Avaliação da adequação de Instituto Federal à Lei Geral de Proteção de Dados Pessoais

Marco Antonio Torrez Rojas[1], Jucelio Kulmann de Medeiros[1]

[1]Instituto Federal de Santa Catarina (IFSC) – Florianópolis, SC - Brasil

marco.rojas@ifsc.edu.br, jucelio.medeiros@ifsc.edu.br

Abstract. *Information security and data privacy are considered areas that present great challenges for the information society due to the technological advance of Artificial Intelligence, Big Data and Internet of Things that make use of the large volume and variety of data generated by information systems, and the use of current computational power can transform data into information and intelligence for making decisions. This process can violate the users' privacy and their fundamental rights. In order to regulate how public or private companies will manage user data in their environment, Brazilian government has sanctioned the Law 13.709/2018, known as the General Data Protection Law (LGPD). This article identify the application of the law to educational institutions, in particular to the Federal Institute assessment compliance within the law. In the evaluation carried out, it was identified that the Federal Institute is in the initial stage of complying with the law, which is critical due the volume of work that consists of adapting the institution's processes and systems, as well as changing the institutional culture of management of personal data. Increasing the criticality, there's a short time to complying with the law, as it goes into effect in Mai 2021.*

Keywords*: LGPD Evaluation. LGPD Adequation. Privacy.*

Resumo. *A segurança da informação e a privacidade de dados são consideradas áreas que apresentam grandes desafios da sociedade da informação em função do avanço tecnológico da Inteligência Artificial, Big Data e Internet das Coisas, que fazem uso do grande volume e variedade de dados gerados pelos sistemas de informação e que, utilizando o poder computacional atual, podem transformar os dados em informações e inteligência para a tomada de decisões. Esse processo pode gerar violação à privacidade dos usuários e seus direitos fundamentais. Para regulamentar como as empresas públicas ou privadas vão tratar os dados dos usuários em seu ambiente, o governo do Brasil sancionou a Lei 13.709/2018, conhecida por Lei Geral de Proteção de Dados (LGPD). Este artigo buscou identificar a aplicação da lei às instituições de ensino e, em especial, efetuar a avaliação do Instituo Federal no atendimento à lei. Na avaliação efetuada identificou-se que o Instituto Federal encontra-se no estágio inicial de atendimento a lei, o que é crítico face ao volume de trabalho em que consiste a adequação dos processos e sistemas da instituição, bem como a mudança de cultura institucional de tratamento de dados pessoais. Aumentando a criticidade, há curto prazo de atendimento à lei, que entrará em vigor em maio de 2021.*

Palavras-chave: *Avaliação da LGPD. Adequação à LGPD. Privacidade.*

1. Introdução

A humanidade, no decorrer dos tempos, passou por diversas formas de organização social e econômica para o seu desenvolvimento. Cada uma destas formas teve uma característica fundamental que marcou o seu período. Assim, tivemos a sociedade agrícola, sociedade industrial, sociedade pós-industrial e sociedade da informação. A sociedade da informação também é conhecida como a quarta revolução industrial, e nesta sociedade a informação tem o papel principal e fundamental. Este protagonismo foi possível graças à evolução tecnológica, que possibilitou a criação de mecanismos capazes de processar (computadores), armazenar e transmitir informações por meio das redes de computadores em quantidade e volumes não imaginados nos períodos anteriores (Bioni, 2019).

A tecnologia que trouxe benefícios para o desenvolvimento da sociedade da informação também apresenta desafios, sendo um deles considerar a sua utilização como neutra, mas ela não é: a tecnologia é neutra, não a sua utilização. Assim, as grandes organizações e estados que podem fazer uso da tecnologia de modo mais efetivo e mais produtivo não a utilizam com neutralidade (Drummond, 2003).

Além das tecnologias tradicionais, têm-se as tecnologias emergentes, por exemplo, a Inteligência Artificial (IA), *Big Data* e Internet das Coisas (IoT) que servem de motor para a transformação digital das organizações, dos governos, das indústrias e das nossas vidas, com utilização, por exemplo, em áreas como a produção, a mobilidade, o entretenimento, os sistemas financeiros, a saúde, a educação, etc. A IA contribui muito com a melhoria de entendimento dos dados auxiliando, assim, na tomada de decisões complexas em tempo hábil por meio de suas principais técnicas de reconhecimento de padrões que são conhecidas por Aprendizado de Máquina (*Machine Learning*, ML) (Bigonha, 2018). O *Big Data* é composto por algoritmos capazes de procurar e desvendar padrões e tendências em grandes quantidades de dados, e também em grande variedade de tipos de dados (Letouzé, 2018). A IoT possibilita a coleta de dados oriundos de diversos objetos inteligentes com capacidade de sensoriamento, assim aumentando o volume de dados que podem estar relacionados a uma pessoa ou grupo de pessoas (Santos, 2016). Porém, as tecnologias de IA e *Big Data* possibilitam, por meio dos algoritmos de processamento de dados, gerar informações que podem afetar a privacidade e anonimização dos dados, em especial de pessoas que tiveram seus dados coletados e analisados (Bigonha, 2018; Letouzé, 2018).

Tendo em vista a questão do tratamento de dados pessoais por meio de tecnologias de informação e comunicação (TIC), o Brasil sancionou a Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018 BRASIL (2018). Segundo Mendes (2019), o país editou de forma inédita um regime geral de proteção de dados, pois acredita que não existem dados irrelevantes diante do processamento automatizado e generalizado na sociedade da informação. Então, "uma vez que os dados pessoais são um meio de representação da pessoa na sociedade, qualquer tratamento de dados pode afetar a sua personalidade e, portanto, tem o potencial de violar seus direitos fundamentais" (Letouzé, 2018 p. 2). A adoçao da lei no Brasil foi também motivada pelo lançamento da *General Protection Data Regulation* (GPDR), lei com mesmo intuito promulgada na Europa, bem como vazamentos em larga escala já anunciados e divulgados mundialmente.

Como a LGPD aplica-se a todos os setores econômicos e também ao setor público, o presente trabalho busca efetuar uma avaliação da adoção da lei por parte do

da instituição de ensino da rede federal, chamada neste trabalho de Instituto Federal, visando preservar a privacidade e informações da instituição que cooperou com esta pesquisa. Por meio desta avaliação, foi possível identificar o estado atual de adequação à lei por parte do Instituto Federal, e por consequência, identificar pontos que necessitam ser adequados, em especial para o tratamento de dados de alunos nos sistemas do Instituto Federal.

2. Tecnologias Habilitadoras

Segundo Marquesone (2016), nas décadas de 80 e 90 a maioria dos dados estavam armazenadas em formato analógico (e.g. discos de vinil, fitas cassete e vídeo, etc.) e somente 0,8 % no formato digital, enquanto que em 2007 os dados já estavam 94 % no formato digital. Os dados são a matéria-prima para a sociedade da informação, pois, por meio do processamento e análise destes dados é possível gerar conhecimento, utilizado pelas organizações para apoiar a tomada de decisão em seus processos (Comarela, 2019).

Com a expansão da utilização da Internet, em especial da adoção das redes sociais e comércio eletrônico nos últimos anos, dados relacionados aos usuários foram gerados. Em sua grande maioria, estão online e são de acesso público, passando a ser utilizados na previsão de eventos e tomadas de decisões por parte das organizações, com base nos padrões de interações interpessoais, opiniões e compras (França, 2014).

Devido à adoção das tecnologias chamadas habilitadoras, em especial da *Big Data* e IA de forma integrada sobre os dados abundantes de usuários providos pela Internet das Coisas, passou-se a gerar conhecimento sobre os mesmos. Este conhecimento gerado aumentou os riscos aos direitos individuais e de grupo, à privacidade e à segurança dos indivíduos que utilizam as tecnologias da informação e comunicação de forma intensa nos dias atuais (Letouzé, 2018).

2.1. Big Data

Segundo Celes (2017), o termo *Big Data* é empregado em diferentes situações no contexto de dados massivos. Por massivos compreende-se lidar com um grande volume de dados, gerados e processados em alta velocidade, e que possuam uma variedade de dados em função das diferentes fontes de onde são obtidos.

Essas características relacionadas ao volume, à variedade, e à velocidade dos dados são conhecidas como os três V's do *Big Data*. O volume é considerado a característica mais significativa, pois é a dimensão onde a quantidade de dados a serem processados é levada em consideração face às tecnologias tradicionais que não conseguem tratar deste volume de dados. A variedade está relacionada à estrutura de armazenamento (tipo, tamanho e forma de sequenciamento) utilizada para armazenar dados, este armazenamento pode ser estruturado, como no caso dos bancos de dados relacionais1, mas também pode ser semiestruturado (possuem estrutura pré-definida, porém não rigorosa. e.g. arquivos JSON (*JavaScript Object Notation*) e XML (*eXtensible Markup Language*) e não estruturados (e.g. vídeos, imagens e textos). Considera-se que 20 % dos dados disponíveis globalmente sejam estruturados. Por velocidade entende-se a velocidade em que os dados são coletados, analisados e utilizados. Para que se possa compreender este universo, em apenas um minuto mais de dois milhões de pesquisas são feitas no buscador do Google, seis milhões de páginas são visitadas no Facebook e 1,3 bilhão de vídeos são vistos no Youtube. Assim, a dimensão

da velocidade também engloba a velocidade com que os dados são gerados (Marquesone, 2016).

Além dos tradicionais três V's, temos os 3 C's: *impulcrumbs* (migalhas), *capacities* (capacidades) e *communities* (comunidades). Impulsionados pelas tecnologias digitais relacionadas a um fenômeno social mais amplo, são considerados mais atuais dentro do contexto de *Big Data* devido às suas limitações, segundo Letouzé (2018).

O primeiro C, *crumbs* (migalhas digitas ou migalhas de dados) representa dados que não são gerados para serem processados ou analisados, em sua maioria são deixados de forma passiva pelos humanos ao fazer uso de dispositivos ou serviços digitais. A utilização dessas tecnologias deixa um rastro digital que, acumulado, compõe a maior parte do *Big Data* como fonte de dados na atualidade, podendo ser estruturado e não estruturado.

O segundo C refere-se a *capacities* (capacidades), ou seja, ferramentas, métodos, software e hardware que consistem dos arcabouços das soluções *Big Data* disponíveis no mercado seja de forma paga ou software livre (*softwares* disponibilizados pela comunidade para uso de forma gratuita). Assim, nestes sistemas temos computadores poderosos, sistemas de computação paralela, técnicas estatísticas utilizando aprendizado de máquina e algoritmos capazes de procurar e desvendar padrões e tendências em grandes quantidades de dados complexos.

O terceiro C, *communities* (comunidades), envolve os atores individuais e instituicionais multidisciplinares que constituem a comunidade interna e externa ao *Big Data*, os quais buscam encontrar ordem na desordem e transformar em significado, ou seja, informação. Assim, com este conjunto de ferramentas disponibilizado pelo arcabouço *Big Data* é possível inferir a partir dos dados, ou seja, predizer com base nos dados atuais ou efetuando previsão, o que deve acontecer. Além disso, também é possível fazer inferências causais, ou seja, estabelecer correlação entre eventos (Letouzé, 2018).

Esta grande capacidade de manipulação de dados, além de suas vantagens, trouxe riscos e desafios. Riscos relacionados à privacidade, à identidade e à segurança; e desafios relacionados aos limites éticos para tratamento dos dados (Cisco, 2019; Letouzé, 2018; Marquesone, 2016).

2.2. Inteligência Artificial

Segundo Bittencourt (1998), a Inteligência Artificial (IA) é um ramo da ciência da computação ao mesmo tempo recente e muito antigo, pois a IA foi construída a partir de ideias filosóficas, científicas e tecnológicas herdadas de outras ciências, algumas tão antigas quanto a lógica. O objetivo central da IA é simultaneamente teórico (criação de teorias e modelos para a capacidade cognitiva) e prático (a implementação de sistemas computacionais baseados nestes modelos). Para Tafner (1995) a IA busca imitar por meio de programas computacionais as formas de resolução dos problemas do mesmo modo que o ser humano faz, no caso, por meio da utilização de algoritmos. A IA têm muitas linhas de atuação, sendo as principais a computação evolutiva e a computação conexionista. A computação evolutiva tem sua inspiração nas computações biológicas realizadas pelos seres vivos para viver e se reproduzir, com principal aplicação em problemas combinatórios, organizacionais e otimizações. Os algoritmos genéticos são um dos principais exemplos desta linha. A computação conexionista tem sua base na

simulação dos componentes do cerébro (modelagem à inteligência humana), as redes neurais são o principal exemplo desta linha, com aplicação no reconhecimento de padrões (Bittencourt, 1998). Logo, temos linhas de estudo focadas em reproduzir o pensamento e raciocínio humano, e outras buscam entender e simular o comportamento humano.

Segundo Bigonha (2018), os algoritmos são o motor e o combustível os dados para as aplicações de Inteligência Artificial, em especial, as técnicas de Aprendizado de Máquina (*Machine Learning*). As técnicas de aprendizado de máquina consistem em programas capazes de aprender a solucionar um problema por meio de experiências passadas (dados) e não uma programação explícita. Assim, quanto maior a quantidade, a qualidade e a diversidade dos dados disponíveis, mais se favorece o aprendizado por parte dos algoritmos de tarefas mais complexas. Logo, estas técnicas são muito utilizadas para o reconhecimento de padrões, como exemplo, reconhecimento de imagens, sistemas de recomendação de compras e filmes, etc., pois, permitem que o comportamento do usuário seja analisado e seu padrão de comportamento identificado. Este padrão é utilizado pelas empresas para oferecer mais produtos ou serviços personalizados, pois, estão atrelados ao perfil de consumo do consumidor.

A popularização da IA e suas abordagens têm relação direta com a abundância e barateamento da infraestrutura para processamento, armazenamento de dados e conectividade, bem como aos avanços em algoritmos utilizando IA aliados a uma maior disponibilidade de dados e, por fim, à disponibilidade dessas tecnologias em código aberto. Este cenário favorece os sistemas de Inteligência Artificial, pois conseguem tomar decisões mais complexas em tempo hábil para tomada de decisão (Bigonha, 2018).

2.3. Internet das Coisas

Internet das Coisas (*Internet of Things* (IoT)) refere-se à integração de objetos físicos (sensores e atuadores) e virtuais em redes conectadas à Internet, permitindo que qualquer dispositivo (“coisa”) que possa fornecer algum dado, colete, troque e armazene dados em enorme quantidade, que, uma vez processados e analisados, geram informações em escala inimaginável (Almeida, 2015; Borba, 2018). A IoT surgiu dos avanços de várias áreas como sistemas embarcados, microeletrônica, comunicação e sensoriamento, e tem recebido bastante atenção por parte da academia e indústria em função do seu potencial de aplicação nas mais diversas áreas das atividades humanas, porém apresentando riscos e desafios técnicos (e.g. regulamentações, segurança e padronizações) e sociais (Santos, 2016; Borba, 2018).

Devido ao avanço das tecnologias das redes sem fio, a conectividade e convergência entre tecnologias heterogêneas de coleta e transmissão de dados foi possível, assim, estima-se mais de 40 bilhões de dispositivos conectados em 2020 (Borba, 2018). Além de computadores conectados teremos, por exemplo, TVs, *Laptops*, automóveis, *smartphones*, consoles de jogos, *webcams* e dispositivos vestíveis (*wearables*), e também uma divesidade de novas aplicações como, por exemplo, cidades inteligentes (*SmartCities*), saúde (*Healthcare*), casas inteligentes (*Smart Home*) (Santos, 2016). Estimas-se 1,1 bilhões de dispositivos vestíveis até o ano 2022, que utilizam principalmente as tecnologias Wi-Fi e Bluetooth para comunicação de dados (Cisco, 2019). Segundo Rose (2015), as projeções dos impactos do IoT na Internet e economia são de impressionar, levando em conta 100 bilhões de dispositivos conectados, e um impacto global na economia de 11 trilhões de dolares até o ano 2025.

Segundo Borba (2018), dentro do contexto de IoT, segurança e privacidade são questões diferentes. Segurança está relacionada ao sistema que deve preservar a sua integridade e funcionalidades mesmo em casos de ataques; já privacidade considera que o sistema deve preservar a confidencialidade das informações pessoalmente identificáveis, ou seja, dado ou informação que possa relacionar o mesmo a uma pessoa ou sistema de informações. Assim, pode-se verificar que a segurança tem papel importante para auxiliar nas questões que envolvem a privacidade dos dados dos usuários em dispositivos ou dispositivos que fazem parte de um sistema integrado de maior porte.

Os dispositivos de IoT quando estão interconectados à Internet, assim como os computadores pessoais ou corporativos passam também a ser mais um vetor de possíveis ataques visando a comprometer o sistema e seus dados. Dessa forma, necessitam no mínimo os mesmo níveis de proteção, sem considerar as suas peculiaridades com relação ao dispositivo em si, que é um ambiente de computação muito mais restrito, seu sistema operacional, aplicações e protocolos de comunicação.

Os requisitos fundamentais de segurança CID (Confidencialidade, Integridade e Disponibilidade) devem também ser atendidos por este cenário heterogêneo de dispositivos e também levando em consideração as suas peculiaridades e respectivas limitações de hardware e software, pois necessitam ter mecanismos para cuidar dos dados que por ele são processados, armazenados e encaminhados (Rose, 2015; Santos, 2016).

3. Lei Geral de Proteção de Dados Pessoais (LGPD)

Nesta seção será abordada a revisão da literatura relacionada as questões que envolvem à LGPD, iniciando pela definição de privacidade de dados e seu respectivo entendimento no contexto da lei. Também serão abordados de forma sucinta os dez capítulos que compreendem a lei, e por fim um levantamento dos principais desafios que envolvem as instituições de ensino com relação a sua adequação e atendimento ao solicitado na LGPD.

3.1. Privacidade de Dados

A segurança em computação contempla três princípios fundamentais: confidencialidade, integridade e disponibilidade (CID), conforme Bishop (2003), além das seguintes funções necessárias para o tratamento dos dados, informações e serviços de computação de acordo com Stallings (1999): autenticação, controle de acesso e irretratabilidade.

A confidencialidade trata de duas abordagens, a primeira com relação à confiabilidade dos dados, assegurando que a informação será manipulada somente por quem tem permissão, a segunda é com relação à privacidade, assegurando que os indivíduos possuam o controle apropriado sobre os seus dados, compreendendo a coleta, a armazenagem e a sua divulgação. A integridade busca assegurar que os indivíduos terão seus dado modificados ou alterados somente por quem tem o respectivo privilégio, a disponibilidade busca assegurar que os dados vão sempre estar disponíveis para serem utilizados pelos indivíduos.

Comumente, segurança e privacidade são tratados como sinônimos, sendo que a segurança engloba os mecanismos que pode ser empregados para assegurar que os requisitos de privacidade sejam atendidos, principalmente aos dados em formato

eletrônico. Segundo Brands (2000), a definição mais aceita na literatura para a questão de privacidade do usuário com relação a sua informação e dados é: privacidade pode ser definida como o direito de um indivíduo, grupo ou instituição de determinar por si próprio quando, como, para quem e em que nível as informações sobre si são comunicadas a outros. Esta relação entre privacidade e segurança vai além dos dados em formato eletrônico, abrangendo também o contexto físico dos dados, ou seja, quando existe a necessidade de se proteger a informação que se encontra em outras mídias (e.g., termos de uso, contratos, etc). Neste sentido a privacidade é mais complexa com relação ao tratamento de dados sensíveis.

Segundo Turn (1986) os principais mecanismos para assegurar a proteção às informações pessoais são caracterizados como: legislativo, administrativo e técnico. Com relação à proteção da privacidade através de leis, segundo Maciel (2019), a partir de 2013 o mundo presenciou acontecimentos que motivaram a criação e renovação de legislações de proteção dados visando à privacidade e proteção de informações pessoais em vários países do mundo. No caso do Brasil tivemos o Marco Civil da Internet (Lei n° 12.965/2014), que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, e tratando do termo jurídico privacidade (Brasil, 2014) e a Lei Geral de Proteção de Dados (LGPD), lei 13.709/2018 (Brasil, 2018), que apresenta um regime geral de proteção de dados para o setor público e privado.

Na parte administrativa, existem boas práticas e normas que se destinam à questão de privacidade: ISO IEC 27000, NIST SP 800-122 (Guia para proteger a confidencialidade de informações pessoais) e HIPPA (*Health Insurance Portability and Accoutability Act*, especifica para o contexto de proteção para a área de saúde empregada nos Estados Unidos), etc. Em Dezembro de 2019, no Brasil, foi lançada a norma ABNT NBR ISO/IEC 27701 – ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/ IEC 27002, para gestão da privacidade da informação – requisitos e diretrizes. A norma tem foco em um Sistema de Gestão de Privacidade da Informação que contribui com a comunidade pública e privada no caminho de adequação à LGPD (Farias Junior, 2019).

Na parte técnica, existem diversas ferramentas tecnológicas que podem atender à necessidade de privacidade dos dados, por exemplo, o uso de soluções de criptografia de forma geral, firewalls (controle de acesso) e a aplicação de boas práticas de governança (Maciel, 2019; Pinheiro, 2018).

3.2. A Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados (LGPD) foi promulgada no Brasil seguindo o exemplo de outros países (e.g.; *General Protection Data Regulation* (GPDR) em vigor no âmbito da União Europeia), visando a regulamentar o tratamento dos dados, sejam eles gerados no meio digital ou não, protegendo os direitos fundamentais do cidadão, como privacidade, liberdade de expressão e direitos humanos, consolidando as questões sobre proteção de dados e direitos do titular em um único dispositivo (Pinheiro, 2018). A LGPD é constituída de dez capítulos com relação ao tratamento de dados que devem ser seguidos pelas organizações, sejam públicas ou privadas. De forma sucinta estes capítulos contemplam as descrições a seguir relatadas.

O Capítulo I – DISPOSIÇÕES PRELIMINARES dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica realizados no território nacional, e suas respectivas finalidades e fundamentos e princípios, bem como

definições adotadas na lei, como, por exemplo, dado pessoal, titular, controlador, operador, etc. A definição e atribuições dos atores controlador e operador requerem atenção especial.

O Capítulo II – TRATAMENTO DOS DADOS PESSOAIS dispõe sobre as condições em que o tratamento de dados pode ser realizado e também sobre as suas exceções. A necessidade de consentimento para tratamento dos dados é um dos assuntos discutidos e que requer atenção, bem como a questão dos direitos do titular dos dados. A questão do tratamento de dados pessoais sensíveis e dados pessoais de crianças e adolescentes são abordados, assim como a questão sobre os aspectos que envolvem o término do tratamento dos dados. Também os papeis do operador e controlador no contexto do tratamento dos dados são abordados e requerem atenção para a correta aplicação e entendimento da lei.

O Capítulo III – DIREITOS DO TITULAR aborda os aspectos relacionados à titularidade dos dados pessoais e seus direitos a liberdade, intimidade e privacidade, bem como é abordada a relação entre controlador e titular. O papel e atribuições do controlador para com as necessidades do titular são especificadas e necessitam atenção para as instituições que forem assumir o papel de controlador no processo de tratamento de dados.

O Capítulo IV – TRATAMENO DE DADOS PELO PODER PÚBLICO aborda aspectos com relação às regras e responsabilidades no tratamento de dados pessoais pelas pessoas jurídicas de direito público e as sociedades de economia mista, buscando atender, executar e cumprir a lei no contexto do serviço público. Atenção especial deve ser dada para a questão de compartilhamento de dados entre instituições públicas e privadas.

O Capítulo V – TRANSFERÊNCIA INTERNACIONAL DE DADOS aborda os aspectos relacionados à transferência de dados pessoais para países e organismos internacionais e respectivas regras. A autoridade nacional poderá designar organismos para fiscalização desta questão de transferência de dados pessoais em contexto internacional. Esta fiscalização se faz necessária pela necessidade de verificação se os países em questão têm leis similares e com o mesmo nível de proteção previstas na LGPD.

O Capítulo VI - AGENTE DE TRATAMENTO DE DADOS PESSOAIS dá ênfase às obrigações e papeis dentro do contexto da LGPD do controlador e operador no trato dos dados pessoais, bem como a relação entre ambos para o atendimento a lei. Também são abordadas as responsabilidades legais e respectivos ressarcimento de danos em caso de alguma violação da lei efetuada pelo operador e/ou controlador.

O Capítulo VII – SEGURANÇA E BOAS PRÁTICAS estabelece que os agentes de tratamento de dados (operador e controlador) devem adotar medidas de segurança da informação para proteger os dados pessoais que são responsáveis, basicamente é necessário um controle de acesso, que envolve os acessos indevidos e/ou situações de tratamento inadequado ou ilícito aos dados pessoais. Também são recomendados a adoção de boas práticas de gestão dos dados, controles e governança por parte dos agentes de tratamento de dados. Os agentes devem estar preparados para demonstrar a efetividade de suas ações perante a solicitação da autoridade nacional. Para as empresas que necessitam se adequar a lei, este item é um grande desafio, pois, não é de um dia para outro que se cria uma cultura de gestão de dados com foco em segurança e privacidade. Além de cultura também é necessário ter profissionais

capacitados para implementar ferramentas, normas, processos e políticas que demandam as medidas de segurança da informação.

No Capítulo VIII – FISCALIZAÇÃO, são definidas as sanções administrativas aplicáveis pela autoridade nacional para com os agentes de tratamento de dados em caso de algum descumprimento da LGPD. As multas previstas em caso de alguma violação consistem de até 2% (dois por cento) do faturamento do responsável pela infração, limitado a R$ 50.000.000,00 (cinquenta milhões de reais) por infração. Como todas as empresas públicas ou privadas que manipulam dados pessoais estão envolvidas na lei, este valor é mais uma preocupação que os gestores devem ter além dos custos necessários para se adequar as necessidades apontadas pela LGPD.

O Capítulo IX – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE visa a criar e definir o papel da ANPD, bem como a sua estrutura como órgão que responde pela criação das diretrizes da política nacional de proteção de dados pessoais e da privacidade. A ANPD é o órgão responsável por operacionalizar a parte de fiscalização, bem como definir, quando necessário, questões técnicas mínimas a serem adotadas pelos agentes de tratamento de dados. Quando a LGPD foi sancionada pelo Presidente Michel Temer, a criação da ANPD foi vetada, sendo sancionada somente em 09/07/2019, com vetos, pelo Presidente Jair Bolsonaro. Considerando que a lei entraria em vigor a partir de Agosto de 2020, esta aprovação tardia de um órgão tão importante é considerado crítico devido a indefinições que podem surgir durante o processo de implantação da lei por parte das empresas públicas ou privadas. Porém, em abril de 2020 o governo voltou a prorrogar o início de vigor da LGPD, passando a ser 03 de maio 2021.

O Capítulo X – DISPOSIÇÕES FINAIS E TRANSITÓRIAS aborda algumas alterações e disposições na lei, e define a data de início de vigor da lei. Neste capítulo podemos destacar a necessidade da possibilidade de exclusão definitiva dos dados pessoais quando solicitada por parte do titular a quem tiver fornecido.

Pode-se verificar que a lei apresenta as questões que devem ser abordadas para a proteção dos dados pessoais por parte das empresas públicas e privadas que manipulam dados. A lei compreende, além de aspectos jurídicos, aspectos técnicos relacionados à segurança da informação e governança. Este aspecto interdisciplinar da lei requer maior atenção das empresas a seu atendimento, bem como uma equipe similar para auxiliar na atividade. Para auxiliar no processo de entendimento dos aspectos da lei e também da sua implementação, recomenda-se a leitura dos livros escritos por Bioni (2019), Maciel (2019) e Pinheiro (2018), e do artigo de Mendes (2019), que abordam com profundidade este assunto.

3.3. Recomendação da LGPD às Instituições de Ensino

Para identificar as recomendações às instituições de ensino com relação à adequação da LGPD, foi realizada uma busca na Internet por palavras-chave. O sitio de buscas utilizado foi o Google e as palavras chave foram: LPGD + Escolas + Educação + Ensino. Após a realização da busca, oito referências foram identificadas e analisadas (Iscool, 2019; Borelli, 2019; Escolas, 2019; Freitas, 2019; Pinto, 2019; Tadeu, 2019; Telefônica, 2019; Zaidan, 2019). Neste levantamento foram identificados vinte e seis recomendações, classificadas pelo autor em sete temas e quantificadas pelo seu número de ocorrências, sendo eles: Processos com dez recomendações; Dados com sete

recomendações; Infraestrutura com três recomendações; Conscientização e Consentimento com duas recomendações cada; e Negócio e Financeiro com uma recomendação cada. Essas recomendações classificadas por tema são apresentadas a seguir.

Processos

- Necessidade de adaptação em termos de normas e processos;
- Necessidade de plano de ação envolvendo um comitê multidisciplinar para gerar uma política de privacidade, acesso e revisão do fluxo de dados;
- Necessidade de mapeamento de dados, criação de políticas de privacidade e acesso e, paralelamente, o engajamento do corpo pedagógico e a conscientização de todos;
- Revisão da política de acesso aos Sistemas para atendimento à LGPD;
- Necessidade de uma política de gestão de dados, treinamentos e evangelização dos colaboradores;
- Mapear como os dados de alunos, pais, colaboradores e fornecedores são coletados e tratados;
- Mapeamento de riscos e elaboração de relatório de impacto à proteção de dados pessoais, e conformidades;
- Instituições que oferecem cursos no exterior (EaD) em português necessitam atender a lei;
- Transformar em processo a monitoração do atendimento a LGPD; e
- Revisão de todos os documentos (contrato de matrícula, contrato de trabalho, terceirizados com acesso a dados pessoais, política de privacidade, portais, aplicativos, contrato de armazenamento em nuvem, etc);

Dados

- Gestão dos dados (alunos, pais, responsáveis e visitantes);
- Atenção especial para o tratamento de dados de crianças e adolescentes.
- Envio de dados sensíveis ao MEC (relatórios), o que fazer com os casos que não foram autorizados pelo aluno ou responsáveis;
- Confirmação de dados sensíveis para alunos que recebem bolsa;
- Dados tratados de forma física (*off-line*) ou digital (*on-line*), e independente do seu porte; e
- Atenção aos dados sensíveis (origem racial ou étnica, convicções religiosas, opiniões políticas, filosóficas, saúde, vida sexual, dados genéticos ou biométricos). Recomenda-se cláusulas separadas no contrato para tratar estes tipos de dados.

Infraestrutura

- Necessidade de ferramentas de segurança e boas práticas para gerenciar o ambiente tecnológico, evitando vazamentos;
- Necessidade de atuação das áreas de TI (governança e segurança) e jurídica; e

- Criar o papel de DPO para responder a Autoridade Nacional de Proteção de Dados, seja por ações de alunos ou colaboradores.

Conscientização

- Professores, famílias e alunos cientes dos propósitos da coleta dos dados e forma de utilização, ou seja, compreender o que estão autorizando; e
- Necessidade de educação dos alunos, para cuidar da informação (proteção a privacidade) em acessos a Internet.

Consentimento

- Validar consentimento de acesso a informações. Consentimento explícito pelo titular dos dados, autorização sobre os dados, em contrato no momento da matrícula; e
- Dados de menores de idade, o consentimento é dado por ao menos um dos pais ou responsável legal.

Negócio

- Prazo mais curto para atendimento da LGPD pelas necessidades de adequação em função das matriculas que se iniciam antes e outros, ou seja, forma de funcionamento das instituições de ensino relacionada ao calendário acadêmico.

Financeiro

- Necessidade de investimentos para adequação e atendimento a LGPD, e avaliação de atendimento a lei.

4. Procedimentos Metodológicos

Para o desenvolvimento deste artigo foram utilizadas duas abordagens metodológicas, a revisão da literatura e o estudo de caso (Prodanov; Freitas, 2013).

A revisão da literatura ou revisão bibliográfica consistiu em fundamentar de forma crítica quais foram os principais vetores tecnológicos e como contribuíram para gerar impacto à privacidade dos dados e sua relação com os seus atores, ou seja, correlacionar ações e atos por meio da análise dos dados e desta forma poder identificar características que podem ser utilizadas para gerar perfis ou padrões, e como estes podem ser aplicados a diversas áreas e desta forma vir a impactar a privacidade dos envolvidos. Assim, foram pesquisadas as tecnologias *Big Data*, Inteligência Artificial e Internet das Coisas, sua relação e suas características que possibilitam formar uma tríade que tem sido utilizada na análise de dados de forma massiva e de forma eficiente e efetiva.

Aplicando a técnica de revisão sistemática, que consiste em efetuar uma revisão bibliográfica direcionada e de forma sistêmica, ou seja, em etapas, buscando identificar os objetivos de busca definidos e efetuar a sua análise, foi efetuado o levantamento dos impactos da LGPD nas instituições de ensino. A pesquisa foi realizada no sitio de buscas Google e utilizando as palavras chave LPGD + Escolas + Educação + Ensino. Após a busca e processos de filtragem da técnica foram identificados e analisados oito trabalhos relacionados, e o resultado da aplicação da técnica apresentada no capítulo

2.2.3 intitulado “A LGPD nas Instituições de Ensino”. Para auxiliar a compreender melhor a questão dos impactos da LGPD no contexto das instituições de ensino, a abordagem Estudo de Caso foi utilizada neste artigo. O público-alvo do estudo de caso foi o Instituto Federal, representado pelos servidores da área de Tecnologia da Informação (TI). O levantamento de dados correu por meio de entrevista, utilizando o questionário desenvolvido pela empresa ICTS Protiviti como base, as questões fazem parte da Tabela 1 da seção 5 Resultados e Discussão. Foram entrevistados pelo autor, o Diretor de Tecnologias da Informação, o Chefe do Departamento de Sistemas de Informação e o Coordenador de Governança de TI da instituição. A área de TI da instituição é responsável pelas questões de políticas, planos e normas de segurança da informação e governança de TIC (Tecnologia de Informação e Comunicações), e também pelo Comitê de Segurança da Informação. As questões de Privacidade de Dados e as questões da LGPD estão sobre a responsabilidade desta diretoria. No processo de avaliação de adequação adotou-se três critérios para a avaliação, o nível Básico considera que o atendimento à questão ainda esta em estágio inicial, o nível Intermediário considera que o atendimento a questão é parcial e o nível Pleno considera que o atendimento a questão foi atendida de forma plena, e o nível Não Atendido quando nada foi efetuado com relação a necessidade endereçada pela questão.

O estudo de caso buscou avaliar o grau de adesão do Instituto Federal aos requisitos da LGPD, esta avaliação foi efetuada por meio de entrevistas tendo como base questionário elaborado pela empresa ICTS Protiviti com questões pertinentes a necessidades apresentadas na lei. A ICTS Protiviti é uma empresa de consultoria, auditoria e serviços em gestão de riscos (Protiviti, 2019).

A *Data Protection Impact Assessment* (DPIA, 2019) publicou um guia para auxiliar no processo de condução de avaliação dos impactos na proteção de dados de acordo com as necessidades previstas na GPDR (*General Data Protection Regulation*) vigente na União Europeia. Para avaliação do Instituto Federal ambas foram avaliadas, porém neste artigo foi utilizado o questionário desenvolvido pela ICTS Protiviti, pois é mais adequado a LGPD e também pelo fato do quida da DPIA ser muito genérico e direcionado as necessidades previstas na GPDR. Porém, as perguntas que constam na avaliação desenvolvida no DPIA estão contidas no questionário desenvolvido pela ICTS Protiviti e de forma mais abrangente, este fato ressalta que ambas as leis estão alinhadas com relação a necessidade do tratamento da privacidade de dados.

5. Resultados e Discussões

Por meio do levantamento sobre a LGPD em instituições educacionais, foi possível verificar que o atendimento à lei é um grande desafio as instituições de ensino públicas ou privadas e necessitam de suporte de equipes multidisciplinares para atender as necessidades previstas na lei. Além disso, existem questões da lei que não estão claras para seu atendimento, como o caso do aluno que se recusa a dar consentimento e esta informação é necessário por um órgão do governo, e também como vão figurar estes alunos nas estatísticas, etc. Também foi possível identificar que não existem estudos focados na aplicação da lei no contexto das instituições de ensino públicas ou privadas, somente o que foi levantado, porém muito pouco para poder auxiliar os gestores nesta adesão a lei.

A Tabela 1 que contém as treze questões que constituem o questionário e utilizadas na entrevista, as respostas da equipe de TI do Instituto Federal, bem como a avaliação de adequação a LGPD elaborada pelo autor e respectivas considerações.

Tabela 1: Avaliação da adequação do Instituto Federal à LGPD

Questão	Resposta Equipe de TI	Avaliação do Autor
1) A Instituição possui um programa estruturado de Segurança de Informações?	Possui política de segurança e comitê de segurança da informação. Normas relacionadas ao uso dos recursos de TI, porém poucas normas focadas em segurança da informação.	Intermediário - Devido as necessidades apontadas pela LGPD, é necessário um maior foco em normas relacionadas a Privacidade de Segurança dos Dados, e também ter um processo estruturado para atendimento das necessidades apontadas pela LGPD.
2) A instituição possui políticas e/ou normativos sobre suas práticas de Proteção?	A instituição possui sistema de governança, sem aprovação pelo conselho superior da instituição. No plano ainda não aprovado tem gestão de dados, porém no sentido de segurança e não dados no sentido da LGPD.	Básico - A instituição deve atualizar as normas ou políticas vigentes para atender as demandas da LGPD e também os critérios por ela estipulado.
3) Todos os servidores foram capacitados na política de segurança de informações da instituição e políticas de Proteção?	Não foi efetuada capacitação formal na parte de segurança e proteção de dados. Porém, esta diretirz consta na nova normativa da instituição. Na Intranet da instittuição é abordada a questão de senhas de segurança, porém não foi efetuado nenhum treinamento ou capacitação dos servidores neste sentido.	Básico - É necessário que a instituição desenvolva capacitação dos servidores, contendo um programa de conscientização que deve contemplar “o que”, “como” e “por que” fazer com relação a tratamento de dados pessoais. Esta capacitação também deve apresentar a LGPD e suas necessidades.
4) A instituição tem mapeado os riscos de segurança de informações e Proteção de dados, bem como possui um plano formal de mitigação que é acompanhado e patrocinado pelo C-level?	A instituição possui em fase final de elaboração o Plano de Gestão de Riscos, contemplando o levantamento dos riscos e sua classificação, e alinhados com o plano de continuidade. O respectivo Plano de Gestão de Riscos não contempla a Proteção de Dados.	Básico - Recomenda-se atualizar o Plano de Gestão de Riscos para que contemple as necessidades de Proteção de Dados previstas na LGPD e a mesma seja colocada em prática.
5) A instituição tem mapeado os dados pessoais utilizados,	A instituição não tem estes mapeamentos. Mas, em função da utilização dos	Básico - A instituição deverá realizar um inventário de dados em seus sistemas e estrutura

bem como tem registrado onde e como eles estão armazenados e utilizados?	sistemas este mapeamento existe, porém sem focar tanto na questão de dados pessoais.	física, objetivando identificar seus controladores e operadores, bem como atribuindo na LGPD visando a justificar manutenção e tratamento dos dados. Também é necessário preparar o pedido de consentimento do uso de dados pessoais que deve ser dado pelo proprietário do dado, de forma clara e de fácil acesso, com o propósito de processamento de dados.
6) A instituição tem mapeado os dados pessoais sensíveis e aplica as medidas de proteção adequadas?	A instituição não tem estes mapeamentos. Mas, em função da utilização dos sistemas este mapeamento existe, porém sem focar tanto na questão de dados pessoais.	Básico - A instituição deverá realizar um inventário de dados em seus sistemas e estrutura física buscando a identificação de dados pessoais sensíveis, tais como religião, posição política e saúde, objetivando direcionar ações específicas, tais como anonimização, pseudoanonimização ou para limitar o acesso a tais bases, buscando assim mitigar os riscos relacionados a vazamento deste tipo de informação.
7) Quando os dados pessoais são tratados por terceiros, sua instituição verifica se todas as medidas de aderência à LGPD foram por eles aplicadas?	A instituição não possui um levantamento dos dados pessoais tratados por terceiros e respectivas medidas relacionadas à LGPD.	Não Atendido - Recomenda-se elaborar um completo mapeamento de todo o processo de coleta e tratamento dos dados dos usuários, bem como uma reformulação da política de Proteção e dos termos de uso de *websites* e aplicativos. Caso exista a necessidade de transferência de dados para outros países é obrigatório este mapeamento, em especial para dados enviados a União Europeia e países membros.
8) A instituição tem ciência das situações em que os dados são transferidos para fora do Brasil, e toma medidas efetivas para	A instituição não tem levantamento de dados que são transferidos para fora do Brasil.	Não Atendido - Para transferência internacional de dados é necessário uma série de mecanismos legítimos para além da regra da adequação, como o consentimento e o

proteger tais dados?		cumprimento de compromissos assumidos em acordo de cooperação internacional conforme orientações da LGPD.
9) Todos os requisitos de aviso, escolha e consentimento para cada uso de dados pessoais foram atendidos?	A instituição não tem este levantamento de dados efetuado.	Não Atendido - A instituição necessita criar processos para gerenciamento de consentimento e respectiva remoção quando necessário. O consentimento para uso de dados pessoais deve ser dado de forma clara e de fácil acesso, com o propósito de coleta, armazenamento e processamento de dados. A instituição, por tratar com crianças e adolescentes, necessita elaborar este processo de gestão de consentimento com muita cautela e atenção.
10) A instituição possui meios para demonstrar as "medidas organizacionais e técnicas de segurança" que foram aplicadas aos dados pessoais?	A instituição não efetua as técnicas de segurança requisitadas aos dados pessoais, em função disso não tem como demonstrar a aplicação das medidas organizacionais e respectivas técnicas de segurança requisitadas.	Não Atendido - Recomenda-se que a instituição implemente medidas técnicas e processos organizacionais para assegurar o nível de segurança adequado aos dados pessoais que a instituição manipula. Estes processos tem que ser demonstráveis em caso de solicitação por parte do usuário/ cliente ou órgão regulador.
11) A instituição possui estrutura para proteção de dados e interface com autoridades externas?	A instituição possui estrutura e comitê que tratam da governança e segurança da informação, porém os aspectos de proteção de dados e formas para tratar com as autoridades externas não esta definida.	Básico - A instituição, para atender a LGPD, necessita definir um DPO (*Data Protection Officer*), ou seja, um responsável na instituição pelos dados pessoais. Além disso, a empresa deve desenvolver processos que contemplem atividades de treinamento e concientização dos servidores e empresas relacionadas envolvidas com o tratamento de dados pessoais.
12) A instituição	A instituição não tem o	Não Atendido - A instituição

possui mapeadas as bases legais para tratamento/ processamento de dados pessoais ou dados sensíveis?	mapeamento questionado e também processos que abordem o tratamento dos dados pessoais e/ou dados sensíveis.	necessita efetuar o mapeamento completo do fluxo de informações em seus sistemas e estrutura física, e também os controladores e operadores previstos na LGPD. O pedido de consentimento do uso dos dados pessoais deve ser fornecido pelo proprietário do dado ou responsável em caso de menor de idade. Este processo deve ser efetuado caso o mapeamento não tenha sido desenvolvido ou esteja em desenvolvimento. O pedido de consentimento não exime a instituição de elaborar o mapeamento para poder ter um controle pleno do tratamento dos dados e atender à LGPD na integra.
13) A instituição possui processo para que a Proteção (*privacy by design*) seja adotada por padrão e desde o início do desenho das soluções que serão implementadas?	A instituição não tem o processo de *Privacy by Design* (desenvolver sistemas já levando em consideração requisitos de privacidade, em especial os solicitados na LGPD) instituído pela área de desenvolvimento de sistemas.	Não Atendido - Recomenda-se que a instituição leve em consideração adotar o *Privacy by Design* em seus processos de desenvolvimento de sistemas e aplicações utilizadas na instituição.

Conforme a Tabela 1, o Instituto Federal foi avaliado em seis questões (2, 3, 4, 5, 6 e 11) com de atendimento à LGPD no nível Básico, ou seja, está em um estágio inicial e crítico de atendimento à LGPD, pois a lei entraria em vigor em Agosto de 2020 e a entrevista foi efetuado em Novembro de 2019. A lei acabou sendo adiada em Abril de 2020 para entrar em vigor em 3 de Maio de 2021. O Instituto Federal foi avaliado em seis questões (7, 8, 9, 10, 12 e 13) com atendimento à LGPD no nível Não Atendido, ou seja, existe muito trabalho a ser feito para que a adequação à LGPD ocorra de forma plena e acredita-se que seja muito difícil que tenha condições de estar pronta para atender à lei na sua forma plena, no prazo estipulado pela lei. O nível Intermediário foi avaliado em uma questão, a questão 1, que aborda a questão de infraestrutura para tratar da questão da segurança da informação. Apesar de a instituição possuir corpo técnico e comitê que trata da questão de segurança da informação, os assuntos relacionados à Privacidade de Dados não fazem parte dos processos e normas por ela tratados, mas este mesmo corpo técnico deve conseguir apoio da direção da instituição para dar prioridade e buscar a sua adequação à LGPD, mesmo que não seja

no prazo previsto na lei. Em função do tempo para adequação, é necessário definir prioridades e o mínimo a ser feito para que a instituição não sofra as sanções previstas na lei. Por fim, destaca-se que o Instituto Federal não conseguiu atender em nível Pleno em nenhuma das questões que abordam a adequação a LGPD.

A Tabela 2 apresenta um resumo da avaliação efetuada, contendo a quantidade de questões por nível e sua respectiva porcentagem.

Tabela 2: Resumo do resultado da Avaliação efetuada

Nível Avaliado	Quantidade de Respostas	Percentual Atingido
Intermediário	1	7,69%
Básico	6	46,15%
Não Atendido	6	46,15%

Conforme a Tabela 2, tivemos os itens Básico e Não Atendido dentendo 46,15% cada dos critérios de avaliação, totalizando 92,31% dos resultados, e o nível Intermediário dentendo 7,69%. Também verifica-se que existe muita demanda de esforço e trabalho para se atingir o nível Pleno, ou seja, somente 7,69% tem condições de atingir este nível no próximo passo de melhoria, o nível Básico com 46,15% tem dois níveis de esforço para atingir o nível Pleno, o nível Não Atendido com 46,15% tem três níveis de esforço para atingira o nível pleno. Se efetuar uma análise de risco sobre os critérios avaliados é difícil especificar um plano de ação com as respectivas prioridades de atendimento a serem desenvolvida pela equipe do Instituto Federal. Portanto, a Tabela 2 ratifica o nível crítico que encontra-se o Instituto Federal face o atendimento a lei e seu prazo curto para entrar em vigência.

6. Considerações Finais

Com base na avaliação efetuada do atendimento do Instituto Federal à LGPD pode-se verificar que existem muitos pontos em aberto que necessitam ser trabalhados para que a mesma possa atender à lei de forma plena. Existem também ações que estão em seu estágio inicial, porém sem foco no atendimento à lei, pois fazem parte de ações anteriores à sua edição. Apesar do conhecimento da lei por parte da instituição e equipe e comitê responsável, não foi identificado um plano de ação para adequação dos processos e sistemas do Instituto Federal para estar de acordo com as necessidades demandas pela lei.

Recomenda-se o desenvolvimento de um plano de atividades de adequação à LGPD. Dentre as ações do plano é primordial e fundamental definir os responsáveis por gerir o processo e iniciar por um mapeamento dos processos e sistemas que manipulam dados pessoais e/ou dados pessoais sensíveis, pois sem este mapeamento, não é possível decidir os critérios que devem ser adotados para proteger os dados pessoais manipulados pela instituição. Estes critérios são a base da lei e que também fundamentam as sanções financeiras previstas em caso de não atendimento.

A mudança cultural da instituição e seus servidores face à necessidade de tratamento de dados pessoais também é um grande desafio, pois mudanças culturais demandam tempo e investimentos em divulgação e treinamento. Como a LGPD entraria

em vigor em Agosto de 2020 estas ações são urgentes para atendimento mínimo da lei, necessitando ser avaliadas e desenvolvidas pelo Instituto Federal para que atenda a lei sem comprometer a sua operação. Com o novo adiamento para entrar em vigor em 3 de Maio de 2021, a instituição ganhou tempo extra. Porém, em função da pandemia do COVID-19 o impacto nas atividades das instituições foi grande e compromentendo mais ainda a sua implementação, mesmo com o tempo extra.

Destaca-se que esta avaliação reflete a posição do período de tempo em que foi feita a entrevista. Assim, a situação da instituição com relação ao atendimento da lei pode estar diferente do apresentado.

References

Almeida, Hyggo. Internet das Coisas: Tudo Conectado. Internet das Coisas. Nós, as cidades, os robôs, os carros: Tudo conectado. Revista da Sociedade Brasileira de Computação. n. 29, abr. 2015, p.6-8. Disponível em: https://www.sbc.org.br/images/flippingbook/computacaobrasil/computa_29_pdf/comp_brasil_2015_4.pdf. Acesso em: 05 nov. 2019.

Bigonha, Carolina. Inteligência Artificial em Perspectiva. Panorama setorial da Internet. n. 2, out. 2018, a. 10. p.1-9. Disponível em: https://nic.br/media/docs/publicacoes/1/Panorama_outubro_2018_online.pdf. Acesso em: 23 set. 2019.

Bioni, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 1. ed. Rio de Janeiro: Forense, 2019.

Bishop, Matt. Computer Security: Art and Science. Upper Saddle River: Pearson Education, 2003.

Bittencourt, Guilherme. Inteligência Artificial: Ferramentas e Teorias. Florianópolis: UFSC, 1998.

Borba, V. U. PROPOSTA DE UM MODELO DE REFERÊNCIA PARA INTERNET DAS COISAS: aspectos de segurança e privacidade na coleta de dados. 2018. 88 f. Dissertação (Mestrado em Ciência da Informação) - Faculdade de Filosofia e Ciências – Universidade Estadual Paulista “Júlio de Mesquita Filho” –UNESP – campus de Marília, São Paulo, 2018.

Brands, Stefan. A. Rethinking public key infrastructures and digital certificates: building in privacy. Montreal: The MIT Press, 2000.

Brasil. Lei nº 13.709, de 14 de ago. de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 23 set. 2019.

Brasil. Lei nº 12.965, de 23 de abr. de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 jan. 2020.

Borelli, Alessandra. LGPD – Como escolas e universidades devem estar preparadas para esta nova realidade?. abr, 2019. Disponível em: https://www.fundacred.org.br/site/2019/04/16/lgpd-como-escolas-e-universidades-devem-estar-preparadas-para-esta-nova-realidade/. Acesso em: 30 out. 2019.

Celes, Clayson S.F. de S. et al. Big Data Analytic no Projeto de Redes Móveis: Modelos, Protocolos e Aplicações. Minicursos do Simpósio Brasileiro de Redes de Computadores-SBRC2017, [S.1.], v.35, p.1-58, 2017.

Cisco. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022 White Paper. feb. 2019. Disponível em: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html. Acesso em: 14 out. 2019.

Comarela, Giovanni. et al. Introdução à Ciência de Dados: Uma visão pragmática utilizando Pythom, Aplicações e Oportunidades em Redes de Computadores. Minicursos do Simpósio Brasileiro de Redes de Computadores-SBRC2019, [S.1.], v.37, p.1-50, 2019.

Data Protection Impact Assessment. Sample DPIA Template. jan, 2019. Disponível em: https://iapp.org/resources/article/sample-dpia-template/. Acesso em: 20 out. 2019.

Drummond, Victor Cameiro. Internet, Privacidade e Dados Pessoais. 1. ed. Rio de Janeiro: Lumen, 2003.

Escolas, Direcional. Lei de Proteção de Dados chega às escolas: saiba como se preparar. fev, 2019. Disponível em: https://direcionalescolas.com.br/lei-de-protecao-de-dados-chega-as-escolas-saiba-como-se-preparar/. Acesso em: 30 out. 2019.

França, Tiago Cruz. et al. Big Social Data: Principios sobre Coleta, Tratamento e Análise de Dados Sociais. Simpósio Brasileiro de Banco de Dados-SBBD. Tópicos em Gerenciamento de Dados e Informações 2014, v.1, p.8-45, 2014.

Freitas, Mariana. Como a Lei Geral de Proteção de Dados impacta as escolas. mar, 2019. Disponível em: https://www.tuneduc.com.br/lei-geral-de-protecao-de-dados-nas-escolas/. Acesso em: 30 out. 2019.

Farias Junior, Ariosto. Vem aí a ABNT NBR ISO/IEC 27701. n. 8 boletim ABNT, set./ out. 2019. Disponível em: http://www.abnt.org.br/images/Docspdf/Artigos/Artigo_27701.pdf. Acesso em: 15 jan. 2020.

Fundação Telefônica. Lei Geral de Proteção de Dados Pessoais: por que sua escola precisa se preocupar?. jun, 2019. Disponível em: http://fundacaotelefonica.org.br/educacao-do-seculo-xxi/lei-geral-de-protecao-de-dados-pessoais-por-que-sua-escola-precisa-se-preocupar/. Acesso em: 30 out. 2019.

Iscool APP. Especial LGPD: As adequações a serem feitas pelas escolas. abr, 2019. Disponível em: https://iscoolapp.blog/tag/lei-geral-de-protecao-de-dados/. Acesso em: 30 out. 2019.

Letouzé, Emmanuel; ALLIANCE, Data-Pop. Big Data e desenvolvimento: uma visão geral. Panorama setorial da Internet. n. 1, out. 2018, a. 10. p.1-11. Disponível em: https://www.nic.br/media/docs/publicacoes/6/Panorama_estendido_maio_2018_online.pdf. Acesso em: 23 set. 2019.

Maciel, Rafael F. Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei no. 13.1709/18). 1. ed. Goiânia: RM Digital Education, 2019.

Marquesone, Rosangela. Big Data: Técnicas e tecnologias para extração de valor dos dados. 1. ed. São Paulo: Casa do Código, 2016.

Mendes, Laura Schertel. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento: conceitos e modelos de aplicação. Panorama setorial da Internet. n. 2, jun. 2019, a. 11. p.1-7. Disponível em: https://www.nic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acesso em: 23 set. 2019.

Pinheiro, Patricia Peck. Proteção de Dados Pessoais: comentários à Lei n. 13.1709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

Pinto, Diego de Oliveira. LGPD: Entenda o seu Impacto nas Instituições de Ensino. Mar, 2019. Disponível em: https://blog.lyceum.com.br/lgpd-lei-geral-de-protecao-de-dados/. Acesso em: 30 out. 2019.

Prodanov, C. C.; Freitas, E. C. D. Metodologia do Trabalho Científico: Métodos e Técnicas de Pesquisa e do Trabalho Acadêmico. Novo Hamburgo, RS, Brasil: Editora Feevale, 2013.

Protiviti. Proteção de Dados Pessoais: Como as empresas devem se preparar para as novas regras? out, 2019. Disponível em: https://www.protiviti.com/BR-por/protecao-de-dados-pessoais. Acesso em: 21 out. 2019.

Rose, Karen. et al. THE INTERNET OF THINGS: AN OVERVIEW - Understanding the Issues and Challenges of a More Connected World. oct. 2015. Disponível em: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf. Acesso em: 07 jan. 2020.

Santos, Bruno P. et al. Internet das Coisas: da Teoria à Prática. Minicursos do Simpósio Brasileiro de Redes de Computadores-SBRC2016, [S.1.], v.34, p.1-50, 2016.

Stallings, William. Cryptography and Network Security: Principles and Practice. Upper Saddle River: Prentice Hall, 1999.

Tadeu, Erivelto. O impacto da nova lei de proteção de dados. abr, 2019. Disponível em: https://revistaensinosuperior.com.br/nova-lei-protecao-de-dados/. Acesso em: 30 out. 2019.

Tafner, Malcon A. e al. Redes Neurais Artificiais: introdução e princípios de neurocomputação. Blumenau: Furb/Eko, 1995.

Turn, R. Security and privacy requirements in computing. In Proceedings of 1986 ACM Fall joint computer conference (ACM '86). IEEE Computer Society Press, Los Alamitos, CA, USA, 1106-1114.

Zaidan, Paula. Educação: prazo para a LGPD pode ser menor. ago, 2019. Disponível em: http://www.securityreport.com.br/destaques/educacao-prazo-para-estar-em-conformidade-com-a-lgpd-pode-ser-menor/#.Xi9YzXVKhuQ. Acesso em: 30 out. 2019.