INTRODUÇÃO

A crescente interação e aproximação entre os mercados financeiros de diversos países, proporcionadas pela globalização, só se tornou possível graças à tecnologia da informação e às constantes inovações tecnológicas.

As Tecnologias de Informação e Comunicação (TIC), em cujas interfaces computacionais apresentam-se múltiplos instrumentos que interferem nos modos de produção de informação e de conhecimento, tornam homens e máquinas um novo sistema hibridizado pelas suas formas de interação (ARAYA; ELIZABETH, 2010).

Tomando proveito do contexto atual de revolução tecnológica, proporcionado pelas tecnologias de informação e comunicação (TIC), surge o fenômeno da globalização, fenômeno este que proporcionou uma maior interação e aproximação entre os mercados financeiros de diversos países.

Globalização, nome novo para o antigo processo de internacionalização ou de criação do mercado mundial nascido com o próprio capitalismo (GORENDER, 1997).

O cenário atual globalizado proporcionado pelo desenvolvimento tecnológico torna visível a dependência cada vez maior de tecnologia por parte das organizações, que percebem ser impossível atuar em um mundo globalizado, em seus respectivos mercados, sem o uso de ferramentas de tecnologias de informação e comunicação.

Existem diversos motivos pelos quais as organizações começaram a fazer uso de tecnologia, dentre os quais podemos citar: Busca por vantagem competitiva, melhora nos processos, melhora no gerenciamento empresarial, administração, RH, produção, contabilidade, economia de recursos, comunicação, etc.

Segundo WAGNER e HOLLENBECK (2010), a tecnologia de uma organização consiste no conhecimento, nos procedimentos e nos equipamentos de transformação de recursos primários em bens ou serviços acabados.

Neste contexto tecnológico, algo muito importante aqui deve ser lembrado e abordado, que é a questão dos problemas relacionados à segurança da informação.

Abaixo segue uma história de incidente de segurança que ocorreu com a empresa Pfizer:

> Embora muitos aparelhos eletrônicos e aplicações de software possam trazer vantagens para uma empresa - por exemplo, ajudando os funcionários a fazer seu trabalho de forma mais eficiente -, as implicações de segurança são muitas, disse Ken Silva, chefe de segurança da VeriSign, especializada em software de segurança de rede. “Quando acrescentamos essas coisas às redes corporativas, deixamos algumas brechas abertas no ambiente”. A empresa farmacêutica Pfizer descobriu isso da maneira mais difícil. O cônjuge de um funcionário instalou um software de compartilhamento de arquivos em um laptop da Pfizer em casa, criando uma brecha de segurança que parece ter comprometido os nomes e números do Seguro Social de 17 mil funcionários e ex-funcionários da Pfizer, segundo uma carta enviada pela Pfizer aos procuradores-gerais do Estado. A investigação da Pfizer mostrou que 15.700 desses funcionários tiveram de fato seus dados acessados e copiados (BALTZAN; PAIGE, 2016).

Para além do exemplo de vazamento e roubo de dados ocorrido na Pfizer, mencionado por Paige Baltzan em seu livro Tecnologia Orientada para Gestão, tem ocorrido

com cada vez mais frequências situações semelhantes em outras empresas e organizações, sendo um dos mais recentes o caso de roubo de dados que ocorreu com a companhia aérea britânica EasyJet em maio de 2020.

A empresa concordou que sofreu um ataque cibernético avançado e que como consequência de tal evento, teve os dados de mais de 9 milhões de seus clientes foram roubados por hackers. A investigação do ocorrido está sendo conduzida com ajuda do Information Commisioner's Office e do National Cyber Security Center, ambos órgãos do Reino Unido.

Diante do exposto, tem sido cada vez maior a preocupação por parte das empresas com a segurança de suas informações. Essas empresas demandam soluções tecnológicas de segurança, normas e processos que eliminem vulnerabilidades e forneça elevado grau de proteção contra ataques, invasões e espionagem, que acabem por resultar em roubo de dados.

O investimento generoso em TI comprova-se, portanto, como um ponto forte na segurança, pois contribui a evitar vazamentos de dados e informações que acarretariam em perdas de receita e de imagem imensuráveis para a empresa ou organização, sendo que uma companhia que protege bem os seus sistemas e posteriormente os seus dados têm, portanto, maior vantagem competitiva contra aquelas as quais tiveram incidentes de segurança que acarretaram em perdas e vazamentos de dados.

Sobre o emprego da TI como vantagem competitiva em específico, Paige Baltzan (2016) relatou o seguinte:

> "A TI é descrita como um facilitador de vantagem competitiva, eficácia e eficiência organizacional. Como ferramenta competitiva, a TI pode diferenciar os produtos, serviços e preços de uma organização de seus concorrentes, melhorando a qualidade do produto, diminuindo os prazos de desenvolvimento ou fornecimento do produto, criando novos produtos e serviços baseados em TI e melhorando o atendimento ao cliente antes, durante e depois das transações."

Neste contexto de expansão comercial, tecnologia e segurança de informação, surge em 14 de agosto de 2018 a Lei nº 13.709 - Lei geral de Proteção de Dados Pessoais (LGPD) que tem como objetivo regulamentar a questão de tratamento de dados pessoais no Brasil.

De forma similar, ocorreu também na União Europeia (UE) com a GDPR, "*General Data Protection Regulation*", que significa em português, Regulação Geral de Proteção de Dados.

A GDPR passou a ter validade no dia 25 de maio de 2018, e é a legislação vigente referente a matéria de proteção e tratamento de dados, para todos os estados-membros da UE e da EEA (European Economic Área ou Zona Econômica Europeia), da qual fazem parte a Islândia, Liechtenstein, e a Noruega.

O GDPR foi aprovado pelo Parlamento Europeu, com caráter uniformizador e manteve o modelo geral do critério da proteção equivalente da Diretiva 95/46 (VIEIRA, 2019).

A Diretiva Europeia nº 95/46/CE de 24 de outubro de 1995, é uma diretiva que tem por objetivo tratar sobre a proteção de indivíduos, no que diz respeito ao tratamento de seus dados pessoais e à livre circulação de tais dados.

Objetivo

O objetivo deste trabalho é realizar uma revisão sistemática a respeito da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), apresentando um resumo referente as diversas opiniões, críticas e comentários à lei realizados por diversos membros da comunidade acadêmica brasileira. A contribuição de tais autores na discussão sobre a LGPD ocorreu na forma de artigos e trabalhos acadêmicos.

REFERENCIAL TEÓRICO

Antes de entrarmos em detalhes a respeito da LGPD, para melhor entendimento da pesquisa por parte do leitor, precisamos fazer menção a algumas tecnologias e conceitos.

Segurança da Informação

A segurança da informação, do inglês, Information Security, também frequentemente referida de maneira abreviada como InfoSec, refere-se aos processos e ferramentas desenvolvidos e implantados para proteger as informações sensíveis de empresas e organizações de modificação, disrupção, destruição e inspeção.

> "A segurança da informação tornou-se uma necessidade crucial para proteger quase todos os aplicativos de transações de informações. A segurança é considerada como uma importante disciplina científica, cujas complexidades multifacetadas merecem a sinergia das comunidades de ciência da computação e engenharia." (AWAD e FAIRHURST, 2018).

Invasão

Acesso não autorizado a um sistema por meio de exploração de brechas e vulnerabilidades.

Cibersegurança e Segurança da Informação

É comum confundir os dois termos, a segurança da informação é uma parte crucial da cibersegurança, mas, ela se refere exclusivamente aos processos desenvolvidos para a segurança de dados. A cibersegurança é um termo mais geral, que incluí a segurança da informação.

> A cibersegurança é a coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gerenciamento de riscos, ações, treinamento, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético e a organização e os ativos do usuário. Os ativos da organização e do usuário incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade das informações transmitidas e / ou armazenadas no ambiente cibernético. A segurança cibernética se esforça para garantir a obtenção e a manutenção das propriedades de segurança da organização e dos ativos do usuário contra riscos de segurança relevantes no ambiente cibernético (AWAD e FAIRHURST, 2018).

Os objetivos gerais de segurança incluem o seguinte:

- Disponibilidade;
- Integridade, que pode incluir autenticidade e não repúdio;
- Confidencialidade.

Segurança de Aplicação

A segurança de aplicações trata sobre vulnerabilidades de softwares em aplicações web e mobile. Tais vulnerabilidades podem ser encontradas na autenticação ou autorização de usuários, na integridade do código, configurações. Vulnerabilidades em aplicativos podem criar brechas de segurança. A segurança de aplicações é importante componente da segurança da informação.

Segurança em Nuvem

A segurança em nuvem tem como objetivo garantir a segurança das aplicações e serviços hospedados em ambiente web.

A "nuvem" não é um lugar, mas um método de gerenciar os recursos de TI que substitui máquinas locais e data centers privados por uma infraestrutura virtual. Nesse modelo, os usuários acessam recursos virtuais de computação, rede e armazenamento disponibilizados online por um provedor remoto.

Segurança de Infraestrutura

É aplicada ao ambiente aonde estão localizados os dispositivos de hardware, isto é, os servidores (data centers), computadores, dispositivos de rede (roteadores, switches, modems).

Criptografia de Dados

A criptografia de dados é uma maneira de converter os dados de um formato padrão e legível em um formato codificado, em que não é possível ler e entender as informações.

> "A ideia básica por trás da criptografia é aplicar um algoritmo de criptografia nos dados, usando uma chave de criptografia especificada pelo usuário ou pelo administrador do banco de dados. A saída do algoritmo é a versão criptografada dos dados. Também existe um algoritmo de descriptografia, que recebe os dados criptografados e uma chave de descriptografia como entrada e, então, retorna os dados originais. Sem a chave de descriptografia correta, o algoritmo de descriptografia produz lixo. Os algoritmos de criptografia e descriptografia em si são admitidos como publicamente conhecidos, mas uma ou ambas as chaves são secretas." (RAMAKRISHNAN e GEHRKE, 2008).

Blockchain

A tecnologia Blockchain nada mais é do que um livro de razão pública (ou livro contábil) que faz o registro de uma transação de moeda virtual, (a mais popular delas é o Bitcoin), de forma que esse registro seja confiável e imutável. O registro é distribuído em toda a rede de computadores que participa do sistema do bitcoin.

Todas as transferências são processadas e verificadas por milhares de computadores espalhados pelo planeta. Resolvendo complicados cálculos, os computadores que processam o sistema verificam a veracidade das transações (FRABASILE, 2019).

> "As transações não são registradas uma a uma, mas sim em blocos. No bitcoin, um bloco é formado a cada dez minutos, e contém todas as informações de transações feitas durante aqueles dez minutos. Cada bloco é interligado ao bloco seguinte e ao anterior. Isso garante que não seja possível alterar as informações que foram registradas em um bloco passado. Se um computador fizer uma alteração, os demais entendem que aquela alteração não deveria ter sido feita e a descartam." (FRABASILE, 2019).

As transações das moedas virtuais são criptografadas, o que torna difícil saber quem foram as pessoas envolvidas na transação, ao menos que se tenha a chave para descriptografia. A tecnologia também é usada por outras moedas tais como litecoin e ethereum.

Caso AT&T

Ocorreu em janeiro de 2018 com um dos pioneiros no campo das cripto moedas, Michael Terpin, de acordo com Michael Kaplan, editor do portal de notícias americano NYPOST, Terpin estava em seu laptop preparando-se para uma conferência em Las Vegas, então seu telefone vibrou com uma mensagem do google notificando que sua senha havia sido alterada porém Terpin não havia alterado. Temendo que estivesse sendo hackeado, o empreendedor de 62 anos verificou um segundo telefone, um velho Blackberry, para ver se tinha algum problema, o aparelho estava inutilizável, incapaz de ficar online e receber chamadas. Terpin havia sido vítima de um golpe de vanguarda conhecido como troca de SIM. Ladrões inteligentes em tecnologia conseguiram trocar remotamente a identidade digital de Terpin do cartão SIM que controlava seu Blackberry para um cartão SIM em branco em um de seus telefones.

De alguma maneira os hackers conseguiram acessar uma de suas carteiras virtuais e roubar mais de US $ 23,8 milhões de dólares em ativos, acumulados em cerca de dois anos. O ocorrido levou Terpin a entrar na justiça pedindo uma compensação no valor de US $ 224 milhões de dólares contra a empresa AT&T, por fraude e negligência grave, por ter permitido que criminosos fizessem a troca de SIM de seu telefone.

Se o caso estivesse ocorrido no Brasil durante a vigência da LGPD, Terpin provavelmente estaria amparado pela legislação. Pois a AT&T foi negligente, no sentido de ter permitido que uma falha de segurança fosse explorada, o que levou os dados do seu cartão SIM que controlava o seu celular a serem roubados e transferidos para outro dispositivo móvel.

A LGPD, em seu art. 52º, inciso II, prevê, em razão de infrações cometidas às normas previstas na lei, conforme Figura 1 abaixo.

Figura 1 – Sanções administrativas previstas.
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Resposta a Incidentes

A resposta a incidentes consiste em monitorar, investigar e agir com ações contra ataques, invasões e comportamentos maliciosos.

Antes do incidente ocorrer, a equipe de TI da organização deve ter um planejamento claro de como deve agir, na forma de um plano de resposta a incidentes.

Segundo SCHETINA (2002), O maior erro que a maioria das organizações comete quando ocorre resposta a incidentes é não ter uma política e procedimentos de resposta a incidentes predeterminados para auxiliá-las.

Gerenciamento de Vulnerabilidades

O objetivo é procurar por fraquezas e brechas nos sistemas que, se não identificadas, podem acarretar em riscos a serem explorados, riscos estes que após explorados, se tornam em incidentes.

Gestão de vulnerabilidades é o processo de identificação, análise, classificação e tratamento das vulnerabilidades. Esse tratamento consiste na correção das fraquezas, aplicação de controles e minimização de impactos no ambiente (DURBANO, 2019?).

Inteligência Artificial

A inteligência artificial é um ramo de pesquisa da ciência da computação que busca, através de símbolos computacionais, construir mecanismos e/ou dispositivos que simulem a capacidade do ser humano de pensar, resolver problemas, ou seja, de ser inteligente (SILVA, 2018).

> A Inteligência Artificial (IA) como projeto efetivo só se tornou possível após o aparecimento dos computadores modernos, ou seja, após a segunda guerra mundial (de 1945 em diante). Até então havia dificuldades técnicas que precisavam ser superadas para que o projeto dessas máquinas mais modernas pudesse sair do papel (TEIXEIRA, 2019).

Machine Learning

É uma tecnologia que faz parte do universo da inteligência artificial, consiste em alimentar um computador com dados de maneira que a máquina aprenda por conta própria e chegue ao resultado de maneira independente.

> “O machine learning, aprendizado de máquina ou aprendizagem automática, no português, é uma tecnologia que possibilita que os computadores possam agir e decidir sozinhos, baseando-se em dados em vez de seguirem à risca uma programação para realizar uma determinada tarefa. O machine learning se vale do reconhecimento de padrões nos dados com que têm contato e são projetados para aprender e melhorar ao longo do tempo quando expostos a novos dados.” (MATOS, 2017).

Análise de Dados

A análise de dados é a transformação de números em informação, em significado, em solução de problemas (SANTOS, 2016). É utilizada, por exemplo, nas empresas e organizações no auxílio para a tomada de decisões. A análise de dados auxilia as empresas a entender melhor o perfil e o comportamento de seus clientes. Algumas das ferramentas utilizadas na análise de dados são o SAS, R, Python, Tableau, Orange, Matlab.

Big Data

Big data são ativos de informações de alto volume, alta velocidade e / ou alta variedade que exigem formas inovadoras e econômicas de processamento de informações que permitem uma visão aprimorada, tomada de decisão e automação de processos (GARTNER, 2020).

> O Big Data pode ser usado para combater desvios de verbas públicas, facilitar o sequenciamento genético para a descoberta, por exemplo, da cura do câncer e analisar o comportamento dos indivíduos para decifrar seus hábitos de consumo. E ainda: prever tendências de mercado, riscos de investimentos, aumentar a produtividade das empresas (GUIMARÃES, 2017).

Empresas e organizações podem ter uma ampla gama de razões para utilizar de um Big Data, ele pode ser utilizado para desenvolvimento de novos produtos, por exemplo, criando modelos preditivos para novos produtos e serviços, na manutenção de equipamentos industriais, através do armazenamento de dados estruturados (ano de fabricação, fabricante e tipo de equipamento que deu defeito) e não estruturados, (dados de sensores, logs, mensagens de erro), na segurança da informação, através da coleta de dados referentes a tentativas de invasões, na prospeção de novos clientes, através da coleta de dados de redes sociais, páginas mais visitadas, produtos mais pesquisados, e assim por diante. O Big Data é muito versátil e pode ser utilizado com foco em uma ampla gama de atividades e objetivos.

Big Data e Segurança da Informação

Apesar de o Big Data ajudar na coleta de dados para resolução de problemas e melhoramento de processos e serviços, devemos atentar para a necessidade de que o grande volume de dados coletados seja devidamente protegido do uso ilícito e indevido. Os dados massivos coletados não podem ser usados para coagir ou chantagear nenhum indivíduo, e a equipe de TI responsável pela coleta de dados deve estar atenta para isto. O uso incorreto de dados pessoais sensíveis, por exemplo, pode causar consequências desastrosas, e inclusive violar os direitos da personalidade. Nesse sentido, a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) tem como missão importante atuar para proteger os direitos individuais e de personalidade, contra o uso abusivo dos dados por parte das organizações.

Caso Cambridge Analytics

O Escândalo de dados do Facebook-Cambridge Analytica envolve a coleta de informações pessoalmente identificáveis de até 87 milhões de usuários do Facebook que a Cambridge Analytica começou a recolher em 2014 (WIKIPÉDIA, 2018).

Os políticos norte-americanos Ted Cruz e Donald Trump teriam se beneficiado dos dados coletados pela empresa. Os dados também teriam sido utilizados no Reino Unido na campanha a favor do Brexit.

Há um entendimento que nos dois casos a Cambridge Analytica influenciou enormemente os resultados favoráveis de ambas eleições para seus clientes (GOGONI, 2018).

Para uma determinada campanha política, os dados foram detalhados o suficiente para criar um perfil, o qual sugeriu que tipo de propaganda seria mais eficaz para persuadir

uma pessoa em particular em um determinado local para algum evento político (WIKIPÉDIA, 2018).

A companhia mantinha informações de usuários e de seus contatos e manipulava através de propagandas políticas singularizadas e de *fake news* o eleitorado estadunidense (COELHO, 2019).

O caso Cambridge Analytics é um exemplo do uso abusivo, incorreto e indevido de informações pessoais coletadas por ferramentas de Big Data. Dai a importância da devida atenção à preceitos de segurança da informação durante operações de coletas de dados. Neste caso, não houve um vazamento, roubo ou invasão dos bancos de dados em posse da Cambridge Analytics, o que é ainda pior, a empresa coletou e realizou o tratamento dos dados dos usuários da rede social já sabendo que seriam utilizados para finalidade indevida e uso antitético.

Para exemplo da gravidade do assunto, MELLO (2017) faz uso do termo "manipulação da democracia" como título para seu artigo que trata sobre o escândalo protagonizado pela Cambridge Analytics.

Sobre a Lei Geral de Proteção de Dados

A LGPD tem como principal objetivo proteger dados pessoais contra qualquer atividade que acarrete em uso ilícito, indevido ou abusivo por parte dos agentes de tratamento. Possui em seu dispositivo legal regulamentação para a coleta, armazenamento e tratamento de dados pessoais, também prevê sanções, inclusive multa, para quem cometer infração.

É importante ressaltar que a lei exige o consentimento por parte do detentor dos dados pessoais para a coleta e uso dos seus dados, em alguns casos o consentimento é dispensado, como por exemplo, para a coleta de dados manifestados publicamente pelo titular, mais ainda sim são resguardados seus direitos de acordo com os princípios previstos na lei. Embora a dispensa de consentimento possa ocorrer, isso não isenta os agentes de tratamento de dados com as demais obrigações previstas na LGPD, que tratam da observância aos princípios gerais e garantia de direitos.

Histórico

As bases fundamentais para criação da LGPD começam na verdade com a legislação referente ao Marco Civil da Internet (lei nº 12.965/2014), que admitia a proteção de dados pessoais como princípio relativo ao uso da internet e estabelecia em seu artigo 3º, inciso III, a elaboração de lei específica para a proteção de dados, o que só ocorreria posteriormente, em 10 de julho de 2018, data em que a LGPD obteve aprovação.

O surgimento da LGPD se deu a partir do Projeto de Lei da Câmara de nº 53, de 2018, projeto este protocolado pelo Deputado Federal Mílton Monti (PR/SP). A lei foi sancionada em 14 de agosto de 2018 e publicada no Diário Oficial da União em 15 de agosto de 2018.

Domínio de aplicação da legislação

A lei dispõe sobre o tratamento de dados pessoais), por pessoas naturais ou jurídicas, de direito público ou privado, independentemente do país onde estejam localizados os dados ou do país de sua sede, visando a proteção dos seus direitos fundamentais de liberdade, privacidade e desenvolvimento da personalidade.

Realizando uma síntese dos três primeiros artigos, o principal a se observar e destacar é que a lei é bem ampla pois além de aplicar-se a pessoa natural ou jurídica, de direito público ou privado, aplica-se também a dados armazenados fora do país, ressalvadas as seguintes condições a seguir, conforme o art. 3º:

I - A operação de tratamento de dados seja realizada no território nacional;

II - A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

III - Os dados pessoais objetos do tratamento tenham sido coletados no território nacional.

Ademais, pela leitura do art. 1º, depreende-se que a lei também é vigente para casos onde os dados pessoais foram armazenados em meio físico, como por exemplo, formulários, cartões ou fichas de cadastros, e não apenas para dados obtidos e armazenados no meio digital.

Segundo o artigo 4º da LGPD, a lei não possui aplicabilidade quando o tratamento de dados é:

I - Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - Realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os artigos. 7º e 11 desta Lei;

III - Realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequados ao previsto nesta Lei.

Regulamentos de privacidade no mundo

Com o aumento dos negócios on-line, a importância da privacidade e da proteção de dados é cada vez mais reconhecida em âmbito mundial.

Atualmente 132 de 194 países adotaram legislação garantindo a proteção e privacidade de dados, como mostram os dados das Nações Unidas na Figura 2 abaixo:

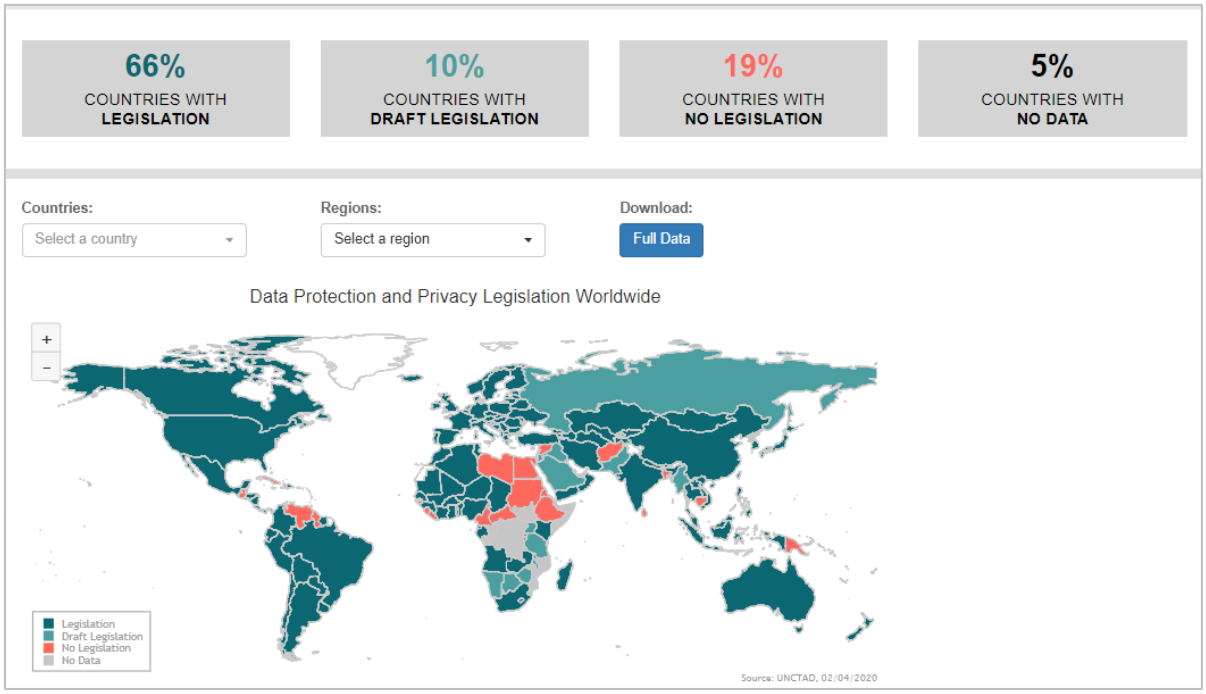

Figura 2 – Países das Nações Unidas com legislação sobre ao dados.
https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Dados pessoais e outras descrições

Os dados pessoais estão classificados em dado pessoal, dado pessoal sensível e dado pessoal anonimizado.

Dado pessoal é toda e qualquer informação que torna possível identificar uma pessoa física e alguns exemplos bem comuns são: RG, CPF, endereço, estado civil, data de nascimento, e-mail, número de telefone, entre outros.

Dados pessoais sensíveis têm caráter mais subjetivo, isto é, estão ligados mais ao íntimo do indivíduo e são aqueles que em caso de exposição indevida tem potencial para causar danos à imagem do titular, e como consequência violar os direitos de personalidade.

Dado anonimizado é um tipo de dado pertencente a uma pessoa física, porém não identificável, graças às técnicas específicas de anonimização de dados.

Exemplo de dado anonimizado: Pesquisa de intenção de voto.

A anonimização é um processo descrito pela LGPD que tem como objetivo desfazer o vínculo entre os dados pessoais coletados e o indivíduo titular original dos dados. É uma maneira de proteger os dados dos indivíduos titulares dos dados contra possíveis usos indevidos e como consequência, proteger a identidade e integridade do titular dos dados.

Contudo, para que os dados sejam verdadeiramente anonimizados e saiam do escopo de proteção da Lei, a anonimização tem de ser irreversível (VIEIRA, 2019).

A Pseudonimização é similar à anonimização, a diferença é que o processo de pseudonimização ainda permite que os dados possam ser associados novamente a uma

pessoa natural, por meio de consulta a informação adicional respectiva mantida separada em outro ambiente, respeitados os requisitos de segurança.

Para melhor entendimento, imagine um banco de dados com uma tabela que contém dados pessoais de um indivíduo, tais como nome, gênero, data de nascimento, nacionalidade, profissão.

Após a pseudonimização os dados que seriam mostrados seriam: gênero, nacionalidade e profissão, sendo impossível identificar a identidade do detentor destes dados a priori, porém, em outro banco de dados, teríamos uma tabela com um número identificador único para cada indivíduo cadastrado, através do qual seria possível associar com os dados registrados, e por fim, identificar novamente a identidade do detentor dos dados.

Banco de Dados: Um banco de dados é uma coleção de dados relacionados. Os dados são fatos que podem ser gravados e que possuem um significado implícito (ELMASRI e NAVATHE, 2005)

Pode estar disponível tanto em meio físico como em meio digital sendo que o conjunto de dados pessoais representa uma informação.

Requisitos e condições necessárias para o tratamento de dados pessoais

Entende-se que Tratamento seja todo tipo de trabalho, ação ou operação realizado em dados pessoais, isto é, a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, modificação, comunicação, transferência, difusão, extração.

O agente responsável pelo tratamento dos dados deve observar os fundamentos necessários para a proteção dos dados pessoais que são: o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Agentes de tratamento de dados pessoais

Agente de tratamento são os controladores e operadores dos dados. O controlador é uma pessoa natural ou jurídica que será responsável pela competência no tratamento dos dados pessoais, isto é, pelos motivos e pela maneira como os dados pessoais deverão ser tratados.

O operador é uma pessoa natural ou jurídica que será responsável pelo tratamento dos dados do titular em nome do controlador e conforme sua determinação.

Para VIEIRA (2019), um dos princípios mais relevantes é o da finalidade, juntamente com o princípio da minimização da coleta.

Por minimização da coleta entende-se que seria coletar apenas a quantidade mínima necessária de dados para a atividade para o qual foram destinados.

Direitos do titular

Os direitos do titular são tratados no art. 18º do capítulo III, o mesmo capítulo dispõe especificamente sobre os direitos do titular.

O titular tem os seguintes direitos em relação ao tratamento de seus dados, os quais pode solicitar ao controlador:

I - Confirmação da existência de tratamento;

II - Acesso aos dados;

III - Correção de dados incompletos, inexatos ou desatualizados;

IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei;

V - Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

VI - Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

O acesso a todos estes direitos por parte do indivíduo proprietário dos dados certamente constitui um grande ponto forte para a LGPD em matéria de liberdade, o que possibilita ao detentor dos dados mais poder efetivo em relação à destinação e o futuro de seus dados. Se o titular se sentir inseguro pode a qualquer momento, mediante requerimento ou de representante legalmente constituído, comunicar ao controlador e solicitar, por exemplo, a eliminação de seus dados.

Os parágrafos 1º e 2º asseguram que o titular pode a qualquer momento peticionar em relação aos seus dados contra o controlador perante autoridade nacional e opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na lei, respectivamente.

A autoridade nacional de proteção de dados é o órgão com atribuições relacionadas à proteção de dados pessoais e à privacidade e que será responsável pela fiscalização do cumprimento da lei.

Responsabilidade e Ressarcimento de Danos

A lei exige que o tratamento de dados realizado pelo agente de tratamento seja feito com responsabilidade, e caso ocorra infração, prevê sanção e multa ao controlador ou operador que causar dano patrimonial, moral, individual ou coletivo ao titular dos dados devido a não cumprimento dos parâmetros previstos pela legislação.

Por outro lado, em seu art. 43. define os casos para os quais os agentes de tratamento não serão responsabilizados: Quando os agentes provam que não realizaram o tratamento de

dados pessoais que lhes foi atribuído, ou que embora tenham realizado tratamento não houve violação à legislação, ou que o dano ocasionado foi de culpa exclusiva do titular dos dados ou de terceiros.

METODOLOGIA

O presente estudo foi desenvolvido através de uma pesquisa de abordagem qualitativa e de natureza básica, em que foram reunidas e apresentadas informações e conceitos relacionados à segurança da informação e demonstrado a sua importância para as empresas, organizações e a sociedade em geral, bem como realizar a correlação entre a segurança da informação e suas tecnologias e a nova legislação brasileira sobre proteção de dados pessoais.

A pesquisa foi feita com a finalidade de desenvolver uma revisão sistemática sobre a nova lei geral de proteção de dados pessoais (LGPD) e teve por objetivo não apenas coletar e reunir as informações correntes na comunidade científica a respeito da LGPD, mas também mostrar a importância do investimento e de legislação relativa a segurança da informação, através dos casos relatados em que ocorreram vazamentos de dados e perdas monetárias e de imagem significativas.

A Revisão Sistemática é um tipo de pesquisa em que é feito uma investigação a respeito de estudos relevantes realizados sobre determinado assunto na literatura da comunidade científica e acadêmica, sendo os resultados obtidos revistos e comentados de forma crítica e abrangente pelo pesquisador.

Para a coleta e levantamento das informações, foi realizado uma pesquisa exploratória com procedimento bibliográfico, em que foram consultados livros relacionados a tecnologia da informação, através da ferramenta google livros e da biblioteca de livros Kindle da Amazon, artigos acadêmicos e científicos pesquisados no Google Scholar, na revista jurídica - Uni Curitiba e no portal de periódicos EBSCO, utilizando as palavras-chave Lei Geral de Proteção de Dados Pessoais, Tecnologia da Informação, Segurança da Informação.

> "A pesquisa bibliográfica, ou de fontes secundárias, abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico etc., até meios de comunicação orais: rádio, gravações em fita magnética e audiovisuais: filmes e televisão. Sua finalidade é colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto, inclusive conferências seguidas de debates que tenham sido transcritos por alguma forma, querem publicadas, quer gravadas." (MARCONI e LAKATOS, 2003).

ANÁLISE DOS RESULTADOS

Através da pesquisa bibliográfica foi possível localizar e identificar uma série de artigos e trabalhos acadêmicos em que os temas centrais destes trabalhos eram relacionados pelos autores com a LGPD que são: transferência internacional de dados, autonomia privada, ciberespaço, ambiente online, o tratamento de dados pessoais sensíveis e os limites do estado, direitos da personalidade, direito empresarial, transparência de dados.

Gunther (2020) realizou um profundo questionamento em relação à necessidade de absoluta seriedade na aplicação da LGPD, para sustentar seu pensamento, utiliza como

exemplo o fato ocorrido na prefeitura de São Paulo em 2016, que envolveu o vazamento de dados pessoais de usuários do SUS através do aplicativo e-Saúde.

Júnior e Faustino (2019), comentam a necessidade de confiabilidade e credibilidade na aplicação de uma lei que regulamente o tratamento de dados, especialmente em relação a aplicativos de Saúde (e-Saúde). Os autores dão ênfase em discutir sobre os aplicativos relacionados a área de Saúde, e como tais aplicativos tratam com dados sensíveis dos usuários.

Segundo Júnior e Faustino (2019), embora os aplicativos sejam oferecidos no Brasil e o usuário, em sua grande maioria, seja brasileiro, os termos de uso e políticas de privacidade são todos escritos em inglês, dificultando, mais ainda, a compreensão dos termos utilizados, bem como a possibilidade da manifestação do consentimento dos usuários em relação à forma que seus dados pessoais serão tratados pelo proprietário desses aplicativos, o que evidencia, mais uma vez, um grande risco e possibilidade de lesão a uma quantidade muito grande de pessoas.

Frazão (2018), mencionou a preocupação da LGPD com a anonimização de dados, a autora do artigo procurou mostrar as fragilidades da lei, por exemplo, em sua análise pessoal, especialmente em relação ao inciso IX do art. 7º, este possui conceitos vagos e ambíguos.

> Todavia, no inciso IX do art. 7º, a LGPD prevê uma das mais controversas hipóteses de tratamento de dados: necessidade de atendimento de interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (FRAZÃO, 2018).

Segundo Frazão (2018), o problema é que: “a lei não prevê a prevalência prioritária dos direitos dos titulares de dados, mas somente daqueles em relação aos quais a situação concreta exigir a proteção”.

Mezzaroba et col. (2019), os autores procuram realizar uma correlação entre a Lei Geral de Proteção de Dados (LGPD) com o Direito Empresarial, bem como uma análise sobre os possíveis impactos e consequências econômicas nas empresas ocasionados pela legislação.

Segundo Mezzaroba et col. (2019), a Lei Geral de Proteção de Dados traz em seu arcabouço legal uma série de consequências para os agentes que lhes estão sujeitos, especificamente para as empresas, sendo indicadas séries de peculiaridades que envolvem a reestruturação de rotinas, de procedimentos, bem como treinamento de colaboradores, efetivações de novas contratações de pessoas, serviços e novas aquisições de equipamentos.

Para os autores Silva e Melo (2019), a LGPD constitui um instrumento de concretização da autonomia privada, pois permite que o indivíduo possa consentir quanto ao fornecimento de seus dados pessoais.

O indivíduo passa a ser titular de um direito ao consentimento quanto à circulação de seus dados pessoais, reconhecendo-se ser uma violação à dignidade da pessoa humana a utilização de suas informações pessoais sem a sua anuência, em atenção à autonomia privada (SILVA e MELO, 2019).

Agostinelli (2018), teve por objetivo discorrer sobre a importância de uma legislação específica que tratasse a respeito de armazenamento e proteção de dados pessoais na internet,

nomeadamente a Lei Geral de Proteção de Dados Pessoais (LGPD) bem como mostrar os benefícios decorrentes da respectiva lei para empresas e consumidores.

Vieira (2019) procurou comentar a relação entre a LGPD e a transferência internacional de dados, ressaltando que a LGPD proporcionou avanços através de uma legislação específica que tratasse sobre o tema, o que abre a possibilidade para que o Brasil se torne um país destinatário de dados pessoais internacionais.

Carvalho et col. (2019), comentou diversos artigos da legislação, levantando, para cada artigo da LGPD, questões importantes que levam a possíveis desafios relacionados à transparência organizacional, interna, social e externa, e como que as organizações que realizam o tratamento dos dados poderão lidar com tais desafios.

Costa (2018) defende a definição de proteção de dados pessoais como novo direito de personalidade, com o objetivo de proteger os titulares dos dados de abusos por partes de plataformas e provedores. Discorre sobre direito à privacidade, à autodeterminação informativa, e o princípio de proteção da dignidade dos seres humanos.

Coelho (2019), assim como Costa (2018), trataram também de comentar sobre direitos de personalidade, e sobre a evolução dos direitos de personalidade, isto é, a intimidade, a vida privada, o sigilo, a honra, a imagem, e relaciona a proteção de tais direitos com a LGPD, uma vez que a legislação tem como objetivo proteger dados pessoais, principalmente dados pessoais sensíveis, que se comprometidos, podem prejudicar gravemente a imagem e a vida social do indivíduo titular.

CONCLUSÃO

A pesquisa permitiu levantar uma série de questões a respeito da grande importância financeira que a coleta de dados pessoais representa atualmente, e como as vezes o lucro para algumas empresas e organizações está acima da ética, do respeito aos direitos individuais e do bom senso, como pode ser observado com o episódio ocorrido com o Facebook e a Cambridge Analytics.

A criação de uma legislação para coibir e reprimir abusos específicos relacionados ao uso de dados pessoais é de fato um grande avanço, uma vez que a LGPD prevê em seu dispositivo sanção na forma de multa para o agente de tratamento que cause danos ao titular dos dados.

A LGPD pode atuar no sentido de evitar ou ao menos minimizar escândalos que envolvam o uso abusivo de dados pessoais ou vazamento de dados, mas para isso, é necessário que a lei seja aplicada com absoluta seriedade e que haja fiscalização por parte da Autoridade Nacional de Proteção de Dados (ANPD).

A Liberdade, a privacidade, os direitos individuais e de personalidade devem ser protegidos e garantidos, e essa é a proposta da LGDP, proteger o indivíduo e assegurar os seus direitos.

REFERÊNCIAS BIBLIOGRÁFICAS

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014.

(Marco Civil da Internet). Presidência da República, Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 abril de 2020.

ARAYA, Elizabeth Roxana Mass; VIDOTTI, Silvana Aparecida Borsetti Gregorio. **Criação, proteção e uso legal de informação em ambientes da world wide web.** São Paulo: Cultura Acadêmica; UNESP, 2010.

GORENDER, Jacob. **Globalização, tecnologia e relações de trabalho**. Estud. av., São Paulo, v. 11, n. 29, p. 311-361, abr. 1997. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40141997000100017&lng=pt&nrm=iso>. Acesso em: 25 abril de 2020.

WAGNER III, John A.; HOLLENBECK, John R. **Comportamento organizacional - criando vantagem competitiva.** 3. ed. São Paulo: Saraiva, 2012.

BALTZAN, Paige. **Tecnologia orientada para gestão.** 6. ed. Porto Alegre: AMGH, 2016.

AWAD, Ali Ismail.; FAIRHURST, Michael. **Segurança da informação:** fundamentos, tecnologias e aplicações. Londres, Reino Unido: Instituto de Engenharia e Tecnologia, 2018.

RAMAKRISHNAN, Raghu; GEHRKE, Johannes. **Sistemas de gerenciamento de banco de dados.** 3. ed. São Paulo: McGraw-Hill, 2008.

SCHETINA, Erik; GREEN, Ken; CARLSON, Jacob. **Aprenda a desenvolver e construir sites seguros.** Rio de Janeiro: Campus, 2002.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

GARTNER glossary. Big Data. Gartner, c2020. Disponível em:<https://www.gartner.com/en/information-technology/glossary/big-data/>. Acesso em: 15 junho de 2020.

FRABASILE, Daniela. **Blockchain: o que é e como funciona**. Época Negócios, 2019. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2019/04/blockchain-o-que-e-e-como-funciona.html>. Acesso em: 22 junho de 2020.

DURBANO, Vinicius. **Gestão de Vulnerabilidades:** 8 passos para proteger o seu negócio. Ecoit, 2019.Disponível em: <https://ecoit.com.br/gestao-de-vulnerabilidades/>. Acesso em 16 junho de 2020.

TEIXEIRA, João. **O que é inteligência artificial.** 3. Ed. São Paulo: e-galáxia, 2019.

MATOS, David. **Conceitos Fundamentais de Machine Learning**. Cienciaedados, 2017. Disponível em:<http://www.cienciaedados.com/conceitos-fundamentais-de-machine-learning/>. Acesso em: junho de 2020.

SANTOS, Virgílio F. M. **O que é Análise de Dados? Como estruturar a sua?** FM2S, 2016. Disponível em:<https://www.fm2s.com.br/analise-de-dados-como-estruturar/>. Acesso em: 18 junho de 2020.

GUIMARÃES, Leandro. **Como o BigData beneficia a segurança da informação?** Knowsolution, 2017. Disponível em:<https://www.knowsolution.com.br/como-o-big-data-beneficia-a-seguranca-da-informacao/#close>. Acesso em: 18 junho de 2020.

WIKIPÉDIA**. Escândalo de dados Facebook-Cambridge Analytica.** Wikipédia, 2020. Disponível em: <https://pt.wikipedia.org/wiki/Escândalo_de_dados_Facebook-Cambridge_Analytica>. Acesso em:14 maio de 2020.

GOGONI, Reinaldo. **O maior roubo de dados da história do facebook que ajudou a eleger Donald Trump.** Meiobit, 2018. Disponível em: <https://meiobit.com/381701/facebook-cambridge-analytica-roubo-dados-ajudou-campanha-donald-trump-e-brexit/>. Acesso em: 14 maio de 2020.

MELLO, João. **A manipulação da democracia através do Big Data.** Jornalggn, 2017. Disponível em:<https://jornalggn.com.br/analise/a-manipulacao-da-democracia-atraves-do-big-data-por-hannes-grassegger-e-mikael-krogerus/>Acesso em: 14 maio de 2020.

ELMASRI, Ramez.; SHAMKANT B., Navathe. **Sistemas de banco de dados.** 4. ed. São Paulo: Pearson Addison Wesley, 2005.

GUNTHER, Luiz Eduardo; COMAR, Rodrigo Thomazinho; RODRIGUES, Luciano Ehlke. **A proteção e o tratamento dos dados pessoais sensíveis na era digital e o direito à privacidade:** os limites da intervenção do estado. Revista Jurídica vol. 02, nº. 27, Curitiba, 2020. p. 25 - 41. DOI: 10.21902. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/3972>. Acesso em junho de 2020.

BARRETO JUNIOR, Irineu Francisco; FAUSTINO, André. **Aplicativos de serviços de saúde e proteção dos dados pessoais dos usuários**. Revista Jurídica vol. 01, n°. 54, Curitiba, 2019. p. 292 - 316. DOI: 10.6084. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3311/371371803>. Acesso em 17 junho de 2020.

FRAZÃO, Ana. **Nova LGPD:** as demais hipóteses de tratamento de dados pessoais. Jota.info, 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa- Acesso em 19 junho 2020.

MEZZAROBA, Orides; LUPI, André Lipp Pinto Bastos; DASSAN, Lucas Amaral. **Lei geral de proteção de dados:** impactos normativos no direito empresarial. Revista de Relações Internacionais Vol. 02, nº. 23, Curitiba, 2019. p. 272 - 288. DOI:10.21902. Disponível em:<http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/3899/371372231>. Acesso em: junho de 2020.

SILVA, Lucas Gonçalves; MELO, Bricio Luís da Anunciação. **A lei geral de proteção de dados como instrumento de concretização da autonomia privada em um mundo cada vez mais tecnológico**. Revista Jurídica Uni Curitiba. Vol. 03, n°. 56, Curitiba, 2019. pp. 354 - 377

AGOSTINELLI, Joice. **A importância da lei geral de proteção de dados pessoais no ambiente online**. Etic-encontro de iniciação científica ISSN 21-76-8498, v. 14, n. 14, 2018.

VIEIRA, V. R. N. Lei Geral de Proteção de Dados: **Uma análise da tutela dos dados pessoais em casos de transferência internacional.** 2019. 77 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Uberlândia, 2019.

CARVALHO, Luiz et al. **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.

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. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018.

COELHO, Amanda Carmen Bezerra Coelho. **A lei geral de proteção de dados pessoais brasileira como meio de efetivação dos direitos da personalidade**. 2019. 53 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal da Paraíba, João Pessoa, 2019.