

Uma análise da Lei Geral de Proteção de Dados e seus reflexos

Reginaldo Lourenço dos Santos^{1*} Aroldo Bueno de Oliveira²

¹ Acadêmico do 10º período do curso de Direito no Centro Universitário São Lucas Ji-Paraná (UniSL), Ji-Paraná, RO, Brasil. E-mail: E-mail reginaldo-lourenco@hotmail.com

² Professor orientador, Mestre em Direito pela Universidade de Marília UNIMAR (2012), Especialista em Direito Ambiental pela Universidade Federal do Paraná – UFPR (2020), Especialista em Controladoria e Gestão Financeira pela Faculdade Paranaense – FACCAR, Bel. em Economia pela Universidade Estadual de Londrina - UEL (1995) e Bel, em Direito pela UMPAR (2009). E-mail: aroldobueno_adv@yahoo.com.br .

***Autor Correspondente:** Reginaldo Lourenço dos Santos - Acadêmico do 10º período do curso de Direito no Centro Universitário São Lucas Ji-Paraná (UniSL), Ji-Paraná, RO, Brasil. Rua Aluizio Ferreira nº 664, bairro Urupa. Tel (69) 99975-9700. E-mail reginaldo-lourenco@hotmail.com

Recebido: 31/05/2022 - **Aceito:** 07/07/2022.

Resumo

Com o avanço da tecnologia, todas as informações e tudo que precisamos ficaram acessíveis por meio da internet com a facilidade de adquirirmos ou obtermos a informação através de um clique. Estudar, ler, comprar, publicar artigos e ideias, buscar informações que antes eram consideradas “lixos” podem se tornar valiosíssimas. Nesse sentido, tão valiosas que para processá-las e armazená-las, os administradores desses dados são considerados um marco histórico e ficou conhecida como a “Big Data”. O valor destes dados está relacionado, a princípio com o marketing, o capitalismo, saber o que oferecer aos clientes antes mesmo deles pedirem. Por outro lado, tantos dados armazenados chamaram atenção de pessoas má intencionada e devido seu valor, passaram até mesmo a ser roubadas. Desta forma, o objetivo deste artigo é identificar a necessidade de regulamentação do tema, identificando os motivos que levaram a estas violações de privacidade, conceituando o “Big data” e as consequências destas violações para as microempresas apresentando soluções. O estudo se deu por meio da pesquisa exploratória através da pesquisa bibliográfica e por meio do método qualitativo. A Lei de Proteção de Dados é promulgada no sentido de estabelecer parâmetros, cuidados, e punições a quem fizer mau uso ou ainda deixar vulnerável as informações dos seus clientes. Assim, esta pesquisa abordará alguns impactos causados por essa “nova era” digital e por meio deles justificar a criação e a necessidade da implantação urgente da LGPD (Lei Geral da Proteção de Dados), bem como seu estudo.

Palavras-chave: LGPD. Big data. Dados.

Abstract

With the advancement of technology, all information and everything we need became accessible through the internet with the ease of acquiring or obtaining information through a click. Studying, reading, buying, publishing articles and ideas, searching for information that was previously considered “junk” can become extremely valuable. In this sense, so valuable that to process and store them, the administrators of this data are considered a historical landmark and became known as the “Big Data”. The value of this data is related, in principle, with marketing, capitalism, knowing what to offer to customers before they even ask. On the other hand, so much stored data caught the attention of malicious people and due to their value, they even started to be stolen. In this way, the objective of this article is to identify the need for regulation of the subject, identifying the reasons that led to these privacy violations, conceptualizing the “Big data” and the consequences of these violations for micro-enterprises, presenting solutions. The study took place through exploratory research through bibliographic research and through the qualitative method. The Data Protection Law is enacted in order to establish parameters, precautions, and punishments for those who misuse or even leave their customers' information vulnerable. Thus, this research will address some impacts caused by this digital “new era” and through them justify the creation and the need for the urgent implementation of the LGPD (General Data Protection Law), as well as its study.

Keywords: LGPD. Big data. Data.

1. Introdução

O mundo está cada vez mais digital, pois através da internet podem-se ouvir músicas, estudar, assistir filmes, jogar jogos

online, fazer compras e por isso as empresas querem informações, dados pessoais dos usuários e para isso utilizam-se de técnicas para melhor conhecer seus perfis.

As empresas querem identificar o porquê o cliente desistiu da compra, seu número de acessos naquele site, quais os critérios que utilizou para efetuar a compra e tantas outras indagações que possam lhes proporcionar uma vantagem na competição capitalista.

Para isso foi necessário o desenvolvimento da tecnologia e técnica para atingir o processamento de dados em tempo real, com velocidade, volume e variedade e esta técnica chama-se “Big Data” e constitui-se em um marco histórico em relação ao manuseio de dados pessoais.

Esse estudo tem por objetivo analisar a união e o avanço do direito e da tecnologia identificando as vantagens e dificuldades presentes nesta relação, bem como a necessidade destas regulamentações.

Nesse sentido, analisa-se o tema desta pesquisa, sendo o propósito desta pesquisa é compreender sua relação com a proteção de dados e as relações comerciais brasileiras.

2. Metodologia

Essa pesquisa foi desenvolvida através da pesquisa bibliográfica, por meio de método qualitativo realizando pesquisas nas mais diversas fontes, dentre elas artigos científicos, notícias, relatórios e documentos diversos em língua portuguesa e inglesa, sendo de abordagem qualitativa.

A pesquisa buscou conceituar o “Big Data” contextualizando com o avanço das tecnologias e mensurar a gravidade dos vazamentos de dados pessoais tanto para as pessoas como para as empresas.

Foi analisada a legislação de outros países em relação ao tema em um processo comparativo e realizada uma breve abordagem da nova Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais.

O estudo utilizou-se da pesquisa bibliográfica e por meio do método qualitativo realizou a seleção de artigos científicos, notícias e a própria legislação, além do posicionamento de seus autores sobre o tema, utilizando textos tanto da língua portuguesa quanto da língua inglesa e optou em excluir artigos e notícias repetitivas e de fontes que não tivessem credibilidade primando ainda pelas obras científicas.

3. Resultados e Discussões

3.1 Conceituando o “Big Data”

O “Big Data” tem seu nome em inglês e é usado para coletar e processar grandes quantidades de dados e informações que são produzidas no mundo digital. Veja-se a definição trazida pelo analista Rodrigo Valinor (2021. p.2):

As empresas que desejam se manter competitivas no mercado e se destacar precisam acompanhar os movimentos gerados pela transformação digital. Isso permite oferecer soluções mais adequadas ao público, além de obter diversas oportunidades de otimização na gestão e no planejamento estratégico.

Entre as possibilidades, vale destacar o Big Data. Ele tem relação com o volume de informações que as empresas podem acessar diariamente — que, se usadas corretamente, podem trazer diversos benefícios para o negócio.

O volume de dados a ser armazenado e processado só se concretizou com a confluência de alguns fatores como o preço para armazenar dados que diminuiu, além do desenvolvimento da tecnologia em armazenar grandes quantidades.

O analista André Petry (2013, p.2. Disponível em: **Erro! A referência de hiperlink não é válida.** Acesso em: 23/03/2022) assim explica:

A era do Big Data só se materializou com a confluência de alguns fatores. Caiu o custo de armazenar dados. Há duas décadas, estocar 1 gigabyte saía por 1000

dólares. Hoje, custa 6 centavos. Os processadores tornaram-se velozes, os programas ficaram mais inteligentes e a quantidade de dados cresce exponencialmente. Tudo isso junto é o berço do Big Data.

A evolução dessas tecnologias permitindo processar tantos dados e captar tantas informações sobre as pessoas levaram a vazamentos de dados e com a informatização de todos os setores somada à posse de informações pessoais, criminosos conseguem criar perfis falsos que os possibilitam aplicar golpes. Desta forma surge a necessidade do direito intervir na tecnologia, de modo a garantir a proteção de dados dos usuários. Um caso que demonstra isso é a situação ocorrida nos Estados Unidos em uma das lojas da Target, onde após coletar informações dos clientes e traçar perfis, um senhor entrou em uma das lojas para reclamar que sua filha recebera um cupom de descontos para produtos de bebê.

Restou ao gerente conferir os cupons e pedir desculpas por entender tratar-se de um erro de sistema, entretanto dias depois o pai descobriu que a sua filha estava grávida. (RODRIGUES e SANTOS. 2013. Disponível em: Acesso em: 23/03/2022).

Observa-se que o caso concreto demonstra as consequências desta violação de privacidade, embora existam consequências piores que estas, pois a cada dia surgem novas formas de fraudes utilizando-se destes dados.

3.2 O marco histórico: Big Data

Ainda sobre o “Big Data” além de ser definido como conjunto de técnicas que analisam uma grande quantidade de dados vale dizer que outras ferramentas não teriam a capacidade de processar estes dados e ainda que reduzisse as informações não teriam a capacidade de colher informações útil.

Entretanto, os dados gerados ficam registrados e armazenados e sem os devidos

cuidados podem ser invadidos por criminosos cibernéticos, pois o sistema embora seja superdesenvolvido não é capaz de evitar as vulnerabilidades apresentadas pelos sites e sistemas das empresas.

Nem mesmos os bancos estão imunes aos ataques. Veja-se a matéria trazida pelo jornalista Cássio Gusson (2021, p.1):

Dados de mais de 10 mil clientes de instituições financeiras do Brasil estão sendo vendidos na DeepWeb, por Bitcoin, em um novo vazamento de dados que comprometeu a empresa brasileira Prisma Promotora, que presta serviço, entre outros para a BV e Banco Safra.

O vazamento foi compartilhado com o Cointelegraph pela equipe de pesquisa da vpnMentor.

A empresa de segurança destacou que uma conta de armazenamento em nuvem conectada ao software foi deixada sem segurança e acessível publicamente pelo proprietário do software.

- Hacker invade canal de cursos de criptomoedas e acusa 'especialista' de fraude

Isso comprometeu as informações privadas de 10.000 pessoas conectadas à Prisma Promotora, expondo-as a fraudes e outros perigos.

Os ataques atingem diversas áreas até mesmo grandes redes sociais como Facebook estão sujeitas aos ataques. Segundo Alex Hern (2019). Disponível em: <https://www.theguardian.com/technology/2019/jan/17/breached-data-largest-collection-ever-seen-email-password-hacking>. Acesso em: 14/03/2022) só no ano de 2019 cerca de 540 milhões de usuários da rede tiveram seus dados vazados, em 2016 uma média de 164 milhões das contas LinkedIn e 360 milhões das contas MySpace em 2008.

Conforme aponta as estatísticas nem mesmo os Bancos que investem alto na proteção e segurança dos dados de seus clientes conseguem escapar destas ameaças. Cita-se a exemplo o Banco Inter que teria vazado informações de cerca de 20 mil

clientes (HIGA, 2018. Disponível em: <https://tecnoblog.net/noticias/2018/07/31/banco-inter-vazou-dados-correntistas-acao-mp/>. Acesso em: 15/03/2022) e poderá ter que arcar com mais de 10 milhões em indenizações.

Através desses dados pode-se observar que empresas com altas tecnologias com equipes preparadas e especializadas no intuito de proteger suas infraestruturas, mesmo assim, não escapam de sofrer falhas de segurança.

São muitos e variados os dados que são roubados pelos hackers para serem utilizados em suas fraudes, indo desde nomes completos até senhas decifradas e dados de pagamentos, clonagem de cartões etc., sendo que por mais que exista a preocupação em proteger estes dados continua fazendo mais vítimas a cada dia.

3.3 A necessidade da criação de leis

Após conseguir acesso à base de dados de uma empresa, os criminosos cibernéticos procuram comercializar esses dados para obter lucros. Como essa ação é ilegal, eles tomam todos os cuidados para manter o anonimato e vendem a base de dados em meios que não são monitorados por indexadores de busca. A chamada Dark Web. Sobre este tema, Letícia Loubak (2019, p.1) explica:

A dark web, pequena fatia da Internet ainda mais sigilosa e obscura que a [deep web](#), não se limita ao comércio de itens ilegais como drogas e armas. Com mercados especializados em venda de dados pessoais, a Internet sombria é popular entre hackers e ciber criminosos, que [se aproveitam de informações e arquivos obtidos por meio de vazamentos](#) para lucrar a partir de golpes.

Paulo Alves (2019, p.1) alerta:

Mais 127 milhões de senhas de oito sites surgiram à venda no Dream Market, um mercado de produtos ilegais que funciona na dark web. A descoberta foi feita pelo site britânico The Register, na última quinta-feira (14), que relatou que pacote completo de informações roubadas podia ser obtido pelo equivalente a R\$ 54 mil em Bitcoin..

Em países como os Estados Unidos, embora não exista uma Lei de Proteção de Dados não significa que não existe regulamentação conforme explica o Blog de educação:

Embora os EUA não possuam uma lei geral de proteção de dados, como a GDPR na Europa e a LGPD no Brasil, isto não significa que não existam leis sobre o assunto no país. Muito pelo contrário. Elas existem, mas são várias leis promulgadas em níveis federal e estadual.(GATEFY (2021, p.1. Disponível em <https://gatefy.com/pt-br/blog/como-funcionam-leis-protecao-dados-estados-unidos>. Acesso em 23 de fev.2022)

O cenário alarmante, fez com que os governos começassem a criar leis para definir os direitos de privacidade dos dados dos usuários e punições explícitas para as situações em que as regulamentações não forem seguidas.

Observa-se a exemplo sobre Leis em relação a este tema cita-se a União Europeia e o Brasil que criaram a General Data Protection Regulation 2016/679 (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD), respectivamente.

O Brasil estava atrás de outros países na América Latina, a Argentina, por exemplo, o assunto foi regulado em 2000 e aplica-se tanto a base de dados pública como a base de dados privada.

O repórter Jonas Valente (2018, p.2) explica:

O tratamento está condicionado ao consentimento do titular, que deve ser livre, expresso e informado. Essa autorização não é exigida nos casos de bases públicas, no cumprimento de uma

obrigação legal, no exercício de funções próprias do Estado e quando as informações se limitam a nome, identidade, profissão, data de nascimento e endereço.

Sobre a importância do tema, Gabriela Tristão et.al. (2021, p.7) explicam:

No atual mundo big data, em que massivo volume de dados pessoais estão em posse de empresas, tornou-se vital a proteção da privacidade dos indivíduos. Neste cenário, foi editada a Lei Geral de Proteção de Dados, inspirada pelo Regulamento Geral sobre Proteção de Dados (RGPD) a legislação busca regular o tratamento de dados, inclusive em meios digitais que venha ser realizado em território nacional. Com isso empresas precisarão de mecanismos de Segurança da informação aptas a proteger acessos não autorizados e o sigilo de informações.

Embora o Brasil tenha largado atrás sobre o tema foi aprovada a Lei nº 13.709/2018, sendo promulgada com objetivo de proteger os dados pessoais das pessoas, afinal trata-se de um direito fundamental de liberdade e de privacidade conforme a própria Lei explica.

3.4 A Lei 13.709/2018 (LGPD)

A lei 13.709/2018 conhecida pela sigla “LGPD” é o resultado do clamor social diante de inúmeras fraudes e constrangimentos sofridos, além de acumuláveis prejuízos financeiros em razão dos vazamentos de dados pessoais.

A referida lei é considerada um marco histórico sobre o tema e tem por objetivo regulamentar o tratamento dos dados pessoais no Brasil, sejam este armazenamento físico ou principalmente aqueles armazenados nas plataformas digitais.

Sobre a lei o site do Governo Federal publicou a seguinte matéria:

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais. (BRASIL, 2021, p.1. Disponível em <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd>. Acesso em 28 fev. 2022).

Sobre a importância da nova legislação o Superior Tribunal de Justiça (2020, p.3. Disponível em: Acesso em: 22 jan. 2022), assim explicou:

A lei representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataformas digitais. Além de mudar a maneira como instituições privadas coletam, armazenam e disponibilizam informações de usuários, a LGPD é destinada às instituições públicas – portanto, deve ser seguida por União, estados, Distrito Federal e municípios.

O Conselho Nacional de Justiça editou a Recomendação 73/2020, com intuito de orientar os órgãos do Poder Judiciário a buscar soluções para aplicar as determinações da nova Lei, de maneira a se adequar, considerando que o dispositivo trouxe algumas alterações significativas.

O artigo 1º da Recomendação 73/2020 do Conselho Nacional de Justiça diz:

Art.1º- Recomendar a todos os órgãos do Poder Judiciário brasileiro, à exceção do Supremo Tribunal Federal, a adoção das seguintes medidas destinadas a instituir um padrão nacional de proteção de dados pessoais existentes nas suas bases:

I – elaborar plano de ação que contemple, no mínimo, os seguintes tópicos:

- a) organização e comunicação;
 - b) direitos do titular;
 - c) gestão de consentimento;
 - d) retenção de dados e cópia de segurança;
 - e) contratos;
 - f) plano de respostas a incidentes de segurança com dados pessoais;
- II – disponibilizar, nos sítios eletrônicos, de forma ostensiva e de fácil acesso aos usuários:
- a) informações básicas sobre a aplicação da Lei Geral de Proteção de Dados aos tribunais, incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores e os direitos dos titulares;
 - b) formulário para exercício de direitos dos titulares de dados pessoais;
- III – elaborar ou adequar, bem com publicar nos respectivos sítios eletrônicos, de forma ostensiva e de fácil acesso aos usuários:
[...]
- IV – constituir Grupo de Trabalho para estudo e identificação das medidas necessárias à implementação da Lei Geral de Proteção de Dados no âmbito do respectivo tribunal, cujo relatório final subsidiará o Conselho Nacional de Justiça na elaboração de uma política nacional. (BRASIL, 2020, p.2).

Observa-se que são diversas as medidas que deverão ser adotadas no âmbito de todo o Poder Judiciário demonstrando a preocupação da entidade em adequar-se a nova legislação devido a sua importância.

A nova Lei Geral de Proteção de Dados Pessoais apresenta alguns aspectos que privilegiam o titular das informações armazenadas, garantindo-lhe o direito ao acesso de maneira facilitada devendo ser disponibilizadas de forma clara e adequada.

A lei criou os agentes de tratamento trazendo duas figuras importantes, o controlador de dados que será uma pessoa natural ou jurídica, tanto faz se de direito público ou privado e terá por competência tomar as decisões referentes ao tratamento de dados pessoais e indicar o encarregado pelo tratamento de dados pessoais.

O encarregado é o outro agente de tratamento trazido pela lei e será a pessoa responsável em estabelecer a comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados ANPD.

A Lei encontra-se em vigência e já motivou diversas ações, entre elas, destaca o caso emblemático julgado pelo TJSP, onde a empresa do ramo imobiliário CYRELA BRAZIL REALTY S/A EMPREENDIMENTOS E PARTICIPAÇÕES foi condenada na ação 1080233-94.2019.8.26.0100 que tramitou na 15ª vara Cível do TJ/SP, a pagar indenização por dano moral ao requerente.

Segue ementa do julgado (SÃO PAULO, 2020, p.1):

Embargos de declaração. Contradição sanada. Contrato celebrado sob a égide da Lei 13.786/2018 (Lei do Distrato). Diante da peculiaridade do caso concreto (contrato que teve pouquíssimo tempo de vigência), mostra-se excessivamente onerosa a aplicação das disposições do contrato e da Lei 13.786/18. Inteligência do art. 51, IV, do Código de Defesa do Consumidor, que admite a possibilidade de revisão das cláusulas contratuais nulas, abusivas ou excessivamente onerosas. Precedentes do TJSP. Inexistência de outros erros materiais, omissões, obscuridades ou contradições. Embargos de declaração acolhidos, para sanar contradição, sem, todavia, atribuir efeito modificativo ao acórdão embargado.

(SÃO PAULO. TRIBUNAL DE JUSTIÇA - EMBDECCV: 10544319420198260100 SP 1054431-94.2019.8.26.0100, Relator: Pedro de Alcântara da Silva Leme Filho, Data de Julgamento: 28/11/2020, 8ª Câmara de Direito Privado, Data de Publicação: 28/11/2020)

Desta forma, observa-se a Lei em questão efetivamente cumprindo sua finalidade em resguardar a inviolabilidade dos

dados pessoais armazenados pelas empresas e consequente aplicação de sanções as violações.

3.5 O impacto nas pequenas empresas

As microempresas e as pequenas empresas não tem capacidade de investir em altas tecnologias para evitar a ação dos hackers e consequente violação de dados que tenha em seu banco de dados.

Por estas razões, embora possuam bem menos dados armazenados que as grandes multinacionais, estas empresas são alvos atraentes para os “cybers criminosos”, às vezes até por dissidia dessas empresas em adotar posturas mais cautelosas com estas informações.

A Bacharela em Tecnologias da Informação e Comunicação Anne Caroline Dias Bezerra traz os seguintes dados em seu artigo “UMA MODELAGEM DE SEGURANÇA DA INFORMAÇÃO BASEADA NA ISO/IEC 27001 E GESTÃO ITIL APLICADA ÀS MICROS E PEQUENAS EMPRESAS” (2015, p.28):

Porém um recente relatório revelado pela Symantec (2013) nos conduz a uma ,realidade diferente, no qual é descrito no relatório de ameaças à segurança na Internet e constatado um crescimento no roubo de informações valiosas e confidenciais no setor de manufatura e, principalmente nas pequenas empresas nas quais, foram alvos de 31% dos ataques em 2012.

Entre as medidas de proteção que podem ser adotados aparecem procedimentos simples que não demandam tanto investimento e podem ajudar a manter os dados de clientes e próprios destas empresas seguros.

Exigir a identificação do usuário e sua autorização de controle de acesso, de modo que acesse a rede apenas usuários cadastrados e que seja adotado níveis de acesso para cada perfil criado.

Neste contexto, surgem os famosos “firewall” em tradução livre significa corta fogo, embora tal significado não explique a sua importância auxilia n compreensão, uma vez que se trata de um sistema de proteção que tem a missão de não permitir o acesso de outra rede, ou seja, “cortar a conexão”.

A mestrandia Sirlei Lourdes Bach (2001, p.72) assim conceitua:

O firewall é um dispositivo de hardware dotado de duas placas de redes (uma ligada á rede corporativa e outra ligada à Internet), rodando software específico de análise e roteamento de pacotes. Como todo pacote enviado de uma rede a outra passa obrigatoriamente pelo sistema, o firewall tem chance de analisá-lo, verificando se apresenta risco, podendo descartá-lo antes que alcance o destino.

Essas medidas acrescidas com uso de antivírus, criptografia e auditoria de acesso às informações são capazes de reduzir consideravelmente as violações destes tão preciosos dados.

4. Conclusão

A Lei Geral de Proteção de Dados Pessoais foi promulgada em 14 de agosto de 2018 e veio alterando a Lei 12.965 de 2014 (Marco Civil da Internet), sendo que teve sua vigência disciplinada no artigo 65 da lei, com alguns prazos estabelecidos.

Observou-se que a referida lei é uma resposta aos anseios da população que foi vítima cada vez mais de ataques dos “cybers criminosos” que mineram dados pessoais armazenados nos bancos de dados.

Conceituou-se o “Big Data” como um conjunto de técnicas avançadas capazes de armazenar e processar grande volume de informações e ainda que em menores quantidades de dados outras técnicas não obteriam o mesmo resultado.

Desta forma, verificou-se a importância destas técnicas de

armazenamento e processamento de dados e conclui-se que com esta evolução o aumento de violações de privacidade em todas as áreas. Embora as pequenas e microempresas tenham um volume menor e dados armazenados, observou-se que os criminosos tenham uma preferência devido a maior fragilidade de seus sistemas de proteção.

Por fim, com a adoção de medidas preventivas e implantação de alguns sistemas de investimento não muito onerosos é possível diminuir consideravelmente os riscos de exposição aos vazamentos de dados e assim, evitar suas consequências.

5. Fontes de financiamentos.

A pesquisa não obteve nenhum financiamento.

6. Declaração de conflitos de interesses

Nada a declarar.

7. Referências

ALVES, Paulo. Hackers vendem dados de 127 milhões de contas na dark web; entenda. 2019. Disponível em <https://www.techtudo.com.br/noticias/2019/02/hackers-vendem-dados-de-127-milhoes-de-contas-na-dark-web-entenda.ghml>. Acesso em 22 abr. 2022.

BACH, Sirlei Lourdes. CONTRIBUIÇÃO DO HACKER PARA O DESENVOLVIMENTO TECNOLÓGICO DA INFORMÁTICA. Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação. 2001. Disponível em <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/82176/184565.pdf?sequence=1&isAllowed=y>. Acesso em 03 abr. 2022.

BEZERRA, Anne Caroline Dias. A Segurança da Informação Através Da Implementação Do ITIL Para Micro e Pequenas Empresas. 2015. Disponível em: http://repositorio.utfpr.edu.br/jspui/bitstream/1/19438/1/CT_GETIC_VIII_2019_01.pdf. Acesso em: 24 mar. 2022.

BRASIL. Conselho Nacional de Justiça - CNJ. Recomendação n. 73, de 20 de agosto de 2020. Diário da Justiça [do] Conselho Nacional de Justiça, Brasília, DF, n. 272, p. 9-11, 21 ago. 2020. Acesso em: 22 jan. 2022.

BRASIL. MINISTÉRIO DA CIDADANIA. Lei Geral de Proteção de Dados Pessoais (LGPD). www.gov.br. 2021. Disponível em <https://www.gov.br/cidadania/pt-br/aceso-a-informacao/lgpd>. Acesso em 28 fev. 2022.

BRASIL. Superior Tribunal de Justiça - STJ. O ABC da proteção de dados pessoais. STJ, 2020. Disponível em: **Erro! A referência de hiperlink não é válida.** Acesso em: 22 jan. 2022.

COMO FUNCIONAM AS LEIS DE PROTEÇÃO DE DADOS NOS ESTADOS UNIDOS. GATEFY. 2022. Disponível em <https://gatefy.com/pt-br/blog/como-funcionam-leis-protecao-dados-estados-unidos>. Acesso em 28 fev. 2022.

GUSSON, Cássio. Dados de clientes de diversos bancos do Brasil são hackeados e vendidos por Bitcoin na DeepWeb. Disponível em: <https://cointelegraph.com.br/news/customer-data-from-several-banks-in-brazil-are-hacked-and-sold-on-deepweb>. Acesso em: 22 fev. 2022.

HERN, Alex. Maior coleção já encontrada de dados violados. 2019. Disponível em: <https://www.theguardian.com/technology/2019/jan/17/breached-data-largest-collection-ever-seen-email-password-hacking>. Acesso em: 14 fev. 2022.

HIGA, Paulo. Banco Inter vazou dados de quase 20 mil clientes, diz investigação do MP. 2018. Disponível em: <https://tecnoblog.net/noticias/2018/07/31/banco-inter-vazou-dados-correntistas-acao-mp/>. Acesso em: 15 jan. 2022.

LOUBAK, Ana Letícia. Dez dados sobre você que podem estar à venda na dark web. 2019. Acesso em: 23 fev. 2022.

PETRY, André. O berço do Big Data A monumental abundância de dados, sua variedade e a velocidade com que trafegam no universo digital estão revolucionando a civilização. 2013. Disponível em: <https://www.cin.ufpe.br/~cjpgf/TECNOLOGIA%20-%20material%20NAO-CLASSIFICADO/BIG%20DATA%20revista%20Veja%202013.pdf> Acesso em: 23 fev. 2022.

RODRIGUES, Alexandre. SANTOS, Priscilla. A ciência que faz você comprar mais. 2012. Disponível em <https://revistagalileu.globo.com/Revista> . Acesso em 03 jan.2022.

SÃO PAULO. TJ-SP – EMBARGOS DECLARATÓRIOS: 10544319420198260100 SP 1054431-94.2019.8.26.0100, Relator: Pedro de Alcântara da Silva Leme Filho Data de Julgamento: 28/11/2020, 8ª Câmara de Direito Privado, Data de Publicação: 28/11/2020.

TRISTÃO, Gabriela. et. al. Lei Geral de Proteção de Dados: Desafios técnicos enfrentados por microempresas e empresas de pequeno porte. 2021. Disponível em: <https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/4/2>. Acesso em: 23 fev. 2022.

VALENTE, Jonas. Legislação de proteção de dados já é realidade em outros países. 2018. AGENCIA BRASIL. Disponível em <https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises>. Acesso em: 12 fev.2022.

VALINOR, Rodrigo. O que é o Big Data e por que investir?. 2022. Disponível em: <https://www.remessaoonline.com.br/blog/o-que-e-big-data/.pdf> Acesso em: 23 abr. 2022.