO

Um sistema de informação ajuda a alcançar objetivos organizacionais ou de negócios, sintetiza dados operacionais para facilitar a tomada de decisões, integra dados de fontes externas e internas, organiza o processamento de dados e o fluxo de informações e coleta, analisa, compartilha e monitora informações usando o Gerenciamento suportado (MORIN, 2002, p.39).

O sistema de informação é dividido em quatro partes principais:

- **Input:** envolve a aquisição de dados brutos do ambiente interno ou externo;
- **Processamento:** inclui o processamento dos dados brutos da organização;
- **Saída:** Consiste no resultado dos dados processados e organizados, fornecido ao usuário final.
- **Feedback:** envolve o repasse das informações usadas para avaliar os resultados do fluxo do sistema.

3.4 CRIMES VIRTUAIS

Crimes virtuais referem-se a todas as atividades criminosas que são executadas por um único computador ou por um conjunto de computadores em diferentes regiões ou até mesmo países. Eles são usados com uma grande variedade de métodos e ferramentas, tais como: sniffers, vírus, spyware,

ransomware e engenharia social, com a utilização dessas táticas a maiorias desses grupos visam principalmente o roubo de informações pessoais. A identidade roubada de um indivíduo na sua grande maioria e usada para fraudes, como acesso não autorizado a bancos e a sites comerciais de livre mercado (AVAST, 2018, p.10).

- **Sniffer:** software que tem a função de interceptar e analisar os dados transmitidos em uma rede.
- **Vírus:** software projetado para danificar um sistema. Eles infectam outro software para se espalhar no sistema.
- **Spyware:** é um software desenvolvido cuja função principal é realizar pesquisas de vulnerabilidade.
- **Ransomware:** esse é um tipo de código malicioso que impede o acesso aos dados armazenados em um dispositivo.
- **Engenharia social:** de acordo com Mitnick e Simon (2003, p. VII), "a engenharia social usa poder e persuasão para convencer as pessoas de que a engenharia social é alguém que elas realmente não são" (AVAST, 2018, p.10).

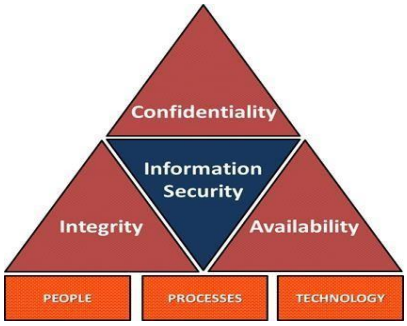
De acordo com a estimativa da Cyberventures, consultoria internacional na área de segurança na Internet, os prejuízos causados com ataques cibernéticos em parâmetro mundial são de mais US$ 8 bilhões em 2019. A consultoria prevê que os crimes cibernéticos custem ao mundo US$ 6 trilhões até 2021. Casos de crimes virtuais têm ocorrido de forma frequente, atingindo geralmente empresas de pequeno e médio porte, pois, devido à falta de investimentos em sistemas de segurança da informação, acabam sendo alvos fáceis (MORGAN, 2019).

Os níveis de proteção dependem do valor que a organização está disposta a pagar em consideração muitas das vezes a importância e medida em cima do potencial dos dados. A segurança não se trata apenas de combater ameaças, mas também de procedimentos e comportamentos que visam impedir vulnerabilidades e impedir ataques quando necessário e bom sempre lembrar que não há segurança perfeita, completa ou absoluta, sempre temos que alcançar uma segurança satisfatória. O que é definido sempre como uma busca para diminuição ou neutralização das possibilidades de crimes cibernéticos (MORGAN, 2019).

3.5 PRINCÍPIOS DA SEGURANÇA DAINFORMAÇÃO

A segurança das informações foi projetada para garantir que as informações sejam protegidas contra vulnerabilidades e que o valor das informações para indivíduos ou para as organizações seja mantido no mais aceitável nível. A segurança da informação enfrenta desafios constantes para alcançar seus pilares, que são designados como os três pilares da CIA, Confidencialidade (*Confidentiality*), Disponibilidade (*Availability)*, Integridade (*Integrity*).

Figura 1 – Segurança da Informação: Tríade CIA



Fonte: livro The Art of Invisibility, Kevin Mitnick.

Princípio da Confidencialidade

Em relação à confidencialidade das informações, assegure-se de que apenas o pessoal autorizado tenha acesso às informações. Para garantir a confidencialidade, é usado o controle de acesso, que pode impedir uma divulgação não autorizada de informações, como autenticação de senha e de permissões de uso (ISO-IEC 17799, 2005, p. 16).

Princípio da Disponibilidade

Permite que as informações estejam disponíveis não apenas para o cliente, mas também para a organização no momento desejado para garantir a continuidade do serviço. A disponibilidade está diretamente ligada à eficácia do sistema e ao seu bom funcionamento. A maneira de garantir a disponibilidade sempre em limite

aceitável pode ser representada também com a realização de backups preventivas (ISO-IEC 17799, 2005, p. 102).

Princípio da Integridade

Garante que as informações não sejam alteradas ou violadas por pessoas não autorizadas e que garanta a integridade das informações para que elas saiam da fonte e cheguem ao seu destino sem serem manipuladas ou alteradas. Os dados permanecem intactos e inalterados. A criptografia e a forma mais usadas para obtenção da integridade de um determinado dado (ISO-IEC 17799, 2005, p. 60).

3.6 CONCEITOS AVALIATIVOS DA SEGURANÇA DA INFORMAÇÃO

Estes são os conceitos para avaliar a competitividade de sistema de informação e sua segurança. São as seguintes:

- **Conformidade:** Semelhante ao princípio da legalidade, a conformidade refere-se aos requisitos legais no processo de segurança da informação, em conformidade com os padrões da organização.
- **Credibilidade:** recursos confiáveis de um sistema consistem na entrega de informações precisas e confiáveis para um usuário, A credibilidade é baseada na conformidade da eficiência.
- **Efetividade:** é a capacidade de produção consistente com um objetivo em atingir um objetivo final. Quanto mais eficaz é um sistema, mais confiável ele se torna.
- **Eficiência:** capacidade de obter o melhor rendimento possível com o mínimo de erros, respeitando o princípio econômico (ISSUU, 2019).

3.7 POLÍTICAS DE SEGURANÇA

A informação é um ativo muito importante para as empresas, que ao longo dos anos, tornou-se quase obrigatório, o uso da tecnologia da informação veio para otimizar os processos de trabalho e trazer uma facilidade na flexibilidade de envio e recebimento das mesmas. Os documentos que geralmente eram armazenados em armários, foram gradualmente transferidos para computadores e transformados de

um documento físico em dados digitais. Devido ao processo de migração, está se tornando cada vez mais importante coletar informações necessárias para proteger os dados do Instituto contra ameaças futuras (ALBERTIN; 2009).

As decisões de segurança tomadas pelos Analistas de Segurança das organizações determinam a segurança da rede, quantas funções ela fornecerá e como será usada. As metas de segurança devem ser determinadas por meio de política de segurança, existem dois tipos de diretrizes que são adotadas pelas empresas: a proibitiva, que significa que tudo o que não é permitido é proibido, e a permissiva, onde tudo o que não é proibido é permitido (ALBERTIN; 2009).

As políticas de segurança são de uma forma muito essencial para um ambiente corporativo, pois e partir dessas definições que é criado e traçado um plano de segurança, o que deixa muitas empresas hoje em dia sem a devida segurança e que muitas não levam muito a sério a questão da segurança deixando a mesma sem segurança. Vale lembrar que dentro de um ambiente de segurança o grande problema hoje enfrentado e em relação a usuários. Que muitas das vezes quebram as políticas e violam uma recomendação (ALBERTIN; 2009).

4 LEI GERAL DE PROTEÇÃO DE DADOS

Em 14 de agosto de 2018, foi sancionada a Lei nº 13.709/2018, nomeada como Lei Geral de Proteção de Dados (LGPD), dispõe sobre o tratamento de dados pessoais por pessoa natural ou pessoa jurídica de direito público ou privado independentemente do meio, do país ou onde esteja localizada a sua sede, desde que a operação de tratamento de dados seja realizada ou coletada em território nacional. O objetivo fundamental da lei é assegurar os diretos a liberdade, a privacidade, e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Com a inserção da internet no meio entre empresas e pessoas físicas, existe uma quantidade gigantesca de dados pessoais que circulam pela internet. A privacidade começou a ser um problema em consequência de práticas que não eram regulamentadas ou proibidas.

A LGPD é uma legislação com interesse em realizar a padronização sobre o assunto de criar regras claras e rígidas sobre a forma de manuseio no tratamento de dados no Brasil, corrigindo as brechas que existem nas leis. Espelhando-se

no Regulamento Geral de Proteção de Dados – GDPR da União Europeia, a LGPD tem o intuito de causar um impacto bastante positivo na sociedade (PINHEIRO, P.P. 2018).

O artigo 5° da LGPD traz conceitos e terminologias que são fundamentais para sua compreensão, para melhor entendimento um quadro foi criado com essas definições.

Quatro 1 – Conceitos Preliminares

CONCEITO	DEFINIÇÃO
DADOS PESSOAIS	Informação relacionada a pessoa natural identificada ou identificável
DADOS PESSOAIS SENSÍVEIS	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.
DADOS ANONIMIZADOS	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
BANCO DE DADOS	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
TITULAR	Pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.
CONTROLADOR	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
OPERADOR	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
ENCARREGADO	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
AGENTES DE TRATAMENTO	O controlador e o operador
TRATAMENTO	Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração
ANONIMIZAÇÃO	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um

	dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Fonte: Lei Geral de Proteção de Dados. Adaptado pelos autores (2019).

4.1 AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Todo o processo de implementação da LGPD exige que a corporação inclua três profissionais em sua estrutura organizacional: o controlador, o operador e o encarregado. O controlador toma decisões a respeito do processamento de dados, o operador coloca suas diretrizes em prática, esses profissionais são chamados de agentes de tratamento. Por fim, o encarregado é responsável por conectar controladores, os titulares dos dados e a Autoridade nacional de Proteção de Dados. (BRASIL, 2018).

Os artigos 37º, 39º e 41º trata sobre as atividades do controlador, operador e encarregado:

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.
> Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.
> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 2º As atividades do encarregado consistem em:
> I - Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - Receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (BRASIL, 2018).

4.2 SEGURANÇA

Segundo PINHEIRO P. P. (2018), os agentes de tratamento têm que adotar medidas de segurança eficientes e adequadas para cada tipo de procedimento realizado com os dados pessoais.

Conforme o art. 46º:

> Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. (BRASIL, 2018).

4.3 SANÇÕES ADMINISTRATIVAS

Conforme o art. 52º da LGPD a empresa que não cumprir a lei será multada em até 2% do seu faturamento, além de outras penalidades previstas no texto, dependendo do grau e da natureza da infração. O valor máximo da sanção é de 50 milhões de reais (BRASIL, 2018).

4.4 ÓRGÃO FISCALIZADOR

De acordo com o art. 55º da LGPD a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), será responsável por zelar pela proteção dos dados, fiscalizar e aplicar sanções caso as corporações descumpram a lei, elaboração e divulgação das políticas nacionais de proteção de dados e privacidade para que a população passe a conhecer a legislação (BRASIL, 2018).

A ANPD também será um elo entre a sociedade e o governo e permitirá que as pessoas enviem perguntas, sugestões e reclamações relacionadas a LGPD para investigação (BRASIL, 2018).

4.5 ADEQUAÇÃO DAS CORPORAÇÕES BRASILEIRAS À LGPD

Para atender aos requisitos regulamentares, as empresas precisam investir na criação de uma estrutura e políticas internas de conformidade digital para o processamento dos dados de seus clientes. Isto se aplica as empresas dos setores público e privado (PINHEIRO P. P., 2018).

A primeira atividade a ser realizada é o diagnóstico por parte da equipe de TI - interna ou terceirizada - com relatórios de análise de risco e análise de impacto de novos requisitos. Com isso, será possível verificar em que estágio a empresa está nessa direção, quais são os pontos mais vulneráveis de seus sistemas e quais são os principais fatores de risco. As empresas devem equipar sua equipe com um número de controladores, operadores e líderes de processamento de dados (PINHEIRO P. P., 2018).

Também é recomendável que as empresas criem um grupo ou comitê exclusivamente responsável pelo desenvolvimento de políticas, metas e planos internos para gerenciamento de proteção de dados e planos de contingência para gerenciamento de crises de segurança e privacidade. É importante que os responsáveis pela tomada de decisões da empresa participem desse comitê para que quaisquer correções e melhorias possam ser feitas com rapidez e eficiência (PINHEIRO P. P., 2018).

Depois de adotar essa estrutura de funcionários, é interessante escrever um manual de políticas internas com base nas diretrizes da empresa sobre este tópico. Investir em programas de treinamento sobre novos regulamentos e processamento de dados é uma maneira de as empresas fortalecerem essa nova política interna e ganharem pontos nessa nova situação do mercado (PINHEIRO P. P., 2018).

5 A DIFERENÇA ENTRE LGPD E GDPR

Influenciada pela General Data Protection Regulation (GDPR), a Lei Geral de Proteção de Dados (LGPD) tem diversas semelhanças com a regulamentação europeu, sendo esta mais detalhada e completa do que a lei brasileira. (MENEZES, 2019)

Ambas as leis são um conjunto de regras jurídicas para coleta, armazenagem e processamento de dados pessoais, efetuadas por pessoas físicas, empresas e organizações públicas. Existem várias semelhanças entre as leis, porém, desde a década de 90, em alguns países da União Europeia já existiam leis que regulamentavam o tratamento de dados pessoais, estando a frente do Brasil, no que

se refere a implementação e desenvolvimento, e consequentemente com um número maior de detalhamento em suas regras. Uma delas seria o conceito de autonomia sobre o controle de informações quando se trada dos dados dos titulares, pois as duas tem a permissão, de que apenas para o controlador pode utilizar esses dados, sendo em clausulas separadas das demais. Também trazem de forma clara e ampla a definição do que vem a ser o processamento de dados pessoais. (MENEZES, 2019)

A GDPR aponta as obrigações das empresas que trabalham com dados pessoais nos países membros da União Europeia e da Área Econômica Europeia, a LGPD determina as atividades das empresas que lidam com os dados privados no Brasil. (MENEZES, 2019)

A GDPR passou a vigorar na União Europeia no dia 25/05/2018 com a Lei Federal nº 13.709/2018, na Europa embasada com bases legais, a LGPD engloba bases legais para justificar o tratamento de dados pessoais. (MENEZES, 2019)

A LGPD é menos detalhista, com muitos pontos em aberto sendo menos rigorosa em relação às penalidades impostas a infratores. (MENEZES, 2019)

A LGPD do Brasil foi influenciada no modelo europeu, a GDPR. No Brasil é permitido a anonimização dos dados no processo de proteção, já na Europa estabelece a criptografia. (MENEZES, 2019)

Na regulamentação Europeia e brasileira é abordada privacidade por padrão, importante conceito para encandeamento e construção de sistemas de proteção. No quadro abaixo pode ser demonstrado algumas diferenças:

Figura 2: Comparativo de LGPD x GDPR

Tópico	GDPR	LGPD
Estão sujeitos à lei	Empresas que atuam na União Europeia, independentemente de sua localização física, e que manipulam dados de pessoas naturais que estejam na região.	Pessoas jurídicas de direito público ou privado que: -Realizam tratamento de dados em território brasileiro; – Cuja atividade de tratamento vise a oferta de bens e serviços ou realize tratamento de dados de indivíduos em território nacional; – Ou cujos dados de tratamento tenham sido coletados em território nacional.
Tratamento de dados sensíveis	Merecem proteção especial e não devem ser tratados, exceto em situações específicas como o cumprimento de uma obrigação legal ou o exercício de funções do interesse público.	Pode ocorrer somente se o titular autorizar, em situações específicas, ou quando estes forem indispensáveis para fins como o cumprimento de obrigação legal pelo controlador, exercício regular de direitos e até mesmo a proteção da vida do titular ou de terceiros.
Tratamento de dados de menores	A partir dos 16 anos de idade, o próprio menor pode dar o consentimento para uso de seus dados.	Em contraste com a GDPR, aqui o consentimento cabe sempre ao responsável legal.
Transferência extraterritorial de dados	A transferência de dados entre países é permitida pela GDPR, desde que comprovado o alto nível de proteção do país receptor e com a autorização da Comissão Europeia.	A norma brasileira e também autoriza a transferência de dados pessoais entre países e órgãos internacionais, mas é necessário que estes tenham o nível de proteção adequado ao que é estabelecido pela regulamentação.
Relatórios de Impacto	É bem clara neste item: em casos onde houver risco elevado aos direitos e liberdades individuais, o responsável pelo tratamento dos dados deve realizar um relatório de impacto. Caso os riscos não sejam passíveis de mitigação, a organização deve consultar a autoridade de controle antes de prosseguir o tratamento.	Apenas mencionando que este poderá ser exigido pela Autoridade Nacional de Proteção de Dados.
Sanção em caso de descumprimento da lei	Em caso de descumprimento da lei, a GDPR determina sanção de 4% do volume global da organização ou uma multa prevista em 20 milhões de euros – o que vale é o maior valor.	No Brasil, a infratora fica sujeita a diversos tipos de sanções, como advertências, multas diárias e multas simples de até 2% do faturamento (em caso de pessoa jurídica de direito privado), limitada em R$50 milhões.
Uso compartilhado de dados	O uso compartilhado de dados não é autorizado pela regulamentação europeia.	O poder público pode compartilhar dados pessoais, desde que para atender a finalidades específicas de políticas públicas ou atribuição legal pelos órgãos e entidades públicas.

Fonte: site: www.guialgpd.com.br

Por fim, como principal diferença entre a LGPD e GDPR esteja na cultura e na legislação europeia que é mais detalhada com sólida cultura de proteção de dados, prevê punições severas aos que a descumprem. Porém, no Brasil está prevista para entrar em vigor a partir de 15/08/2020, com desenvolvimento de matérias complementares à lei e adaptação das empresas às normas. (MENEZES, 2019)

6 RESULTADOS E DISCUSSÕES

A análise dos resultados das entrevistas, que compõe a qualitativa da pesquisa, foi feita utilizando o método de análise de conteúdo. O ponto principal desta pesquisa foi de trazer a percepção dos gestores de TI a respeito da chegada da Lei Geral de Proteção de Dados e a sua implementação pelos setores de TI.

O presente estudo foi realizado com profissionais que estão responsáveis por gerenciar os setores de TI das organizações em que trabalham, a pesquisa foi realizada por meio de questionário contendo 9 perguntas sobre a implementação da Lei Geral de Proteção de Dados, a pesquisa foi realizada nos bairros da Imbiribeira e Boa Viagem, localizadas na cidade de Recife - PE.

O questionário foi elaborado com perguntas abertas para demonstrar o nível de conhecimento dos gestores que o responderam em relação a cada pergunta utilizada sobre a Lei Geral de Proteção de Dados, foi evidenciado que os entrevistados em questão não têm muito conhecimento ou uma perspectiva bem definida em relação a aplicação da lei, em determinados momentos citaram que será necessário aplicar primeiro para se adequar melhor em seu dia-a-dia de trabalho. Contudo serve para conscientizar e regrar a forma de obtenção e tratamento dos dados.

Figura 3 - Questionário apresentado aos entrevistados

Questionario de Perguntas:	
Perguntas	Tipo
1º) Você sabe o que é a LGPD?	Múltipla escolha
2º) Como a empresa na qual você se encontra hoje enxerga as transformações que a LGPD trará ao departamento de TI?	Aberta
3º) Na sua opinião a empresa está preparada para as mudanças com a chegada da LGPD?	Aberta
4º) O corpo administrativo está ciente das mudanças na forma de armazenamentos dos dados dos funcionários e clientes? Se sim, como foram instruídos?	Aberta
5º) O setor de TI atualmente tem políticas de segurança interna? Se sim, explique como é exercida na prática.	Aberta
6º) Na sua opinião a LGPD vai funcionar de fato no Brasil? Favor argumentar.	Aberta
7º) Tendo em vista as várias áreas que a LGPD irá atuar, você acredita que a empresa está trabalhando para manter a conformidade mediante a lei? Se sim, quais	Aberta
8º) Na sua opinião o tempo para adequação da lei nas instituições foi curto? Argumente.	Aberta
9º) Em sua compreensão como cidadão, quais são as perspectivas mediante as propostas da LGPD para a privacidade dos dados no atual cenário brasileiro?	Aberta

Fonte: criado pelos autores (2019)

6.1 APLICAÇÃO DA PESQUISA

Na aplicação da pesquisa foi identificado um certo nível de despreparo das organizações com a manipulação dos dados de terceiros e a suas responsabilidades, em relação a forma da tratativa e prevenção das informações muitas das empresas ainda não estão preparadas para a mudança, pois o alto custo para o contrato das consultorias especializadas é muito alto, também foi descrito o grande problema que hoje as corporações enfrentam, pois muitas não tem políticas de segurança internas ou externas e nem profissionais responsáveis por essa questão, o que deixa claro é que com a implementação da LGPD - Lei Geral de Proteção de Dados, as coisas terão que funcionar de uma forma mais formidável, pois a lei em si estabelece os princípios e padrões que as corporações deverão adotar tendo dentro do ambiente um profissional responsável por tratar e manter em compliance toda estrutura esse profissional tem o nome chamado de DPO - Data Protection Officer, ele vai ser um profissional que estará envolvido em todos os problemas de privacidade relacionado a corporação seja dados dos funcionários ou até mesmo de terceiros, para exercer essa função o profissional precisa ter um conhecimento aprofundado nas leis, certificações e práticas de proteção de dados.

6.2 COLETA DE DADOS

A principal fonte da coleta dados para a análise deste estudo foram as entrevistas realizadas com os gerentes de TI, questionando-os quanto à percepção da diversidade dos dados presente em seu ambiente de trabalho. As entrevistas foram todas transcritas, integralmente, uma a uma, podendo assim ser retirado a amostra dessa coleta, as entrevistas aconteceram em um período de duas semanas, entre o mês de novembro de 2019, com duração de 10 a 20 minutos cada uma.

Figura 4 - Perfil dos Gerentes Entrevistados

Indentificação	Idade	Tempo com Gestor	Formação acadêmica de Origem	Ramo da Empresa	Quantidade de Funcionários
Entrevistado 1*	47	10 Anos	Administração	Financeiro	150 Pessoas
Entrevistado 2*	45	8 Anos	Direito	Varejo	97 Pessoas
Entrevistado 3*	36	8 Anos	Ciência da Computação	Telecomunicações	380 Pessoas
Entrevistado 4*	32	5 Anos	Redes de Computadores	Construção Civil	212 Pessoas
Entrevistado 5*	32	4 Anos	Engenharia da Computação	Varejo	103 Pessoas
Entrevistado 6*	30	3 Anos	Análise e Desenvolvimento de Sistemas	Desenvolvimento de Software	60 Pessoas

Fonte: criado pelos autores (2019)

Com base na pesquisa realizada tivemos a compreensão que pela falta de profissionais qualificados atualmente, as corporações de pequeno e médio porte tendem a terceirizar o trabalho contratando consultorias especializadas na proteção de dados e do profissional responsável por essa função, os responsáveis pelos setores de TI das corporações que utilizamos como amostra de resultado em sua grande maioria tem menção sobre a LGPD, mas não sabem ao certo como será realizada a aplicação da mesma, pois essa situação não envolve apenas os setores de TI mas sim toda a corporação.

7 CONSIDERAÇÕES FINAIS

Atualmente, a LGPD é uma das leis mais importantes em processo de implementação no Brasil, uma lei que tem a finalidade de regulamentar a forma de lidar com a proteção de dados pessoais dos cidadãos brasileiros, o seu impacto é diretamente ligado a qualquer organização presente no território nacional.

Quanto a forma de lidar com dados pessoais, corporativos, e bem como com os dados de terceiros, a LGPD está em conformidade com o GDPR, a Lei Regulamentadora da União Europeia e de todo o seu espaço econômico, uma vez que está sendo aplicada nos países pertencentes à União. Essa maneira de lidar e processar os dados, é muito importante já que os existentes regulamentos não cobriam tudo, apenas adotavam de algumas medidas de privacidade e segurança de dados, medidas essas que muitas das vezes foram violadas por empresas que

usufruíram dos dados de cidadãos para influenciar e comercializar informações dos mesmos ao redor do mundo.

Mapear os dados, classificá-los e usar a tecnologia para se ajustar ao LGPD é de suma importância para os profissionais de TI, pois a segurança dos dados e o seu manuseio torna-se mais seguro e traz uma garantia de maior credibilidade ao mercado corporativo, antes muitas pessoas não tinham conhecimento de como as nossas informações eram compartilhadas e armazenadas, com o grande avanço do desenvolvimento tecnológico presente a cada dia se fez necessário a criação das leis para que adequem-se aos regulamentos que hoje já se encontram presentes em nosso país, pois antes muitas empresas não tinham a responsabilidade para lidar com os nossos dados.

Concluímos que a LGPD é de suma importância para todos nós, há muitas partes da lei que necessitam serem discutidas, pois não deixam de uma forma acessível a sua aplicação, foi visto a tamanha dificuldade que as corporações estão tendo para se adaptarem com a nova lei, podemos descrever que é um avanço muito importante e espera-se um progresso na sua aplicação e que de fato as empresas sejam responsabilizadas caso ocorram problemas de vazamento de dados.

REFERÊNCIAS

BRASIL, Lei nº13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acessado em: 05 Nov.2019.

GOLDENBERG, Mirian. A arte de pesquisar. Rio de Janeiro: Record, 1997.

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2002.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

CARVALHO, Luiz Paulo; OLIVEIRA, Jonice; CAPELLI, Claudia; MAJER, Violeta. Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais. In: Anais do VII Workshop de Transparência em Sistemas. SBC, 2019. p. 21-30.

COELHO, Amanda Carmem Bezerra. A Lei Geral de Proteção de Dados Pessoais Brasileira como meio de efetivação dos direitos da personalidade / Amanda Carmem Bezerra Coelho, João Pessoa, 2019.

COSTA, M. M. da. A era da vigilância no ciberespaço e os impactos da nova lei geral de proteção de dados pessoais no Brasil: reflexos no direito à privacidade. 2018. 93 f. TCC (Graduação) - curso de Direito, Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro - UFRJ, Rio de Janeiro, 2018.

DUNAMYS. Diferença entre LGPD e GDPR. Disponível em <https://www.dunamys.inf.br/diferenca-entre-a-lgpd-e-gdpr/>. Acesso em 28.11.2019

MITNICK, Kevin D.; SIMON, William L. Mitnik A Arte de Enganar. São Paulo: Editora Pearson, 2003.

EUROPA. Regulamento (EU) 679/2016. Disponível em <https://op.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1>. Acessado em 10. Out.2019.

MITNICK, Kevin D.; VAMOSI, Robert. The Art of Invisibility. New York: Little Brown, 2017.

FONSECA, J. J. S. Metodologia da pesquisa científica. Fortaleza: UEC, 2002.

MENEZES, Karina.GUIALGPD. Disponível em <https://guialgpd.com.br/comparativo-entre-lgpd-x-gdpr/>. Acessado em: 10 Nov. 2019.

DIAS, Claudia. Segurança e Auditoria da Tecnologia da Informação. Editora: Axcel Books 142, 2000. ISBN 85-7323-231-9.

MORGAN, Steve, CYBERCRIME MAGAZINE. Disponível em <https://cybersecurityventures.com/cybersecurity-almanac-2019/>. Acessado em: 10 Nov. 2019.

MORIN, E. Ciência com consciência. Rio de Janeiro: Bertrand, 2000.

ALBERTIN, A. L.; ALBERTIN, R. M. M. Dimensões do uso de tecnologia da informação: um instrumento de diagnóstico e análise. Revista de Administração Pública, v. 46, n. 1, p. 125-151, 2012.

NBR ISO/IEC 17799 - Tecnologia da informação - técnicas de segurança. 2. ed. Rio de Janeiro: ABNT, 2005.

AVAST. Crimes Virtuais. Disponível em <https://www.avast.com/pt-br/c-cybercrime>. Acessado em: 07 Nov. 2019.

ISSUU. Segurança da Informação. Disponível em <https://issuu.com/jonclash/docs/seguranc_a_da_informac_a_o>. Acessado em: 04 Out. 2019.