VII ENCONTRO NACIONAL DE PROPRIEDADE INTELECTUAL
22 a 24 de Setembro de 2021
ARACAJU - SE ON-LINE

IMPACTOS DA LGPD EM BIG DATA

Giselda dos Santos Barros[1]; Gildete da Silva Santos[2]; Leonôra Virgínia de Jesus Dias[3]; Maria Suely Regis Souza[4]., Suzana Russo Leitão[5], Gabriel Francisco da Silva[6]

[1]Programa de Pós-Graduação em Ciência da Propriedade Intelectual- PPGPI
Universidade Federal de Sergipe – UFS – São Cristóvão/SE – Brasil
giseldaufs@gmail.com
[2]Universidade Federal de Sergipe - UFS
wggildete@outlook.com
[3]Universidade Federal de Sergipe – UFS
leonoradias13@gmail.com
[4]Programa de Pós-Graduação em Ciência da Propriedade Intelectual- PPGPI
Universidade Federal de Sergipe – UFS – São Cristóvão/SE – Brasil
msrsouza24@gmail.com
[5]Programa de Pós-Graduação em Ciência da Propriedade Intelectual- PPGPI
Universidade Federal de Sergipe – UFS – São Cristóvão/SE – Brasil
suzana.ufs@hotmail.com
[6]Programa de Pós-Graduação em Ciência da Propriedade Intelectual- PPGPI
Universidade Federal de Sergipe – UFS – São Cristóvão/SE – Brasil

RESUMO

Este artigo propõe verificar como a Lei Geral de Proteção de Dados — LGPD — Lei n. º 13.709/2018, pode impactar na utilização do Big Data. Justifica-se o presente estudo aos crimes de invasões e utilização indevidas, nos mais diversificados sistemas de Banco de Dados e sua importância para as unidades acadêmicas, empresariais, governos e instituições de ensino. Este estudo tem por base leis que dão embasamento a Lei Geral de Proteção de Dados de 2018, o Big Data, a Segurança Cibernética. Utilizou-se as bases acadêmicas Google Acadêmico, Scielo Br, Ebsco e ScienceDirect. Esta é uma pesquisa com abordagem qualitativa, de natureza básica, e quanto aos objetivos é exploratória e quanto aos procedimentos é uma revisão bibliográfica, através de artigos e leis. Desse modo observa-se que os resultados mostraram a suscetibilidade de um sistema, sendo uma deficiência ou lapso nas formas de segurança de um Big Data, que ocorrem como imprevisto ou propositalmente, e que a segurança deve juntar-se aos objetivos da missão da empresa, pois o grande volume de dados, provoca a incapacidade de serem detectadas as irregularidades em tempo real. O que permite concluir que os responsáveis pelo Big Data deverão investir em uma segurança cada vez mais reforçada e atualizada, para protegerem o conhecimento do Big Data contra invasões e utilização dos dados por interesses diferentes do acordado com o usuário e fornecimento de dados a terceiros, que responderão diretamente ou solidariamente, administrativamente, civilmente e penalmente.

PALAVRAS CHAVE: big data; lei geral de proteção de dados; cibersegurança

1 INTRODUÇÃO

Com o avanço tecnológico, um maior acesso à rede de computadores e as diversas utilizações da internet, aumentaram os ataques cibernéticos, que no século passado usavam vírus para corromper, apagar ou travar computadores. Agora os hackers têm interesse de conseguir dados pessoais, como foi publicado no Jornal Estadão Romani (2021), que houve vazamentos de dados de 223 milhões de CPF, 40 milhões de CNPJ e 104 milhões de registros de veículos, informações de 39.645 brasileiros e 22.983 empresas nacionais.

A Ciso Advisor em 22 de abril de 2021 publicou no seu site sobre uma pesquisa recente da Intel 471, revelando que cibercriminosos estão usando a tecnologia legítima do Big Data para furtar dados dos usuários e vendê-los nos mercados da Dark Web que utilizam o idioma chinês, estas tentativas de invasões ocorrem em todos os países. No Brasil a encarregada por analisar essas relações de segurança é a lei n. º 12.737/2012 que trata de crimes cibernéticos, e a Lei n. º 13.709 — Lei Geral de Proteção de Dados (LGPD) responsável pelas medidas e regras para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais e que se encontra em vigor (BRASIL, 2018) alterada pela Lei 13.853 de 8 de julho de 2019 (BRASIL, 2019).

Devido à importância do Big Data para as unidades acadêmicas, empresariais, governamentais, instituições de ensino e aos cidadãos nos diversificados sistemas e nas mais diversas utilizações, ao mesmo tempo, pode vir a prejudicar de forma contundente as pessoas que tem os seus dados arquivados expostos, desde os possíveis crimes até a utilização indevida dos dados por seus administradores e a invasão aos bancos de dados para roubar essas informações.

Por isso, este trabalho intitulado Impacto da Lei Geral de Proteção de Dados em Big Data, cujo objetivo é verificar como a Lei de Geral de Proteção de Dados — Lei n. º 13.709/2018, pode impactar na utilização do Big-Data (BRASIL, 2018). Para tanto, será utilizado um método com abordagem qualitativa, de natureza básica, quanto aos objetivos é exploratória e aos procedimentos uma revisão bibliográfica realizada nas seguintes bases: ScienceDirect, Scielo.br, Ebsco e Google acadêmico, realizado entre 08/06 a 15/06/2021.

Logo, este artigo visa responder ao seguinte questionamento: como a Lei Geral de Proteção de Dados poderá impactar a utilização do Big Data, para reduzir as multas e responsabilizações pelos crimes cibernéticos?

2 REVISÃO DA LITERATURA

Esta revisão será apoiada na Constituição Federal de 1988, Lei n. º 12.965/14 considerada o marco da internet no Brasil, artigos que fundamentam o Big Data e a Segurança Cibernética, e a Lei Geral de Proteção de Dados — 2018 (LGPD).

2.1 DIREITO A PRIVACIDADE

O direito à privacidade, na Constituição Federal de 1988, é inviolável e assegurado como direito fundamental no seu artigo 5.º, inciso X, que asseguram serem invioláveis a intimidade, a vida privada, garantindo o direito a indenização pelo dano material ou moral decorrente de sua violação, enquanto no inciso XII consta a inviolabilidade quanto ao sigilo dos dados, salvo, por ordem judicial, nas hipóteses e na forma que a lei estabelece para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Contudo, no inciso XIV, é garantido a todos o acesso à informação, e resguardado o sigilo da fonte, quando se fizer necessário o uso para o exercício profissional (BRASIL, 2018). Percebe-se uma lacuna ao pensar que os acessos seriam só profissionais e não considerou os avanços das tecnologias que possibilitariam acessos ilegais.

Diante do exposto, fez-se necessário a criação da Lei n. º 12.965/14, que estabelece princípios, garantias, direitos e deveres para o uso da Internet, fundamentando-se no art. 2°, inciso V, a livre iniciativa, a livre concorrência e a defesa do consumidor e no art. 3° a disciplina do uso da internet

no Brasil, com os seguintes princípios nos incisos: II — proteção da privacidade; III — proteção dos dados pessoais, na forma da lei. No art. 7°, assegura ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: inciso XIII — aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet (BRASIL, 2014).

Essa lei começou a oferecer aos usuários da internet garantias e limites, entretanto até o momento tinham apenas leis que asseguravam os direitos, porém as infrações cometidas eram julgadas civilmente através do Código Civil e/ou Código do Consumidor para atos de natureza indenizatória e penalmente pelo Direito Penal e leis Penais Especiais.

2.1.1 A Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados — 2018 (LGPD), foi alterada pela Lei de n° 13.853/2019 entrou em vigor desde 09/2020, e passou a ser fiscalizada a partir de agosto de 2021, pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD), e dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2019).

No artigo 5°, inciso IV, considera-se como:

> dados pessoais todas as informações que podem identificar uma pessoa; banco de dados — conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; 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 (BRASIL, 2019).

De acordo Castro (2018), para adequação a LGPD, criou-se uma nova profissão a Data Protection, ou seja, Encarregado de Proteção de Dados, ficando responsável por orientar as empresas e evitando possíveis infrações e realizando o cálculo dos impactos da lei que tem como fundamento a regulamentação, proteção de dados e sanções administrativas, devido aos vazamentos de dados e de crime cibernéticos, em modelos de negócios e de tecnologias utilizando dados pessoais através do Big Data, para o desenvolvimento dos negócios e da economia de forma que o cidadão seja assegurado com relação aos dados informatizados.

2.2 BIG DATA

Com as inovações tecnológicas, para Raminelli e Rodegheri (2016), a informática possibilitou que as informações fossem digitalizadas e armazenadas, que possibilitou a utilização crescente dos setores públicos e privados no ambiente virtual, gerando um novo modelo comportamental dos indivíduos no século XXI, usando a internet na sua essência, permitido e impulsionando que entidades públicas e privadas operem cada vez mais no âmbito virtual, utilizando-se da tecnologia para instaurar comunicação, processamentos, transações, entre pessoas de mesmo interesse.

Para Gunther (2017), o Big Data é definido como um conjunto de tecnologias cuja base é coletar e analisar em alta velocidade grande capacidade de volumes de dados diversificados. Como tal, esses dados são difíceis de processar usando as tecnologias existentes. Ao utilizar tecnologias analíticas avançadas, as organizações podem usar o Big Data para desenvolver conhecimentos, produtos e serviços inovadores.

Enquanto para Techamerica Foundation (2012) o Big Data é um termo que descreve grandes volumes de dados de alta velocidade, complexos e variáveis que requerem técnicas e tecnologias avançadas para permitir a captura, o armazenamento, a distribuição, o gerenciamento e a análise das informações em tempo real.

A tecnologia da informação vem transformando a realidade cotidiana dos seres humanos, e os tornando cada vez mais conectados, que conforme estudos realizados no Comitê Gestor da Internet no Brasil (CGI.br) na sua edição de 2019 indicou que 74% da população brasileira na faixa etária de 10 anos ou mais é usuária da internet.

2.3 A SEGURANÇA CIBERNÉTICA E O BIG DATA

Conforme Westcon (2019) investir em Big Data Analytics leva a empresa a lidar de forma otimizada e mais eficiente com seus processos, aumentando sua receita com novos produtos e serviços personalizados, mas para utilizar o Big Data, precisa-se de uma equipe com analistas capacitados e bem qualificados, usuários de negócios e executivos capazes de fazer as perguntas certas e reconhecer padrões, deduzir dados e prever comportamentos, podendo auxiliar as empresas e clientes na tomada de decisões, exigindo que as empresas fiquem atentas a sua cibersegurança.

Para Santos e Carvalho (2019) o aumento da utilização da rede, tem-se também o crescimento dos ataques às redes corporativas, exigindo que as empresas busquem novas tecnologias para uma proteção mais eficientes, contribuindo para reconhecer ameaças ao grande banco de dados percebendo atividades suspeitas e atitudes estranhas de acesso à rede corporativa.

Martins (2019) afirma que é possível ocorrer invasões de privacidade e a discriminação, a perda de autonomia, descaracterização do indivíduo, fornecimento unilateral de informação e o confronto com informações indesejadas são preocupações essenciais ao tratamento de dados. Logo, se verifica que tanto as invasões e usos indevidos nos Big Datas poderá ir de encontro a LGPD/2019.

As inovações tecnológicas e o crescimento do volume de dados obtidos, armazenados, processados, transmitidos e publicados no ambiente do Big Data, vem produzindo barreiras para o direito à privacidade, à segurança das informações pessoais e corporativas colocando em risco o direito e a segurança. Conforme a norma ABNT NBR ISO/IEC 27002:2013, a Segurança da Informação é a proteção da informação contra diversas ameaças, assegurando ininterrupção do negócio, reduzindo as ameaças e aumentando os lucros sobre os negócios e investimentos.

Para Killmeyer (2006), para assegurar a eficácia da segurança deve fundamentar-se em Confidencialidade: proteção das informações contra acesso não autorizado, independente da forma como ela é armazenada ou local de armazenamento; integridade: é a proteção de informações, aplicações, sistemas e redes contra mudanças intencionais, não autorizadas ou acidentais; e Disponibilidade: é a garantia de que as informações e os recursos estão acessíveis pelos usuários autorizados conforme a necessidade.

Enquanto para a norma ABNT NBR ISO/IEC 27032:2012 a Segurança Cibernética é considerada a segurança do espaço cibernético definida pela Segurança Cibernética da Administração Pública Federal — APF, a SegCiber é a arte de assegurar a existência da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas.

As práticas básicas de segurança para as partes interessadas no espaço cibernético fornecem as diretrizes para melhorar o estado da SegCiber, determinando os aspectos comuns dessa atividade e suas ramificações em outros domínios de segurança, tais como: as redes, computadores e a proteção de infraestruturas críticas de informação (ABNT, 2012). Logo, o cuidado com a administração apropriada das informações no Big Data envolve o ciberespaço que para Killmeyer (2006), é um ambiente propício para a exposição ao risco, das informações e dos meios de armazenamento, transmissão e processamento dos sistemas de informação.

3 METODOLOGIA

O caminho metodológico a ser trilhado por esta pesquisa é de natureza básica, quanto aos objetivos é exploratória, em relação à análise dos dados é uma pesquisa qualitativa e aos procedimentos é uma revisão bibliográfica através de artigos e leis.

As Revisões Bibliográficas, foram realizadas nas seguintes bases: ScienceDirect, Scielo.br, Ebsco e Google acadêmico, realizado entre 08/06 a 15/06/2021 utilizando-se das seguintes palavras-chave: “Big Data” and “data theft”; “big data" and "discrimination"; (“big data" and discrimination); “Big Data” and “data theft”; (“big data” and “discriminante”); "big data e discriminação"; "utilização do big data" e "discriminação" totalizando 186, que filtrando, todos no período de 2017 a 2020, e quando tinha opção revistas acadêmicas com idioma em língua portuguesa, realizando em seguida a escolha por temática, onde ficaram apenas 13 artigos.

Sendo 05 artigos da base ScienceDirect, 01 da Scielo.br, 01 artigo da base Ebsco e 06 artigos do Google Acadêmico, sendo 5 artigos sobre invasão e 08 para uso de dados de formas discriminatórias do Big Data. Procedeu-se então um comparativo dos dados encontrados para fazer um levantamento dos problemas mais citados e suas conclusões nos dois eixos, os quais possibilitará uma análise de como estes problemas serão impactados pela aplicação da LGPD. A análise ocorreu através das seguintes variáveis: autor(es), título, objetivo, síntese/considerações respondidos através dos artigos.

4 RESULTADOS E DISCUSSÃO

Os resultados desta pesquisa foram através de 13 artigos, sendo que 5 citaram as possíveis invasões e 08 a discriminação em várias formas no Big Data que irão responder: Como a Lei Geral de Proteção de Dados poderá impactar a utilização do Big Data aqui no Brasil, para reduzir as multas e responsabilizações pelos crimes cibernéticos?

Os dados mostraram a caracterização dos cinco artigos sobre invasão no Big Data, obtivemos que para Bhathal e Singh (2019), a suscetibilidade de um sistema é uma deficiência ou lapso nas formas de segurança de um Big Data, que poderá ocorrer como imprevisto ou propositalmente e que a segurança deve juntar-se aos objetivos da missão da empresa.

Enquanto para Donkal e Verma (2018), empregar segurança em um banco de dados é uma atribuição difícil, pois não tem token, a duplicação dos dados e a criptografia que são formas de assegurar a proteção dos dados, pois com as inovações tecnológicas e as ferramentas de pontas estão surgindo para proteção, também existe um lado oposto, que por novas técnicas estão aí para examinarem os sistemas a procura de suscetibilidade existente no Banco de Dados e na estrutura.

E para Habeeba e et. al (2019), com o aumento de conectividade e a disponibilização crescente da internet, favoreceu os invasores a investir com ímpeto em ataques as redes, isto é, promovendo roubo de informações em diversas áreas, causando prejuízos financeiros e um confronto cibernético, promovendo enorme inquietude para a detecção de anomalias na rede. E que as indagações realizadas mostraram que o grande volume de dados, provocam a incapacidade de serem detectadas as irregularidades em tempo real.

Zharova e Elin (2017), afirmam que na Rússia os fundamentos das leis de proteção de dados vigentes são rígidos, assegurando os direitos dos cidadãos a uma vida privada e assegura que os dados pessoais sejam confidenciais. Conforme Parasol (2018), a China descomplicou os procedimentos cibernéticos e os encargos, propondo que esta nova lei foi para proteger a infraestrutura principal e a suscetibilidade cibernética.

Enquanto a caracterização dos dez artigos sobre a discriminação no Big Data, os dados mostraram a seguinte análise: conforme Soto (2017), o Big Data faz a interdependência do grande volume de dados com os seus algoritmos matemáticos para os tratamentos de dados, para prever tendências e tomadas de decisões, enquanto os usuários de ferramentas digitais abastecem com seus dados para determinada finalidade, não tendo conhecimento da utilização posterior desses dados para propósitos não autorizados.

Calvard e Jeske (2018), pondera sobre os possíveis riscos e incidentes com o Big Data devido vazamentos de dados por imperícia e utilizações incorretas das informações por empregadores e organizações as quais não fazem parte das análises de riscos previstas. Já Azevedo e Jahn (2020), mostram que a abundância de dados coletados e a utilização da inteligência artificial tem colaborado

para a forma como as empresas estão convocando, escolhendo e administrando os seus empregados nos Estados Unidos.

Conforme Machado (2018), os Bancos de Dados e os algoritmos usados nos diversos programas de *surveillance* não são os causadores de danos em seus diversos campos de aplicabilidade por armazenarem dados dos ditos infratores e sim direcionam as forças de segurança do sistema, o de auxiliarem para possíveis violências policiais focadas em segmentos da sociedade.

Enquanto para Passos (2020), o Sistema Penal permanecerá escolhendo pessoas negras, jovens e com baixa escolaridade para ingressarem no sistema carcerário, tendo como argumento o nível de agressividade da pessoa, através de seus aspectos pessoais, podendo verificar a violação dos direitos de igualdade institucional, onde deveria assegurar os direitos básicos de todos os cidadãos. Apesar de não serem observados pelos responsáveis pelos Big Datas, do momento histórico-tecnológico o combate à discriminação continua sendo um objetivo da República como consta na Constituição Federal (BRASIL, 1988).

Coneglian, Segundo e Sant'ana (2017) o Big data proporcionou mudanças na análise de dados nas ciências, empresas e no governo pela quantidade de dados disponíveis para a tomada de decisões, que para os cientistas e analistas de Big Datas isto é um meio de não existir preconceitos e discriminação nas decisões, mas pesquisadores levantam dúvidas sobre estas afirmações, demonstrando que existe comportamentos discriminatórios já existentes e de maneiras mais ocultas.

Conforme Ribeiro (2021) as discriminações são realizadas através de algoritmo de tratamento automatizado de dados pessoais, que pode ter sua tendência proveniente, da base de dados utilizada no seu treinamento e funcionamento ou no lado do algoritmo, na criação, desenvolvimento e testagem dos mesmos, finalizando por realizar as previsões embutidas no sistema e tomar decisões muitas vezes danosas às pessoas, e até mesmo discriminatórias. Logo é importante que estes vieses discriminatórios em logaritmos sejam eliminados nas tomadas de decisões

Assim, pode-se notar que o Big Data tem vantagens, mas possuem as desvantagens que como citadas a cima, as possíveis invasões e descriminação pelos próprios donos ou funcionários, ou por terceiros. Baseando-se em Gomes (2020), para se precaver das ameaças oriundas do Big Data, de qualquer sistema, deve-se basicamente coletar esses dados observando os princípios da LGPD/2019 e que na sua utilização, não exista o compartilhamento de dados pessoais dos usuários e não utilize de forma não autorizada.

A Lei Geral de Proteção de Dados, tem como base principal o respeito à privacidade, a inviolabilidade da intimidade e o desenvolvimento econômico, tecnológico e a inovação, e como característica reduzir as falhas e outros problemas de segurança no armazenamento e processamento de informações e dados coletados pelas empresas no ambiente físico e digital. (BRASIL, 2019)

Verificou-se que a preocupação com os Direitos do usuário, como privacidade, a confidencialidade e a autonomia não sejam violados pela fragilidade que podem existir ou ocasionar no Big Data, motivo de grande preocupação tanto no setor público como no privado, principalmente com a vigência da LGPD/2019 que junto deverão vir as várias mudanças que irão impactar no uso do Banco de dados, que apesar das dificuldades terão que assegurar a privacidade, os dados pessoais e darem livre acesso aos seus donos, pois as empresas serão as responsáveis por protegerem a base de dados dando segurança eficiente e evitando os acessos indevidos (BRASIL, 2019).

Observando que se a ANPD aplicar o Art. 52.º:

> a lei prevê sanções administrativas aplicáveis pela autoridade nacional podendo ser desde uma advertência com prazo estipulado para adoção de medidas corretivas, multa de até 2% do lucro do faturamento do último exercício limitada a R$ 50.000.000,00, multa diária observado o limite total anteriormente citado, divulgação pública da infração após a devida apuração e comprovação do incidente, bloqueio dos dados pessoais referentes a infração até sua regularização e eliminação dos dados pessoais referentes a infração (BRASIL, 2018).

Os responsáveis pela criação e administração dos Big Datas, deverão adequar-se à Legislação brasileira para que não sofram impactos financeiros. Como foi visto o interesse pela informação de dados são maiores pois, são produzidos em larga escala e podem ser estocados sem perder a qualidade. Dessa forma, o mercado tem seus preços definidos pela oferta e procura desses dados pessoais.

5 CONCLUSÃO

O presente trabalho objetivou verificar como a Lei Geral de Proteção de Dados n. º 13.853/2019, pode impactar na utilização do Big-Data, através da análise das legislações aplicáveis para ao tratamento de dados pessoais, bem como as precauções a serem adotadas para a sua coleta e tratamento no Big Data.

Na pesquisa realizada verificou-se que a LGPD/2019 procura preservar o direito do cidadão e a proteção dos seus dados, pois são direitos inerentes à vida humana, para não causar inúmeros danos, ao mesmo tempo que mantem o desenvolvimento econômico, tecnológico e as inovações, assim, com todos os cuidados e ambiguidade mostrada pela utilização da LGPD. Por isso é importante reconhecer o valor dessa lei que unifica e atribui legalmente o respeito ao tratamento de dados na internet, pois estes dados são como mercado de commodity.

Logo, os impactos trazidos pela LGPD para o Big Data, fará com que seus responsáveis tenham que investirem em segurança cada vez mais reforçadas e atualizadas, para prevenirem a sua base de dados de possíveis invasões e evitar a utilização dos seus sistemas de dados como forma a não cometer descriminações, e não fornecerem os dados a terceiros através de convênios, podendo responderem diretamente ou solidariamente, administrativamente, civilmente e penalmente, para tentar reduzir as multas e responsabilizações pelos crimes cibernéticos.

Portanto, as instituições devem implementar soluções e boas práticas de segurança da informação, adequando-se às normas e leis, controlando o acesso às informações, e capacitando as equipes de Tecnologia da Informação. Em trabalhos futuros, sugere-se a análise de outras inovações tecnológicas, como Inteligência artificial (IA), Internet das Coisas (IOT) e outros, que possa interferir na vida do cidadão, através de natureza qualitativa, da adequação de empresas à Lei Geral de Proteção de Dados vigente.

REFERÊNCIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT . NBR/ISO/IEC 27002:2013 tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação. Disponível em http://www.professordiovani.com.br/AdmRedes/NBRISO-IEC27002.pdf>. Acesso em: 14 jun. 2021

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. NBR/ISO/IEC, 27032: 2012: Tecnologia da Informação-Técnicas de segurança-Diretrizes para segurança cibernética. Rio de Janeiro: ABNT, 2015. Disponível em: https://www.iso27001security.com/html/27032.html. Acesso em: 15 jun. 2021

AZEVEDO, André Jobim; JAHN, Vitor Kaiser. **Direito do trabalho e novas tecnologias: inteligência artificial, big data e discriminação pré-contratual**. Disponível em < Azevedo e Jahn - Direito do Trabalho e Novas Tecnologias - Inteligência Artificial Big Data e Discriminação Pré-Contratual.docx.pdf (andt.org.br)>. Acesso em: 15 jun. 2021.

BHATHAL, Gurjit Singh; SINGH, Amardeep. **BIG DATA**: Hadoop framework vulnerabilities, security issues and attacks. Array, v. 1, p. 100002, 2019. Disponível em < Big Data:

Vulnerabilidades da estrutura hadoop, problemas de segurança e ataques - ScienceDirect> Acesso em 15 jun. 2020

BRASIL. **Constituição, de 05 de outubro de 1988**. Contêm as emendas constitucionais posteriores. Diário Oficial [da República Federativa do Brasil], Poder Legislativo, Brasília, DF, 5 out. 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 10 jun. 2021.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. (LGPD). Diário Oficial da União, Brasília, 15 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >. Acesso em: 15 jun. 2021.

BRASIL. **Lei 13.853, de 08 de julho de 2019**. Lei Geral de Proteção de Dados Pessoais. Altera a Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Brasília, 20 dezembro 2019. Disponível em: < L13853 (planalto.gov.br) >. Acesso em: 15 jun. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da República Federativa do Brasil, Poder Legislativo, Brasília, DF, 23 abr. 2014. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 15 Jun. 2021.

CALVARD, Thomas Stephen; JESKE, Debora. Developing human resource data risk management in the age of big data. **International Journal of Information Management**, v. 43, p. 159-164, 2018.Disponível em < Desenvolvimento do gerenciamento de riscos de dados de recursos humanos na era do big data - ScienceDirect>. Acesso em: 16 de jun. 2021.

CASTRO, Gilberto M. **A figura do Data Protection - DPO na LGPD**, 19 nov. 2018. Disponível em https://www.tiespecialistas.com.br/a-figura-do-dpo-na-lgpd/. Acesso em 16 de jun. 2021.

CISO, Advisor. **Cibercriminosos usam big data para roubar dados e vendê-los na dark web**. Produção de mídia, Chief Information Security Officers São Paulo, SP 2013. Disponível em: <https://www.cisoadvisor.com.br/cibercriminosos-usam-big-data-para-roubar-dados-e-vende-los-na-dark-web/>. Acesso em: 10 jun. 2021

COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. (2019**). Pesquisa sobre o uso da tecnologia de informação e comunicação nos equipamentos culturais brasileiros**: TIC Cultura 2018. São Paulo: CGI.br. Disponível em: https://www.cgi.br/media/docs/publicacoes/2/20201123121817/tic_dom_2019_livro_eletronico.pdf . Acesso em 13 de jun. 2021.

CONEGLIAN, Caio Saraiva; SEGUNDO, José Eduardo Santarem; SANT'ANA, Ricardo César Gonçalves. Big Data: fatores potencialmente discriminatórios em análise de dados. **Em Questão**, v. 23, n. 1, p. 62-86, 2017.

DONKAL, Gita; VERMA, Gyanendra K. A multimodal fusion based framework to reinforce IDS for securing Big Data environment using Spark. **Journal of information security and applications**, v. 43, p. 1-11, 2018. Disponível em < Uma estrutura baseada em fusão multimodal para reforçar o IDS para proteger o ambiente big data usando Spark - ScienceDirect>. Acesso em 13 de jun. 2021

PASSOS, Fernanda Silva dos. **A influência do neoliberalismo na utilização de métodos atuariais e seus problemas**. Disponível em < https://editora.pucrs.br/edipucrs/acessolivre/anais/1422/assets/edicoes/2020/arquivos/9.pdf >. Acesso em: 13 de jun. 2021

GOMES, Victor Werneck. Responsabilidade na internet: os perigos do big data para a privacidade. Direito UNIFACS - Debate Virtual, n. 244, 2020. Disponível em < https://revistas.unifacs.br/index.php/redu/article/view/6934>. Acesso em: 9 jun. 2021.

GÜNTHER ET AL, Wendy Arianne. **Debating Big Data**: A literature review on realizing value from big data. sciencedirect. 2017. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0963868717302615>. Acesso em: 9 jun. 2021.

HABEEB, Riyaz Ahamed Ariyaluran et al. Real-time big data processing for anomaly detection: A survey. **International Journal of Information Management**, v. 45, p. 289-307, 2019. Disponível em < Real-time big data processing for anomaly detection: A Survey - ScienceDirect>. Acesso em Acesso em: 9 jun. 2021

KILLMEYER, J. **Information Security Architecture**: An Integrated Approach to Security in Organization. Florida: Auerbach Publications, 2006. Disponível em < https://www.taylorfrancis.com/books/mono/10.1201/9781420031034/information-security-architecture-jan-killmeyer>. Acesso em: 9 jun. 2021

RIBEIRO, Ana Lídia Lira. Discriminação em algoritmos de inteligência artificial: uma análise acerca da LGPD como instrumento normativo mitigador de vieses discriminatórios. 2021. Disponível em <repositorio.ufc.br/bitstream/riufc/57947/1/2021_tcc_allribeiro.pdf>. Acesso em 10 jun. 2021.

MACHADO, Marcos Rafael Lucca. **O demônio de laplace é digital e discriminador**: o uso (quase) exclusivo de bancos de dados criminais em surveillance como ferramenta estigmatizante. Disponível em < o-demonio-de-laplace-e-digital-e-discriminador-o-uso-quase.pdf (metodistacentenario.com.br)>. Acesso em: 11 de jun. 2021

MARTINS, Daniel. **BigData, revolução digital e o Direito**. mercurylbc. 2019. Disponível em: <http://mercurylbc.com/bigdata-revolucao-digital-e-o-direito>. Acesso em: 12 jun. 2021.

PARASOL, Max. The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams. **Computer law & security review**, v. 34, n. 1, p. 67-98, 2018. Disponível em < https://www.sciencedirect.com/science/article/abs/pii/S0267364917300791 >. Acesso em 12 jun. 2021.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. A Proteção de Dados Pessoais na Internet no Brasil: Análise de decisões proferidas pelo Supremo tribunal Federal. In: **Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir**./UFRGS. Disponível em: < http://seer.ufrgs.br/ppgdir/article/view/61960/39936 > Acesso em 10 jul 2021

SANTOS, Carlos Eduardo Lessa; CARVALHO, Felipe Freire de. **Privacidade e proteção de dados na era do big data**. 2019. Disponível em < https://app.uff.br/riuff/handle/1/13054 > Acesso em 11 jun. 2021.

SOTO, Yasmina. Datos masivos con privacidad y no contra privacidad. **Revista de Bioética y Derecho**, n. 40, p. 101-114, 2017. Disponível em < Datos masivos con privacidad y no contra privacidad (isciii.es)>. Acesso em 22 de jul.

TECHAMERICA FOUNDATION'S. **Demystifying Big Data**: A Practical Guide To Transforming The Business of Government. bigdatawg. Washington, 2012. 10 p. Disponível em: <https://bigdatawg.nist.gov/_uploadfiles/M0068_v1_3903747095.pdf>. Acesso em: 12 jun. 2021.

WESTCON. **Quais os benefícios do big data analytics para os negócios**? Brasil, 2019. Disponível em: <http://digital.br.synnex.com/pt/quais-os-beneficios-do-big-data-analytics-para-os-negocios>. Acesso em: 12 jun. 2021.

ZHAROVA, Anna Konstantinovna; ELIN, Vladimir Mikhailovich. The use of Big Data: A Russian perspective of personal data security. **Computer Law & security review**, v. 33, n. 4, p. 482-501, 2017. Disponível em < https://www.sciencedirect.com/science/article/abs/pii/S0267364917301164> Acesso em: 12 jun. 2021.