UNIVERSIDADE CATÓLICA DE PERNAMBUCO

CENTRO DE CIÊNCIAS E TECNOLOGIA

TRABALHO DE CONCLUSÃO DE CURSO

PROTEÇÃO DE DADOS PESSOAIS MEDIANTE AS LEIS LGPD E GDPR

por

RENATO ANTÔNIO DOS SANTOS

Recife, Junho de 2020

UNIVERSIDADE CATÓLICA DE PERNAMBUCO

CENTRO DE CIÊNCIAS E TECNOLOGIA

CURSO DE CIÊNCIA DA COMPUTAÇÃO

TRABALHO DE CONCLUSÃO DE CURSO

PROTEÇÃO DE DADOS PESSOAIS MEDIANTE AS LEIS LGPD E GDPR

por

RENATO ANTÔNIO DOS SANTOS

Monografia apresentada ao curso de Ciência da Computação da Universidade Católica de Pernambuco, como parte dos requisitos necessários à obtenção do grau de Bacharel em Ciência da Computação.

ORIENTADOR: Fernando José Bertino de Figueiredo, MSc.

Recife, Junho de 2020

Dedico este trabalho à Srª Cláudia Maria Ferreira (Dáda), minha sogra, que hoje está no céu, mas sempre estará no meu coração.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, que é o meu refúgio e fortaleza.

Agradeço à minha mãe, Srª Maria José Simplício dos Santos, por investir em mim e em meus sonhos.

Agradeço à minha esposa, Srª Maria Cláudia Ferreira Marcelino dos Santos, por me fazer ser uma pessoa melhor, a cada dia.

Agradeço a Universidade Católica de Pernambuco pela oferta do conhecimento científico por meio dos docentes do curso de Ciência da Computação e a todos que direta ou indiretamente ajudaram de alguma forma.

PROTEÇÃO DE DADOS PESSOAIS MEDIANTE AS LEIS LGPD E GDPR

RESUMO

As pessoas estão cada vez mais se expondo na Internet. Seja através de fotos, textos, vídeos, números de documentos, cadastros feitos em sites ou pesquisas de opinião. Em muitas dessas situações, dados pessoais são solicitados e não se tem um entendimento do que está sendo feito. A ação de enviar sua informação pessoal, sem questionar, é quase que automática. E isso torna-se muito mais perigoso quando não se tem uma legislação apropriada. O objetivo deste trabalho busca compreender o que há de concordância entre a LGPD e a GDPR. Para isso, foi realizada uma pesquisa bibliográfica, analisando tópicos dessas duas leis. A conclusão dessa pesquisa é que, apesar da LGPD ser inspirada na GDPR, poucos são os tópicos que se assemelham. Outro ponto importante é que, sim, a LGPD trará uma grande segurança para o cidadão.

Palavras-chave: **General Data Protection Regulation, Lei Geral de Proteção de Dados, Segurança da Informação.**

PERSONAL DATA PROTECTION UNDER THE LGPD AND GDPR REGULATIONS

ABSTRACT

People are increasingly exposing themselves on the Internet. Whether through photos, texts, videos, document numbers, entries made on websites or opinion polls. In many of these situations, personal data is requested and there is no understanding of what is being done. The action of sending your personal information, without questions, is almost automatic. This becomes much more dangerous when there is no appropriate legislation. The objective of this work is to understand what is in agreement between the LGPD and the GDPR. For this, a bibliographic research was carried out, analyzing topics of these two laws. The conclusion of this research is that, although the LGPD is inspired by the GDPR, few topics are similar. Another important point is that the LGPD will bring great security to the citizen.

Keywords: **General Data Protection Regulation, Lei Geral de Proteção de Dados, Information Security.**

LISTA DE TABELAS

LISTA DE ABREVIATURAS / SIGLAS

Termo		**Descrição**
GDPR	General Data Protection Regulation	Regulamento Geral de Proteção de Dados
IEC	International Electrotechnical Commission	Comissão Eletrotécnica Internacional
ISO	International Organization for Standardization	Organização Internacional de Normalização
LGPD	-	Lei Geral de Proteção de Dados
SQL	Structured Query Language	Linguagem de Consulta Estruturada
TI	-	Tecnologia da Informação
UE	-	União Europeia

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

Atualmente, as empresas têm como algo valioso sua base de dados. Infelizmente nem todas tratam a segurança como prioridade. São recorrentes as notícias de empresas que sofreram vazamento de dados. Como exemplos podem ser citados dois casos: Em 2017 a empresa Uber revelou um vazamento de 57 milhões de dados de seus usuários e motoristas (OLHAR DIGITAL, 2018). Já a empresa Netshoes relatou que em 2017 e 2018 sofreu do mesmo problema, com o vazamento de quase 2 milhões de dados de clientes (TECNOBLOG, 2019).

Os dados sozinho não é capaz de fazer muita coisa, mas, dependendo de como é utilizado, pode fazer com que as empresas ganhem (ou percam) muito dinheiro, sabendo como transformá-los em informação. O grande diferencial das empresas bem sucedidas, hoje em dia, é a forma como essas protegem os dados (TI INSIDE, 2019). Foi pensando em se adequar às leis estrangeiras que começou-se a pensar em uma legislação para o Brasil - a Lei Geral de Proteção de Dados (LGPD).

Muitas pessoas sequer sabem como seus dados pessoais são obtidos e como são utilizados. Não são só empresas que capturam os dados pessoais. Pessoas má intencionadas criam programas maliciosos com essa mesma finalidade. É bem verdade que profissionais da área de TI (Tecnologia da Informação) possuem conhecimento e técnicas para analisar os dados que trafegam pela rede, a fim de encontrar possíveis erros nela. O crime está no ato de se obter tais dados para realizar ações maléficas.

E é sob esse aspecto que a LGPD (BRASIL, 2018) irá atuar. Mostrando como, quem e quais dados poderão ser manipulados. Trazendo, assim, uma maior segurança para o cidadão brasileiro.

1.2 Motivação

A produção desse trabalho justifica-se pela constatação de que há, em relação à vulnerabilidade no tratamento dos dados pessoais, por parte das empresas, escassez de estudos no sentido de fazer um levantamento de tais vulnerabilidades, a fim de minimizar custos em casos de processo por perda de dados e mitigar erros, em caso de multa por vazamento de dados.

1.3 Objetivos

1.3.1 Objetivo Geral

O trabalho tem como objetivo geral a comparação dos principais conceitos da LGPD em relação aos do Regulamento Geral de Proteção de Dados (GDPR - *General Data Protection Regulation*), que entrou em vigor em 25 de maio de 2018 (GOMES, 2018).

1.3.2 Objetivos Específicos

- Verificar formas de ameaça à segurança da informação;
- Demonstrar como os dados pessoais podem ser interceptados / obtidos;
- Analisar a LGPD e a GDPR.

1.4 Metodologia

Para a realização do presente trabalho, foi feita uma pesquisa bibliográfica, sem um protocolo específico. Segundo PIZZANI *et al.* (2012), é a revisão da literatura sobre as principais teorias que norteiam o trabalho científico. Essa pesquisa, realizada com o levantamento e leitura das duas leis, destaca entre elas os pontos que mais se assemelham. Por tratar-se de um assunto relativamente novo e que está em constante mudança, para embasar ainda mais a fundamentação teórica, foi necessário buscar definições e argumentações em sites da Internet que abordam o assunto em questão. Além disso, esse trabalho traz algumas formas de

ameaça à segurança da informação e um tópico demonstrando como os dados pessoais podem ser interceptados por criminosos.

1.5 Organização

Este trabalho divide-se em quatro capítulos: o Capítulo 1 refere-se a um questionamento sobre a importância de se manter os dados pessoais seguros e fala um pouco sobre a forma como as empresas utilizam os dados. Também traz na seção Introdução os tópicos Contextualização, Motivação, Objetivos (Geral e Específicos), Metodologia e Organização. Este capítulo traz como motivação a escassez de estudos sobre vulnerabilidades na manipulação de tais dados.

Já, o Capítulo 2 enfatiza a Segurança da Informação, trazendo informações sobre os Atributos Básicos e listando algumas Ameaças à Segurança, como ataques do tipo Engenharia Social, *Sniffer* e a banco de dados de Linguagem de Consulta Estruturada (SQL - *Structured Query Language*).

O Capítulo 3 aprofunda-se no tema desta monografia: a LGPD. Esta seção traz a problematização do objetivo geral do trabalho, bem como o Histórico da Lei, diretrizes, características e uma breve comparação entre a LGPD e a GDPR.

E, por fim, o Capítulo 4, que traz a conclusão deste trabalho.

2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação está diretamente relacionada com a proteção de um conjunto de informações, preservando o valor que possuem, para um indivíduo ou uma organização (WIKIPÉDIA, 2020).

2.1 Atributos Básicos

Os atributos básicos da segurança da informação, segundo os padrões internacionais (ISO/IEC 27000) são os seguintes:

- Confidencialidade: propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;
- Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente). O ciclo de vida da informação orgânica - criada em ambiente organizacional - segue as três fases do ciclo de vida dos documentos de arquivos; conforme preceitua os canadenses da Universidade do Quebec (Canadá): Carol Couture e Jean Yves Rousseau, no livro Os Fundamentos da Disciplina Arquivística;
- Disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

2.2 Ameaças à Segurança

As ameaças à segurança vão além de problemas com *malware* e invasões. Criminosos tentam, a todo custo, obter o máximo de informações possíveis em relação ao seu alvo. Para isso, investem tempo e energia na busca de técnicas para obter informações preciosas.

2.2.1 Engenharia Social

Engenharia social, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações (WIKIPÉDIA, 2020). É um artifício utilizado por criminosos virtuais, para conseguir dados confidenciais de pessoas ou empresas. Tal procedimento pode ser feito através de contato via telefone, mensagens de e-mail ou links maliciosos enviados através das redes sociais.

Existem algumas técnicas que utilizam a engenharia social como base. Uma delas é o *Phishing* (UOL SEGURANÇA, 2013). O termo deriva das palavras inglesas *phreaking* (entusiastas que faziam experimentos com as redes de telecomunicações) + *fishing* (pescaria) e é um tipo de ataque onde o criminoso "pesca" informações da vítima, através de um site na Internet.

Muitos *softwares* de antivírus não são capazes de identificar esse tipo de ataque. Pois, na mensagem de e-mail e no link malicioso não há nada de errado. Todo processo, desde a leitura da mensagem de e-mail até o acesso ao site malicioso é feito por livre e espontânea vontade do usuário. O problema ocorre quando dados pessoais são inseridos nesses sites. Para ajudar na identificação de mensagens maliciosas, algumas coisas podem ser feitas:

- Procurar erros de português tanto no endereço de e-mail quanto no corpo da mensagem;
- Verificar se o endereço do remetente condiz com a empresa que o enviou;
- Verificar se o layout do e-mail (tipo de fonte, cores utilizadas na mensagem) condiz com o que é veiculado em propagandas.

Criminosos utilizam essa técnica a fim de conseguir algum tipo de vantagem sobre as empresas. O esforço tem suas recompensas. Quando bem sucedido, esse ataque proporciona acesso à dados confidenciais de funcionários, dados financeiros e até informações estratégicas, dependendo do ramo da empresa.

Essa técnica utiliza-se da boa intenção da vítima que, em muitos momentos, acha que está fazendo algo positivo. Quando, na verdade, está sendo induzida a cometer tais erros. Um criminoso pode, por exemplo, se passar por um novo funcionário da empresa e solicitar que pessoas de um determinado setor acessem um link para efetuar atualizações nas estações de trabalho. Esse tipo de ataque tem boas chances de ser feito sem nenhum problema, pois:

- Os antigos funcionários estarão fazendo seu trabalho, ajudando alguém que está começando agora na empresa;
- Certamente não estranharão a aparência de um determinado site pois, na teoria, é algo interno;
- Caso o sistema operacional emita algum aviso sobre a integridade do arquivo, esse poderá ser ignorado, visto que é algo feito por alguém inexperiente.

O ataque, para ser bem sucedido, leva um certo tempo. O criminoso precisa antes coletar informações sobre a empresa, nomes de funcionários, setores internos, etc. Isso será utilizado para conseguir passar credibilidade às vítimas.

Tudo pode começar com uma simples ligação telefônica. O criminoso pergunta por uma pessoa qualquer. Ao final da ligação, deseja-se saber o nome de quem está dando a informação. Supõe-se que seu nome seja “João”.

Na próxima abordagem, o criminoso diz que precisa entregar a “João” um determinado documento, mas que não sabe em qual setor trabalha. Provavelmente a vítima dirá essa informação, já que pensa ser alguém que, de fato, conhece o funcionário.

De posse dessas informações (nome do funcionário e setor) o criminoso, munido de uma mídia física com alguma espécie de *malware* (AVG, 2020), se encarrega de instalar o software malicioso em uma ou mais estações de trabalho. Com isso, encerra-se a etapa de infecção e o criminoso já está com acesso remoto garantido. O próximo passo é monitorar a rede interna, buscando por credenciais,

documentos internos, números de cartão de crédito ou qualquer coisa que lhe possa ser de valor.

2.2.2 Sniffer

Sniffer (ou sniffing) é uma técnica utilizada por investigadores para capturar pacotes de dados sendo transferidos através de uma rede (Portal GSTI, 2019).

Em alguns momentos, o tráfego da rede pode ficar instável e, com isso, dados podem ser perdidos durante a transmissão. Essa perda pode ocorrer por problema físico, ocasionado por rompimento de cabo ou desligamento inesperado de um dispositivo, ou lógico, no caso de algum endereço de rede ser alterado ou corrompido.

Muitos profissionais de TI o utilizam para identificar comportamentos anormais na rede ou verificar a execução de um programa que envia e recebe dados de um cliente para um servidor (Michaelis, 2020). O programa analisa cada pacote que trafega na rede, identificando origem, destino, tamanho e conteúdo do pacote. Em geral, um pacote de dado tem como destino um endereço específico. Mas nesse caso, independente do endereço que tenha, o dispositivo que estiver executando tal aplicação, conseguirá ler tais dados.

Um criminoso, por exemplo, pode utilizar essa ferramenta na rede interna de uma empresa. Esse processo leva um certo tempo, pois será preciso capturar os dados que trafegam pela rede. Quanto mais tempo um sniffer está em execução na rede, mais dados são capturados. Tudo que é enviado ou recebido, de um dispositivo para outro e que não esteja criptografado será capturado pelo criminoso e salvo em um arquivo texto, que poderá ser visto de tempos em tempos. Nessa captura poderá ter de tudo: de credenciais de e-mails a dados bancários.

2.2.3 SQL Injection

O SQL Injection é uma técnica de ataque baseada na manipulação do código SQL, que é a linguagem utilizada para troca de informações entre aplicativos e

banco de dados relacionais (DEVMEDIA, 2007). Boa parte dos sites hospedados na Internet que possuem um sistema de cadastro ou um campo de pesquisa, certamente estão utilizando um servidor de banco de dados.

O criminoso tenta, de diversas formas, obter acesso não autorizado a um servidor. Uma dessas formas é fazer com que o servidor que está sendo atacado gere um erro quando se insere um tipo de pesquisa personalizada na sua base de dados. A partir desse erro específico, o criminoso consegue injetar comandos legítimos, que acabam por retornar valores que foram previamente cadastrados.

Utilizando-se desse método, um criminoso pode pular diversas etapas em um ataque. Em muitos casos um usuário pode utilizar a mesma senha em diversos tipos de serviço e isso torna o ataque um pouco mais grave.

A forma mais comum de exploração desse ataque é com a utilização de ferramentas que automatizam o processo. Uma dessas ferramentas, certamente a mais popular, é a sqlmap (SQLMAP.ORG, 2020). Com ela, basta inserir o endereço de um site, pressionar a tecla Enter e aguardar o processo chegar ao fim. O resultado da varredura varia, podendo ser o nome do banco de dados, credenciais de acesso (nome de usuário e senha) ou tabelas do banco de dados.

Existem outros tipos de ataque que não foram listados neste capítulo, como por exemplo:

- Negação de serviço (DoS) - Técnica que consiste em esgotar os recursos de um servidor, deixando-o indisponível por um período de tempo;
- Força bruta - A ideia desse ataque é utilizar um dicionário, que vai tentando todas as combinações possíveis de usuário e senha em um determinado serviço (site da Internet, e-mail ou servidor FTP, por exemplo);
- Desfiguração de página (Defacement) - Técnica utilizada para alterar o conteúdo de uma página da Internet, explorando erros de servidores ou aplicações.

Como mencionado anteriormente, esses ataques não foram abordados no texto, pois são utilizados de forma secundária nos ataques e não como forma específica para se obter informações.

3 LEI GERAL DE PROTEÇÃO DE DADOS

Os mecanismos legais atuais não conseguem, de forma satisfatória, impedir ou regulamentar certos comportamentos adotados por parte de algumas empresas, em relação ao uso e armazenamento dos dados de seus clientes. Não se tinha, até então, algo que pudesse punir a comercialização dos dados pessoais, por exemplo. Foi pensando nisso que se começou a discutir a criação e, consequentemente, a implementação de um mecanismo legal que protegesse a integridade do cidadão. Assim, surgiu a LGPD.

3.1 O que é LGPD?

A Lei Federal nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018), traz uma série de regras em relação ao tratamento dos dados pessoais, seja no meio digital ou analógico, com a finalidade de proteger o cidadão a respeito do que é feito com suas informações pessoais. Esse conjunto de novas regras será válido em todo o território nacional, prevalecendo, inclusive, sobre leis municipais e estaduais.

Juntamente com a Lei, foi criado, ainda que somente no papel, um órgão para regular e fiscalizar as operações feitas com dados pessoais, a Autoridade Nacional de Proteção de Dados (ANPD). Mas essa ainda não está em funcionamento (CORREIO BRAZILIENSE, 2020).

3.2 Histórico da LGPD

Há algum tempo os dados pessoais são utilizados com o intuito de direcionar a atenção das pessoas para determinado produto ou serviço. Até então isso era feito de forma indiscriminada e totalmente sem o conhecimento (e consentimento) das pessoas. O máximo que poderia ser feito era utilizar a lei vigente sobre direitos do consumidor. Com isso, viu-se a necessidade de se criar algo especificamente para os dados pessoais.

Em novembro de 2010 começou-se a falar, no Brasil, sobre a proteção dos dados pessoais, com a intenção de se elaborar uma lei específica sobre o tema (REDEBRASILATUAL, 2010). A partir dessa data, diversos deputados criaram projetos de lei, debates e consultas públicas foram feitas, em busca de algo que desse uma maior proteção ao cidadão brasileiro.

O que de fato impulsionou a criação da LGPD foi a entrada em vigor da GDPR, na Europa. Essa lei europeia serviu de base para a criação da lei brasileira.

3.3 Diretrizes da LGPD

O Art. 5° da Lei (BRASIL, 2018) traz com clareza, diversas definições que ajudará na compreensão do texto. São elas:

- Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- Dado anonimizado: 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 objeto 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;
- Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
- Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
- Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

- Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e
- Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A grande questão é o uso inadequado dos dados por parte das empresas, muitas vezes sem o consentimento do titular dos dados pessoais. Em muitos casos, os dados pessoais são utilizados para traçar as preferências do cidadão e enviar propagandas que parecem adivinhar o pensamento das pessoas. Basta uma simples pesquisa em um buscador eletrônico e anúncios semelhantes parecem brotar no navegador, rede social ou no aparelho smartphone. Isso acontece em diversas áreas: seja em bens de consumo, produtos, serviços ou direcionamento político, servindo para eleger políticos (FOLHA DE S.PAULO, 2018).

Sobre o tratamento dos dados, o Art. 6o da Lei n° 13.709, de 14 de agosto de 2018 (BRASIL, 2018) define bem quais atividades poderão ser realizadas a respeito dos dados pessoais:

- Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- 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;

- Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Assim como o inciso I do Art. 7° trata a finalidade dos dados, o Art. 8o demonstra a forma como o controlador deve solicitar o consentimento do titular: “deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular” (BRASIL, 2018). E continua com os seguintes parágrafos:

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

3.4 Comparação entre a GDPR e a LGPD

A GDPR serviu de base para a criação da LGPD. Na União Europeia, a lei já opera desde o ano de 1995 (DRZ.global, 2018). Com o passar do tempo, teve de sofrer algumas alterações para se adequar à questões tecnológicas. Essa atualização ocorreu em 2018 e é o que se conhece como GDPR. Entretanto, apesar de se basear na lei europeia, as duas têm pontos que divergem.

Um fato que merece ser levado em consideração é que, apesar de estar em vigor desde 2018, menos da metade das empresas europeias utilizam a GDPR. Os executivos identificaram algumas barreiras para alcançar a conformidade total com a GDPR. São elas: alinhar os sistemas de TI legados (38%); a complexidade dos requisitos da GDPR (36%); e os custos proibitivos para alcançar o alinhamento com os regulamentos (33%) (E-COMMERCE BRASIL, 2019).

3.4.1 Tratamento de dados sensíveis

A LGPD protege, de forma especial, os dados sensíveis e ainda diz que, o tratamento de tais dados poderá ocorrer somente nas hipóteses trazidas na Lei. Ou seja, quando o titular ou responsável consentir, de forma específica, para finalidades específicas, ou quando, sem o consentimento do titular, nas hipóteses em que for indispensável. Já a GDPR proíbe o tratamento de tais dados, com algumas

exceções. Duas dessas exceções não constam na lei brasileira (art. 11, I e II, da Lei 13709/2018; capítulo II, artigo 9.°, n.° 2, alínea d, do Regulamento (UE) 2016/679):

1. Dados que foram tornados públicos pelo próprio titular;
2. Dados relativos à membros ou ex-membros de associações, fundações ou organizações sem fins lucrativos. Desde que para fins legítimos.

3.4.2 Tratamento de dados de menores

Para a nossa lei, assim como em outros aspectos relacionados à pessoas menores de 18 anos de idade, é obrigatório o consentimento dos pais ou responsável legal para o tratamento de dados pessoais, de acordo com o que consta no Estatuto da Criança e do Adolescente. A coleta de tais dados poderá ser feita sem o consentimento dos responsáveis no caso de ser necessário contatar os pais ou responsável legal. A lei europeia aceita que o consentimento seja dado por um menor, mas desde que o mesmo tenha, pelo menos, 16 anos (art. 14, § 1° e 3°, da Lei 13709/2018; capítulo II, artigo 8.°, n.° 1, do Regulamento (UE) 2016/679).

3.4.3 Políticas de proteção de dados

A LGPD trata da implementação de programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

A GDPR atribui ao responsável pelo tratamento dos dados a obrigação de adotar medidas técnicas e organizativas que sejam adequadas para assegurar que o tratamento é realizado em conformidade com a lei (art. 50, § 2º, I, a, da Lei 13709/2018; capítulo IV, artigo 24.°, n.° 1, do Regulamento (UE) 2016/679).

3.4.4 Representantes

A regulamentação brasileira prevê que a empresa estrangeira será notificada e intimada de todos os atos processuais previstos na Lei. Independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil (art. 61, da Lei 13709/2018).

Diferentemente da lei brasileira, a GDPR diz que o responsável pelo tratamento ou o subcontratante designa, por escrito, um representante seu na União (capítulo IV, artigo 27.°, n.° 1, do Regulamento (UE) 2016/679)

3.4.5 Responsabilização dos agentes

A lei brasileira é bastante direta quando se trata da responsabilização dos agentes, no cumprimento do seu dever. Existem três hipóteses em que o agente de tratamento, seja ele controlador ou operador, não é responsabilizado:

1. Quando o agente não estiver envolvido com o tratamento dos dados;
2. Quando, embora tenham realizado o tratamento dos dados, não houver violação à LGPD;
3. Quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Nesse ponto as duas leis se assemelham. Pois, a GDPR trata dos incisos I e II da LGPD (art. 43, I, II e III, da Lei 13709/2018; razão 146, do Regulamento (UE) 2016/679).

3.4.6 Marketing direto

Sobre o marketing direto, a lei brasileira diz que o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas. Também fala que, quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para tal finalidade, poderão ser tratados.

Já a lei européia fala que o tratamento de dados pessoais, estritamente necessário aos objetivos de prevenção e controle da fraude, constitui, igualmente, um interesse legítimo do responsável pelo seu tratamento (art. 10, II, § 1º, da Lei 13709/2018; razão 47, do Regulamento (UE) 2016/679).

3.4.7 Relação entre controlador e operador

O operador deve realizar o tratamento segundo as instruções fornecidas pelo controlador, mas não informa se é necessária a formalização por meio de contrato. A GDPR diz que o operador deve realizar seu trabalho regido por um contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros (art. 39, da Lei 13709/2018; razão 81, do Regulamento (UE) 2016/679).

3.4.8 Relatório de impacto

Existe na lei brasileira, a definição de relatório de impacto, mas não fica claro em quais situações o controlador será obrigado a realizar tal relatório. A lei europeia diz que o controlador deve realizar uma avaliação de impacto da proteção de dados, nos casos em que a operação de tratamento de dados seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas (art. 5º, XVII, da Lei 13709/2018; razão 84, do Regulamento (UE) 2016/679).

3.4.9 Transferência internacional de dados

A lei brasileira permite a transferência de dados pessoais para países ou organismos internacionais que proporcionem grau de proteção de dados adequados ao previsto na LGPD e quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, direitos do titular e do regime de proteção de dados previstos na lei.

No entanto, a lei europeia diz que quando os dados são transferidos para outros países, o nível de proteção das pessoas deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados para uma organização internacional (art. 33, I e II, da Lei 13709/2018; razão 101, do Regulamento (UE) 2016/679).

3.4.10 Fiscalização do cumprimento da Lei

A fiscalização do cumprimento da Lei ficará a cargo da Autoridade Nacional de Proteção Dados Pessoais (artigo 55-J, inciso IV). Mas essa ainda não está em funcionamento. A lei europeia estabelece a criação do Comitê Europeu para a Proteção de Dados (art. 55-J, IV, da Lei 13709/2018; capítulo VII, seção 3, artigo 68.º, do Regulamento (UE) 2016/679).

3.5 Síntese da comparação

Nesta seção será apresentada a comparação entre as duas leis.

Tabela 1 - Comparação entre tópicos das leis LGPD e GDPR

	LGPD	**GDPR**
Tratamento de dados sensíveis	Protege os dados sensíveis	Proíbe o tratamento dos dados sensíveis, com exceções
Tratamento de dados de menores	Obrigatório por parte do responsável legal	Por menor que tenha acima de 16 anos
Políticas de proteção de dados	Controle facultativo por controladores de dados	Controle obrigatório por controladores de dados

Representantes	Um representante por país	Um representante por Estados-Membros
Responsabilidade dos agentes	Existem três hipóteses em que o representante não é responsabilizado	Existem duas hipóteses em que o representante não é responsabilizado
Marketing direto	O titular dos dados é soberano sobre eles	O titular dos dados é soberano sobre eles
Relação entre controlador e operador	Não há contrato formal exigido para o controle dos dados	Exige um contrato formal para o controle dos dados
Relatório de impacto	Não fica claro na Lei em quais situações será realizado	O controlador deve prover um relatório de impacto à proteção dos dados pessoais
Transferência internacional de dados	Permite a transferência dos dados para países ou órgãos onde existe uma equivalência à Lei	A transferência dos dados pode ser realizada, independente da autorização específica
Fiscalização do cumprimento da Lei	Autoridade Nacional de Proteção de Dados, mas ainda não está em vigor	Comitê Europeu para Proteção de Dados

Com a tabela acima, fica claro que a LGPD, apesar de ser baseada na GDPR, tem apenas três dos dez tópicos aqui listados em comum.

4 CONCLUSÃO

A partir da análise dos pontos que convergem entre a LGPD e a GDPR foi possível concluir que, poucos são os tópicos que, de fato, se assemelham. Eles, em sua grande maioria, divergem. Apesar da LGPD ter sido inspirada na GDPR, a pesquisa mostra que a nossa lei tem sua personalidade.

Mesmo estando em vigor há um ano, na Europa, menos da metade das empresas utilizam a lei europeia, o que é lamentável. Empresas que, notoriamente, protegem os dados pessoais dos seus clientes, passam uma sensação de confiança.

As pessoas estão, cada vez mais, colocando sua vida, em forma de *bytes*, na Internet. Seja como um texto em uma rede social, uma foto em um aplicativo ou um vídeo mostrando o dia a dia, o fato é que elas se tornam mais vulneráveis com a exposição excessiva. Com isso, será preciso criar mais mecanismos que garantam a segurança e integridade dos dados pessoais. A LGPD trará, sem dúvidas, uma grande segurança para o cidadão, que até então não sabia o que fazer quando se sentia lesado em relação ao mau uso dos seus dados pessoais.

4.1 Limitações do trabalho

Em virtude da pandemia do Coronavírus, ocorrida no primeiro semestre de 2020, a entrada em vigor da lei foi adiada e, com isso, não foi possível verificar quais empresas utilizam a LGPD.

4.2 Trabalhos futuros

A entrada em vigor permite que sejam feitos novos estudos da comparação entre as duas leis. Com isso, estudos futuros podem abordar pontos interessantes, como:

- Identificação de empresas, sejam elas públicas ou privadas, que utilizam a LGPD, a fim de verificar como se deu a implementação da lei nessas empresas;
- Verificação de vulnerabilidades no tratamento dos dados pessoais, visando, primeiramente, a proteção do cidadão;
- Criação de planos para mitigação de erros e minimização de custos, em caso de vazamento de dados, para que o prejuízo tanto para as empresas quanto para os cidadãos seja o mínimo possível.

O que se pode aprender com o presente estudo é que segurança nunca é demais. Proteção de dados pessoais não é “coisa de filme”. Quando o roubo vem a ser notado, o prejuízo pode ter chegado em níveis deletérios. As pessoas tendem a acreditar somente naquilo que pode ser visto, como um assalto à mão armada, por exemplo. E, juntamente com a constatação do roubo, vem a sensação de constrangimento, por ter caído num golpe ou por ter sido roubado. Se tem algo dentro de um projeto, empresa ou organização que precisa ser levado a sério, é a segurança dos dados.

5 REFERÊNCIAS BIBLIOGRÁFICAS

SANTINO, Renato. Uber é multada após esconder vazamento de dados de 57 milhões de usuários. Olhar Digital, 2018. Disponível em: <https://olhardigital.com.br/noticia/uber-e-multada-apos-esconder-vazamento-de-dados-de-57-milhoes-de-usuarios/78801>. Acesso em: 15 mar. 2020

VENTURA, Felipe. Netshoes paga R$ 500 mil em danos morais após vazamento de dados. Tecnoblog, 2019. Disponível em: <https://tecnoblog.net/277594/netshoes-acordo-mpdft-vazamento-dados/>. Acesso em: 15 mar. 2020

Pesquisa: consumidores rejeitam empresas que não protegem seus dados. TI INSIDE, 2019. Disponível em: <https://tiinside.com.br/14/10/2019/pesquisa-consumidores-rejeitam-empresas-que-nao-protegem-seus-dados/>. Acesso em: 15 abr. 2020.

BRASIL, Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 19 mar. 2020.

BRASIL, MEDIDA PROVISÓRIA Nº 959, DE 29 DE ABRIL DE 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm>. Acesso em: 10 mai. 2020.

GOMES, Helton Simões. Lei da União Europeia que protege dados pessoais entra em vigor e atinge o mundo. G1, 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda.ghtml>. Acesso em: 10 mai. 2020.

GDPR. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e40-1-1>. Acesso em: 20 mar. 2020.

PIZZANI, Luciana et. al. Pesquisa bibliográfica. UNICAMP, 2012. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/download/1896/pdf_28>. Acesso em: 10 mai. 2020.

ISO/IEC 27000. WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2020. Disponível em: <https://pt.wikipedia.org/wiki/ISO_/_IEC_27000>. Acesso em: 19 jun. 2020.

SEGURANÇA DA INFORMAÇÃO. WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2020. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Seguran%C3%A7a_da_informa%C3%A7%C3%A3o&oldid=58310445>. Acesso em: 20 jun. 2020.

ENGENHARIA SOCIAL (SEGURANÇA). WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2020. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Engenharia_social_(seguran%C3%A7a)&oldid=58266120>. Acesso em: 15 mai. 2020.

O QUE É PHISHING? UOL Segurança, 2013. Disponível em: <https://seguranca.uol.com.br/antivirus/dicas/curiosidades/o-que-e-phishing.html>. Acesso em: 15 mai. 2020.

REGAN, Joseph. O que é malware? Como malwares funcionam e como se livrar deles. AVG, 2019. Disponível em: <https://www.avg.com/pt/signal/what-is-malware>. Acesso em: 10 mai. 2020.

RODRIGUES, André. Sniffing de rede. Portal GSTI, 2019. Disponível em: <https://www.portalgsti.com.br/2018/11/sniffing-de-rede.html>. Acesso em: 10 mai. 2020.

SERVIDOR. Michaelis online, 15 abr. 2020. Disponível em: <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=servidor>. Acesso em: 15 abr. 2020.

FOROUZAN, Behrouz A. Comunicação de Dados e Redes de Computadores. 4. ed. Porto Alegre: AMGH, 2010.

SQL Injection. Devmedia, 2007. Disponível em: <https://www.devmedia.com.br/sql-injection/6102>. Acesso em: 12 mai. 2020.

SQLMAP. SQLMAP, 2020. Disponível em: <http://sqlmap.org/>. Acesso em: 15 mai. 2020.

KAFRUNI, Simone. Mais da metade das empresas não está pronta para a lei de proteção de dados. Correio Braziliense, 2020. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/economia/2020/02/17/internas_economia,828562/mais-da-metade-das-empresas-nao-esta-pronta-para-lei-de-protecao-de-da.shtml>. Acesso em: 20 jun. 2020.

JINKINGS, Daniella. Governo vai debater criação de marco legal para proteção de dados pessoais no Brasil. REDEBRASILATUAL, 2010. Disponível em: <https://www.redebrasilatual.com.br/cidadania/2010/12/governo-vai-debater-criacao-de-marco-legal-para-protecao-de-dados-pessoais-no-brasil/>. Acesso em: 10 mai. 2020.

TARVARES, Joelmir. Empresa que ajudou Trump roubou dados de 50 milhões de usuários do Facebook. FOLHA DE S.PAULO, 2018. Disponível em: <https://www1.folha.uol.com.br/mundo/2018/03/empresa-que-ajudou-trump-roubou-dados-de-50-milhoes-de-usuarios-do-facebook.shtml>. Acesso em: 05 abr. 2020.

DRZ.global. Diferenças entre LGPD E GDPR. DRZ.global, 20189. Disponível em: <https://www.drz.global/blog/diferencas-entre-a-gdpr-e-a-lgpd>. Acesso em: 15 mai. 2020.

E-COMMERCE Brasil. Na Europa, menos de 30% das empresas estão adequadas à GDPR. E-Commerce Brasil, 2019. Disponível em: <https://www.ecommercebrasil.com.br/noticias/na-europa-menos-de-30-das-empresas-estao-adequadas-a-gdpr/>. Acesso em: 15 mai. de 2020.