

Proteção dos dados pessoais: impactos da Nova Lei Geral de Proteção de Dados no Instituto Federal do Tocantins

Wilmar Borges Leal Junior⁽¹⁾,
Suzane Aparecida Cordeiro⁽²⁾ e
Alexis Vinícius de Aquino Leal⁽³⁾

Data de submissão: 25/11/2021. Data de aprovação: 16/5/2022.

Resumo – A coleta de dados pessoais por meios digitais tornou-se comum. É quase impossível acessar algum sistema sem antes realizar um cadastro, seja no setor privado ou no público. O presente trabalho tem como tema central a gestão dos dados pessoais no poder público frente à Nova Lei Geral de Proteção de dados – LGPD. A escolha do tema surgiu da necessidade de mapear, compreender e conhecer a importância da adequação da nova lei no setor público. Este trabalho tem por objetivo avaliar a LGPD sob a ótica do direito e da tecnologia da informação, examinando os sistemas web utilizados no Instituto Federal do Tocantins – IFTO. Além disso, demonstrou-se o potencial de efetividade da Lei no âmbito institucional e a exemplificação de hipóteses de transgressão da Lei e suas consequências jurídicas. A pesquisa baseia-se em um estudo bibliográfico e na revisão da literatura para identificar as produções acadêmicas a respeito do tema ligadas ao setor público, na área de ensino, com a realização de revisões bibliográficas, compreendendo assim a dimensão da discussão acerca do tema. Muitos desafios irão surgir ao longo da adequação do fato à norma. Empresas publicam e manipulam diariamente dados e registros. Contudo, os primeiros passos para a efetiva proteção se mostram perceptíveis à medida que as instituições públicas e privadas buscam o melhor entendimento da Lei, aplicando-a em seu ambiente corporativo, uma vez que, tendo em vista a vigência da norma, a atuação para conformidade deve ser imediata.

Palavras-chave: Dados sensíveis. LGPD. Poder Público. Proteção de dados.

Protection of personal data: Impacts of the New General Data Protection Law on the Federal Institute of Tocantins

Abstract – The collection of personal data by digital means has become common. It is almost impossible to access any system without first registering, whether in the public or private sector. This main theme of this study is the management of personal data in the public power in the face of the New Data Protection Law. The choice of the theme arose from the need to map, understand, and get to know the importance of the adequacy of the new law in the public sector. This work aims to evaluate the data protection law, from the perspective of both law and information technology, examining the web systems used at the Federal Institute of Tocantins. Besides that, the potential effectiveness of the law at the institutional level and the exemplification of hypotheses of transgression of the law and its legal consequences were demonstrated. The research is based on a bibliographic study and literature review to identify academic productions on the topic, linked to the public sector, in the teaching area, with bibliographic reviews, understanding the dimension of the discussion on the theme. Many

¹ Advogado, Bacharel em Direito (UNITINS) e Licenciado em Computação (UNIVERSO/GO), com Mestrado em Modelagem Computacional de Sistemas (UFT). Professor de Direito do IFTO – *Campus* Gurupi. *wilmar.junior@ifto.edu.br. ORCID: <https://orcid.org/0000-0002-1876-6907>.

² Graduada em Gestão Financeira (UNIP) e especialista em Contabilidade Pública e Responsabilidade Fiscal (UNINTER). *suzanecordeiroborges@gmail.com. ORCID: <https://orcid.org/0000-0002-8867-0484>.

³ Graduado em Ciência da Computação (UNIC-MT) e mestre em Ciência da Computação (UFG). Professor da área de Ciência da Computação do IFMT – *Campus* Confresa, Centro de Referência de Canarana-MT. *alexisleal@gmail.com. ORCID: <https://orcid.org/0000-0002-1962-0993>.

challenges will arise when adapting the fact to the standard. Companies publish manipulative data and records daily; however, the first steps towards effective protection are noticeable as public and private institutions seek a better understanding of the Law, applying it in their corporate environment, since, in view of the norm's validity, the action for compliance must be immediate.

Keywords: Sensitive data. LGPD. Government. Data protection.

Introdução

A crescente demanda por conexão à internet no país é demonstrada através de um estudo feito pelo IBGE (2018), em que é constatado o aumento no percentual de domicílios com internet, subindo de 69,3% para 74,9%, de 2016 para 2017, representando uma alta de 5,6 pontos percentuais. Parte da inovação do setor público se faz pelo uso de sistemas informáticos para gerenciar informações, sendo inúmeros os *sites* que coletam dados para permitir um simples acesso ao usuário.

Em outras palavras, em diversos sítios governamentais, para se permitir o acesso a determinado conteúdo, o usuário deve fornecer seus dados. O mundo está cada vez mais virtual: contratos online, *smart contracts*, assinatura digital e até mesmo a resolução de conflitos, que dependia de uma presença física, já alcançou o espaço virtual, por meio da resolução online de disputa – ROD. O que vem se discutindo na atualidade é como regular esse novo setor, o setor da informação.

Nesse diapasão, muito tem se falado sobre a Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais –LGPD, na perspectiva jurídica, razão pela qual a maioria das palestras e cursos sobre a LGPD abriram espaços para várias especializações, a maior parte relacionada ao advogado-consultor da nova lei. Contudo, um ponto significativo dessa discussão acerca da proteção de dados é o administrador de sistemas, de infraestrutura e banco de dados, pois esses são os atores principais no processo, visto que são eles que terão que definir regras nos sistemas de informação para se adequarem à nova norma imposta.

Volvendo-nos principalmente às regras da lei supracitada, temos que, no *caput* do art. 1º, “Esta Lei 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”.

Nesse contexto normativo, a LGPD veio abrangendo todos os setores, do público ao privado, do particular à indústria, mesmo tendo uma *vacatio legis* de 24 meses, como declarado no seu art. 65, inciso II: “Art. 65. Esta Lei entra em vigor: II - 24 (vinte e quatro) meses após a data de sua publicação”. Insta investigar como anda o preparo técnico para recepção da respectiva norma.

A ideia da proteção de dados visa assegurar que o cidadão tenha a seu dispor meios para exercer efetivo controle sobre seus dados.

Conquanto, nasce, ainda que timidamente, a figura do Direito Digital, que representa uma evolução no Direito como ciência, juntamente com a jurimetria, recém-inaugurada, em que são aplicados métodos e técnicas de Estatística, Matemática e Probabilidades aos acontecimentos jurídicos, de forma que se possa ter uma extração de informação. Nesse sentido, estabelece Nunes (2016) o que vem a ser jurimetria:

A jurimetria tem três pilares operacionais: o jurídico, estatístico e computacional. O jurimetrista ideal seria, portanto, um bacharel em Direito capaz de especular sobre o funcionamento da ordem jurídica e familiarizado com conceitos de Direito processual e material; um estatístico capaz de discutir o planejamento de uma pesquisa e conceber testes de suas hipóteses de trabalho; e um cientista da computação capaz de operar programas para minerar e coletar dados. (NUNES, 2016, p. 112)

Várias são as possibilidades de pesquisa ao se incluir Direito, Computação e Estatística, entretanto, este estudo trata-se de uma análise da Lei Geral de Proteção de Dados em seu aspecto técnico e sua (in)aplicabilidade no setor público, segundo diretrizes da Lei.

Delimitação da pesquisa

Este trabalho de pesquisa delimitou-se a analisar o contexto da LGPD no setor público. Tendo em vista as especificidades de cada setor, de maneira empírica, podemos afirmar que parte desse setor carece de mão de obra qualificada para atender, na íntegra, a nova lei. Dessa forma, nos delimitamos a analisar o enquadramento da Lei no Instituto Federal do Tocantins – IFTO, na recepção do novo modelo de gestão de dados, analisando apenas os dados públicos disponíveis no Portal do IFTO nos anos de 2019 a 2020.

O Instituto Federal do Tocantins

O Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO) é resultante da integração da Escola Técnica Federal de Palmas (ETF) com a Escola Agrotécnica Federal de Araguatins (Eafa), e foi criado por meio da Lei nº 11.892/2008, que instituiu a Rede Federal de Educação Profissional, Científica e Tecnológica.

O IFTO é uma instituição de educação superior, básica e profissional, pluricurricular e multicampi (Reitoria, *campus*, *campus* avançado e polos de educação a distância), especializada na oferta de educação profissional e tecnológica nas diferentes modalidades de ensino, com base na conjugação de conhecimentos técnicos e tecnológicos com as suas práticas pedagógicas/andragógicas.

A instituição é vinculada ao Ministério da Educação (MEC) e possui natureza jurídica de autarquia, sendo detentora de autonomia administrativa, patrimonial, financeira, didático-pedagógica e disciplinar.

Com a oferta de cursos no ensino médio-técnico e superior, além de pós-graduações *lato sensu*, nas modalidades presencial e a distância, o IFTO atende todas as microrregiões do Tocantins. São mais de 60 cursos regulares ofertados.

O IFTO atua com uma estrutura multicampi. Possui os *Campi* de Araguaína, Araguatins, Formoso do Araguaia, Lagoa da Confusão, Pedro Afonso, Colinas do Tocantins, Dianópolis, Gurupi, Palmas, Paraíso do Tocantins e Porto Nacional. Entre os seus objetivos está promover a educação profissional e tecnológica de excelência e impulsionar o desenvolvimento sustentável das regiões.

Em todos os *campi*, vários são os sistemas de informação utilizados para tratamento de dados pessoais. Entretanto, vale destacar que o modelo atual não é centralizado, dificultando assim que o titular dos dados possa manipulá-lo, como determina a lei.

Desenvolvimento

Sendo um tema novo, pesquisas acadêmicas nesse campo de estudo ainda são iniciais. Nosso trabalho visa contribuir com o setor público frente aos novos desafios da implantação e implementação por parte dos gestores da LGPD, viabilizando e motivando reflexões acerca do tema. É válido ressaltar que, além desse hiato acadêmico, há também o vínculo profissional que o autor possui com o tema — de um lado, constitui o trabalho acadêmico para o curso de Direito; por outro, o viés técnico.

Analisar o tema de forma genérica é um desafio para qualquer pesquisador, no entanto, ao se refinar o tema, analisando um ponto específico, pode-se contribuir para um melhor ajustamento, fornecendo uma visão geral no aspecto técnico-legal.

Pelo exposto, esta pesquisa justifica-se por uma questão norteadora, em que analisou-se, ao longo da trajetória da pesquisa, a adaptação do Instituto Federal do Tocantins à Nova Lei Geral de Proteção de Dados Pessoais e quais as implicações em relação a essas adequações.

A efetividade da Lei

Rousseau (2007, p. 54), em *O contrato social*, sua obra clássica, diz que as leis são propriamente condições para a associação civil. Dessa forma, o povo submetido às leis deve ser

seu autor, compete apenas aos que se associam regular as condições da sociedade. Em resumo, a lei é criada para atos futuros e pessoas incertas.

É importante ressaltar o múnus público no qual o administrador público está embrenhado: o dever imposto ao sistema público e privado no qual orbita a lei imposta faz com que mudanças sejam necessárias para adequar-se à realidade da norma jurídica em abstrato ao cotidiano do serviço público.

Nessa seara, os representantes da vontade geral, mesmo sabendo da dificuldade do *compliance* e sua adequação ao cotidiano das empresas, a norma nasce para regular de forma geral e genérica a proteção de dados pessoais — esse é o princípio da legalidade —, corroborando nessa perspectiva Montesquieu (2009, p. 35), que, em sua clássica obra, *O espírito das leis*, nos chama à atenção para uma pequena reflexão: “aquele que manda executar as leis sente que ele próprio a elas está submetido, e o peso delas terá que suportar”. O que incube ao administrador público é entender e aplicar o espírito da lei.

Na prática, o governo deverá garantir a segurança dos dados pessoais tratados e comunicar incidentes de segurança da informação ao órgão regulador, a Agência Nacional de Proteção de Dados – ANPD, conforme previsto no capítulo IX da Lei nº 13.709, de 14 de agosto de 2018, que tem por objetivo regular esse novo setor.

Inicialmente, para que o IFTO ou qualquer outro órgão do setor público ou privado alcançasse o mínimo de efetividade no enquadramento da norma, seria primeiramente necessário realizar um estudo detalhado dos sistemas utilizados, suas bases de dados, políticas de acesso e uso, ou seja, o mapeamento completo do tratamento desses dados. Além disso, é cediço que vários *campi* coletam dados através de formulários, utilizando o Google Forms ou o Microsoft Forms.

Assim, levaria tempo e esforço razoável a realização desse levantamento, necessitando de uma equipe técnica constituída para esse fim, visto que muitos usuários utilizam esses sistemas apenas uma vez, com fito de coleta de dados para algo bem específico. Esses formulários se enquadram no quesito tratamento de dados, mas não há como disponibilizar o acesso a esses dados coletados para um determinado usuário, pois sua forma de coleta é simples e não há como realizar a gerência desses dados coletados.

É importante ressaltar que dentro da estrutura interna do órgão há troca de informações entre o órgão central, nesse caso, a Reitoria, e os *campi*. Assim, a fim de melhorar o *compliance*, é necessário elaborar políticas de proteção de dados, adaptando os documentos e sistemas computacionais internos e externos à ISO/IEC 27001, a norma internacional que trata de gestão da segurança da informação.

A realização de um ciclo de treinamento com todos os servidores do IFTO sobre a LGPD e principalmente com o corpo administrativo, que lida diretamente com o tratamento de dados, sintetizando as dúvidas e adaptando a realidade à norma.

Em síntese, a tarefa não é fácil. Devido à sua complexidade, apenas a *vacatio legis* de dois anos não foi suficiente para essa mudança cultural no que tange à coleta, armazenamento e manipulação de dados pessoais, para que se torne de pleno efeito a norma posta.

Hipóteses de transgressão

No vocabulário jurídico, transgredir significa infringir uma norma social, uma lei. Immanuel Kant, em *Fundamentos da metafísica dos costumes*, traz uma breve síntese do que vem a ser um mandamento legal: “Pois só a lei traz consigo o conceito de necessidade incondicionada, objetiva e, em consequência, universalmente válida, e mandamentos são leis a que se deve obediência, isto é, a que se deve cumprir mesmo contra inclinação”. (KANT, 2011, p. 47).

Corroborando Kant, Reale (1999, p. 201) afirma que “a vida jurídica é uma luta incessante contra a transgressão legal e o delito, para salvaguarda de bens e de valores”.

Volviendo-se especificamente às regras implantadas pela Lei nº 13.709/18, temos que, com a edição dessa norma, a adequação às novas regras será em parte difícil de ser concretizada, haja vista que boa parte dos sistemas de informação utilizados pela instituição é mantida por terceiros, isso sem contar a diversa variedade de dados que são coletados através de formulários.

A implementação da LGPD no IFTO ou em qualquer outra instituição de ensino é inadiável, visto que diariamente lidam com dados sensíveis dos alunos. É importante ressaltar que a lei veio a abranger o tratamento de dados tanto no meio físico quanto no meio eletrônico.

A hipótese de transgressão mais comum é o vazamento de dados pessoais, para toda e qualquer instituição de ensino. Insta destacar que o IFTO trata inúmeros dados sensíveis previstos na legislação, como cor, raça, convicção religiosa e dados referente a saúde. Em se tratando de menores de idade, é um agravante. Procedimentos internos deverão ser revistos no tratamento dos dados pessoais, tendo seu maior impacto na gestão dos diversos bancos de dados de cadastro, pois, ainda que tenham sido coletados antes da vigência da lei, enquadrar-se-ão nas hipóteses previstas na LGPD.

Enfim, os exemplos são diversos no que afeta a transgressão da lei: incidentes de segurança, ausência da privacidade, vazamento de informação, formulários para coleta de dados sem o correto controle de acesso — essas são algumas hipóteses de transgressão da LGPD no âmbito institucional.

Referencial teórico

Vivemos em um momento de transformação no modelo de negócio, estamos passando pela transição desse modelo físico para o virtual. A exemplo disso temos os órgãos públicos conectados dando transparência à população, possibilitando o acesso a documentos e serviços que integram o controle social.

Segundo Aguiar (2018), a combinação entre automatização e aprendizado de máquinas possibilita a “liberação” de dados dos sistemas que os criam e mantêm. Novas tecnologias dão às organizações novas formas de gerenciar inter-relações, armazenamento e segurança de dados empresariais.

Assim, com os novos sistemas de coleta e armazenamento de dados mudando do mundo físico para o virtual, de fácil disponibilização e acesso, nasce a importância da tutela jurídica dos dados pessoais, necessitando assim de uma regulamentação.

Partindo de uma definição de dados como um material que serve a um propósito de análise, e de informação como o que resulta dessa análise interpretativa de dados, e, tendo em vista que os dados têm uma certa potencialidade de fornecer uma grande e diversa quantidade de informações, primordialmente, não são os dados em si que devem ser protegidos, mas os sujeitos a quem tais dados se referem (Souza, 2018).

Por conseguinte, é importante definir o conceito de dados e informação. Para o sistema de informação, dado é qualquer elemento identificado em sua forma bruta que por si só não conduz a uma compreensão de determinado fato ou situação. Por outro lado, a informação é o dado sistematizado e organizado de forma a transmitir significado e compreensão dentro de um determinado contexto.

Para o nosso trabalho é importante destacar o que se define como dados pessoais. Segundo a SERASA (2019), empresa responsável por análises e informações de crédito e apoio ao negócio, o conceito de dado pessoal é bastante abrangente, sendo definido como a “informação relacionada a pessoa identificada ou identificável”. Isso quer dizer que um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa natural por trás do dado.

Um aspecto a ser considerado na Lei Geral de Proteção de Dados Pessoais é a busca da definição do que vem a ser dado pessoal. Essa definição é essencial para definir o alcance da lei, uma vez que seu alcance ou restrição deve vir de acordo com a norma. Vejamos o que nos trazem a lei e suas definições.

Quadro 1 – Definição de dados pessoais

LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011.
Art. 4º Para os efeitos desta Lei, considera-se: [...] IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
DECRETO Nº 8.771, DE 11 DE MAIO DE 2016
Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa;
LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.
Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
LEI Nº 13.853, DE 8 DE JULHO DE 2019
Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Fonte: Elaborado pelos autores (2020)

Constata-se que as definições advindas das normas mostradas no Quadro 1, no que diz respeito às definições de dado pessoal ou informações pessoais, são firmes em mostrar que se trata da identificação de uma pessoa natural identificada ou identificável.

Mas, afinal, o que realmente a norma disciplina como objetivo de proteção, segundo o art. 3º da Lei 13.709/18, aplica-se a tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica de direito público ou privado.

A própria norma deixou claro, em seu art. 5º, X, o que vem a ser tratamento de dado:

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

Exemplificando, a LGPD prevê o tratamento em todo o ciclo de vida dos dados. No glossário do Serviço Federal de Processamento de Dados – SERPRO (2018), a maior empresa pública de prestação de serviços em tecnologia da informação do Brasil, segundo a Câmara dos Deputados (2018), divide-se o tratamento de dados em vários pontos, a saber:

Quadro 2 – Tratamento de dados

acesso	acesso - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados
armazenamento	ação ou resultado de manter ou conservar em repositório um dado
arquivamento	ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência
avaliação	ato ou efeito de calcular valor sobre um ou mais dados
classificação	maneira de ordenar os dados conforme algum critério estabelecido
coleta	recolhimento de dados com finalidade específica

comunicação	transmitir informações pertinentes a políticas de ação sobre os dados
controle	ação ou poder de regular, determinar ou monitorar as ações sobre o dado
difusão	ato ou efeito de divulgação, propagação, multiplicação dos dados
distribuição	ato ou efeito de dispor de dados de acordo com algum critério estabelecido
eliminação	ato ou efeito de excluir ou destruir dado do repositório
extração	ato de copiar ou retirar dados do repositório em que se encontrava
modificação	ato ou efeito de alteração do dado
processamento	ato ou efeito de processar dados
produção	criação de bens e de serviços a partir do tratamento de dados
recepção	ato de receber os dados ao final da transmissão
reprodução	reprodução - cópia de dado preexistente obtido por meio de qualquer processo
transferência	mudança de dados de uma área de armazenamento para outra, ou para terceiro
transmissão	movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.
utilização	ato ou efeito do aproveitamento dos dados

Fonte: SERPRO (2019)

Em resumo, o tratamento de dados é toda e qualquer manipulação em dados, desde a coleta, com finalidade específica, armazenamento, por meio físico ou digital, em sistemas de banco de dados complexos ou uma simples planilha eletrônica, até sua eliminação.

Sendo o poder público o maior mantenedor de dados, a LGPD reservou o Capítulo IV para tratar exclusivamente do tratamento de dados no setor público, conforme assim disposto:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: [...] (BRASIL, 2011).

Colocar o setor público no escopo da LGPD é obrigá-lo a realizar adequações em questões de segurança as quais muitas vezes são negligenciadas. O governo, em todas as suas esferas de atuação, tem se tornado cada vez mais digital. Para tanto, vários são os setores que possibilitam acesso a dados por meio eletrônico, bem como transações bancárias, históricos de consumo do setor elétrico, telecomunicações, água e energia, o que em separado não diz muito, mas uma análise mais profunda desses dados poderá formar padrões de consumo.

Em resumo, esses dados, tratados de forma a gerar *insights* estratégicos, podem, de certo modo, extrair informações valiosas com um alto percentual de acerto utilizando técnicas de análise de dados. Por essa razão, os dados armazenados no setor público de consumo do setor público são valiosos. Como exemplo disso, podemos ver o recente julgado sobre vazamento de dados e suas implicações no mundo jurídico. Veja-se o recurso inominado (RI 0047026-37.2019.8.21.9000) a seguir:

“Recurso Inominado. Ação de indenização por danos materiais e morais. Fraude perpetrada. Vazamento de informações cadastrais e negociais do autor. Danos morais não configurados. Ausência de previsão legal para impor danos morais com caráter meramente punitivo. [...] 1. Narra o autor que em razão do vazamento de seus dados sigilosos, foi levado a cair em uma fraude. 2. Sentença que julgou parcialmente

procedente a ação, a fim de condenar o réu ao pagamento da quantia de R\$ 814,02 a título de indenização por danos materiais. 3. Analisando o conjunto probatório, verifica-se que o autor não demonstrou de forma cabal o abalo moral sofrido, a fim de comprovar fato constitutivo de seu direito, ônus que lhe incumbia, nos termos do art. 373, I, do CPC. 4. Com efeito, o autor tinha um acordo com a ré, recuperadora de créditos, sendo que foi contatado por fraudadores, que dispunham dos dados do acordo e, mediante fraude, fizeram-no pagar uma parcela indevida. 5. O presente recurso cinge-se a postular danos morais por conta do manejo de dados fraudulentos. 6. *In casu*, não se trata de situação excepcional capaz de determinar a incidência de danos morais, porque tal se daria apenas em caráter punitivo. 7. Desta forma, entende-se que não restaram caracterizados os danos morais, já que a parte autora não comprovou que tivesse tido abalo em algum dos atributos da sua personalidade, em função da situação vivenciada, tratando-se de mero aborrecimento, o que não é capaz de gerar dano moral indenizável, salvo em situações excepcionais.” TJ/RS, RI 0047026-37.2019.8.21.9000, Rel. Des. Fábio Vieira Heerdt, 3ª Turma Recursal Cível, j. 26/09/2019.

Com isso, verifica-se, no âmbito da jurisprudência pátria acerca da matéria, a relevante observação no que afeta o vazamento de dados, colocando em evidência os atores envolvidos no processo, quais sejam: o titular, o controlador e o operador.

Art. 5º Para os fins desta Lei, considera-se:

V - **titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - **controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - **operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - **encarregado**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)

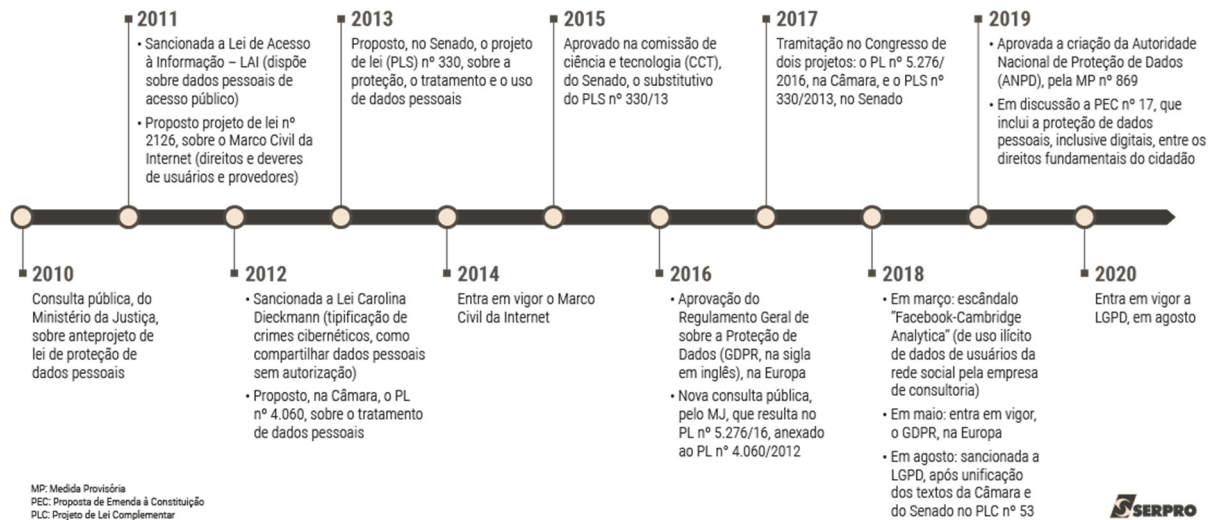
IX - **agentes de tratamento**: o controlador e o operador; (BRASIL, 2018), (grifos nossos).

Quanto ao titular, pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, ao qual a legislação estabelece os direitos elencados no art. 18 da referida lei. Já o operador poderá ser pessoa natural ou jurídica, ou seja, uma empresa especializada e que trabalha com *compliance digital*, de forma que usa-se um conjunto de boas práticas de segurança em sua política de tratamento de dados.

Nesse escopo também teremos a figura do controlador, ao qual compete as decisões referentes ao tratamento dos dados pessoais. No setor público será o órgão público, a exemplo do IFTO, que mantém base de dados de seus servidores, alunos, terceirizados, empregados públicos, enquadrando-se nessa definição.

O encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. A Autoridade Nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. O Brasil há tempos não mede esforços para regular o setor de tecnologia no que concerne a tratamento de dados, que é amplo e a cada dia surgem novas demandas tecnológicas.

Figura 1 – Linha do tempo da proteção de dados pessoais



Fonte: SERPRO (2019)⁴

Como podemos ver na Figura 2, desde a primeira consulta pública a respeito do tema, já se vão mais de 10 anos desde a criação da Lei de Acesso a Informação (LAI), que deu maior transparência aos gastos públicos, até chegarmos à atual LGPD, que entrou em vigor em agosto de 2020.

A regulação do setor é fruto da dinâmica social em que vivemos. Parafraseando Negroponte (1995, p. 19), temos sido capazes de digitalizar diferentes tipos de informação, como áudio e vídeo, reduzindo-os também a uns e zeros. Esses zeros e uns, os bits, não têm cor, tamanho ou peso e são capazes de viajar à velocidade da luz, passando de um simples dado, insignificante e irrelevante, quando separados, mas, quando juntos, de valor inestimável para pessoas, empresas e o governo.

Materiais e métodos

Para a realização da pesquisa, empregou-se como procedimento metodológico, primeiramente, a revisão da literatura, para a identificação de produções acadêmicas sobre o tema “gestão de dados pessoais no poder público”, objetivando assim uma maior compreensão em termos de pesquisas já desenvolvidas. Para Salvador (1981), o levantamento bibliográfico é o conjunto de indicações precisas e minuciosas que permitem a identificação de publicações já realizadas sobre o tema, através da sistematização e análise dos resultados.

Trata-se de uma pesquisa qualitativa que objetiva proporcionar uma visão geral do tema quanto à existência sobre a conformidade ou não da norma no Instituto Federal do Tocantins, por meio de coleta e análise dos dados disponíveis nos sistemas institucionais.

O tipo de pesquisa será predominantemente qualitativo, com fundamento na análise técnica. O método de abordagem será o dedutivo, partindo dos dados particulares constatados para se chegar a uma verdade geral, utilizando-se dos dados coletados como forma de instruir e orientar as atividades de pesquisa, as quais se valerão também da compilação de literatura e legislação correlata, jurisprudência e trabalhos publicados.

⁴ SERPRO. **Serpro e LGPD: segurança e inovação.** Linha do tempo da proteção de dados pessoais e da Lei Geral de Proteção de Dados Pessoais, no Brasil. Disponível em: <https://www.serpro.gov.br/lgpd/menu/arquivos/linha-do-tempo-1/view>. Acesso em: 23 abr. 2020.

Considerando que a LGPD é a norma geral que regulamenta a proteção de dados no Brasil, já em vigor, parece-nos coerente uma abordagem exploratória, visto que, para uma melhor adequação da norma, sobrevirão diversas alterações legislativas.

Além disso, nos ensina Korkmaz (2019) que a LGPD é estruturada a partir de um modelo regulatório construído na experiência europeia, de forma que a sua efetivação dependerá de uma conformidade futura da realidade brasileira.

Importante ressaltar que, conforme Gil (2002), o método exploratório nos proporciona uma visão geral do problema proposto, como uma etapa fundamental para o desenvolvimento de uma investigação mais ampla, gerando assim futuras perguntas de pesquisa.

Pesquisa bibliográfica

Para fundamentação e desenvolvimento do trabalho, foram analisados estudos já publicados nas bases de dados descritas no Quadro 3 que se assemelham à temática escolhida. No entanto, devido à recente norma, foi realizada uma busca sistemática no período de 2014 a junho de 2020. Os descritores utilizados tiveram como objetivo encontrar trabalhos relacionados ao tema com maior relevância. O Quadro 3 mostra as bases de dados escolhidas para a realização do trabalho e seus endereços eletrônicos.

Quadro 3 – Bases de dados utilizadas na realização das buscas

BASE DE DADOS PESQUISADA	ENDEREÇO PESQUISADO
1. Portal de Periódicos da Capes – <i>Cafe</i>	http://www.periodicos.capes.gov.br/
2. Banco Digital de Teses e Dissertações	http://bdtd.ibict.br/
3. Google Scholar	https://scholar.google.com.br

Fonte: Elaborado pelos autores (2020)

Definição dos termos de busca

Foram levantados estudos que tiveram relação direta com o tema proposto. Dessa forma, para realização das buscas nas bases de dados e refinamento da pesquisa, utilizamos as palavras-chaves definidas no idioma português do Brasil, utilizando os seguintes termos combinados:

1. “Poder Público” e ““lei geral de proteção de dados””;
2. “Poder Público” e “LGPD”;
3. “Proteção de dados” e “Dados sensíveis”.

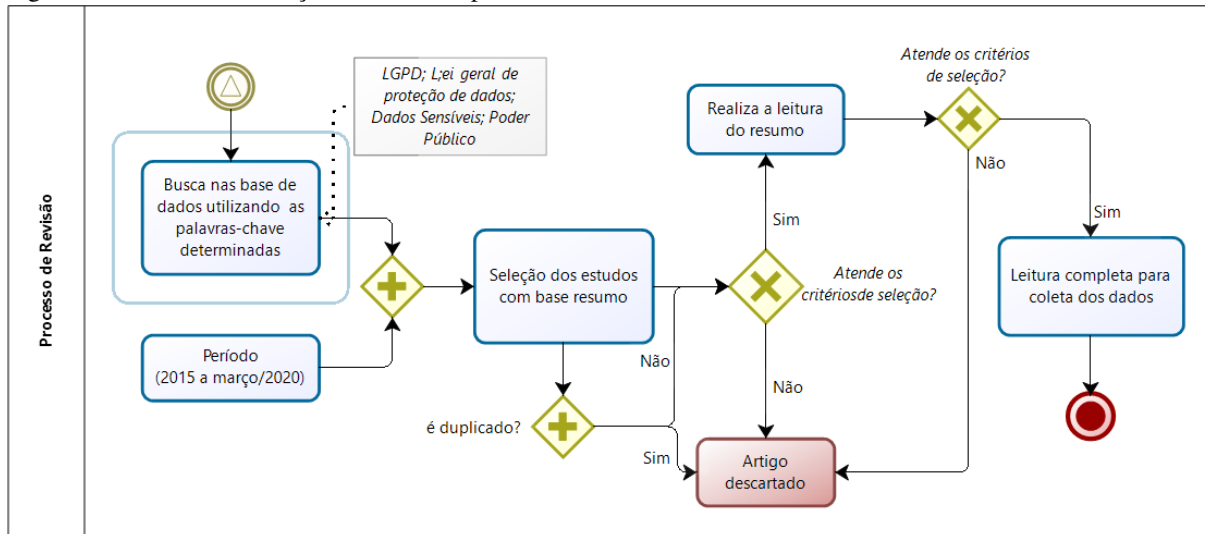
Em posterior análise, para seleção dos artigos, foram escolhidos apenas aqueles que tinham relação com o tema apresentado, uma vez que, sendo interesse da investigação, foram selecionados apenas estudos que mostram a correlação direta com objeto apresentado.

Crítérios de inclusão e exclusão

Os procedimentos metodológicos utilizados na busca e seleção dos artigos publicados foram a escolha dos periódicos a serem analisados, a língua e o período. Dessa forma, a língua escolhida foi a língua portuguesa, visto que a LGPD é uma lei nacional com implicações internacionais.

A busca foi entre 2015 e março de 2020. Ao realizar o mesmo procedimento nas bases de dados observou-se, através de uma leitura dos resumos, que há repetidas publicações dos mesmos trabalhos em diferentes revistas — os quais não foram incluídos. A Figura 3 mostra o processo de seleção e avaliação dos estudos contemplados nesta pesquisa.

Figura 2 – Processo de seleção dos estudos para revisão da literatura



Fonte: Elaborado pelos autores (2020)

Para o critério de exclusão do estudo bibliográfico, levou-se em consideração apenas trabalhos que tratam de forma integral ou relativa o tema. Após a busca pelos trabalhos nas bases de dados mencionadas, foram selecionados aqueles com maior relevância, seguindo as etapas propostas na Figura 3.

Ademais, com o intento de selecionar os mais relevantes, primeiramente realizamos uma leitura breve para identificação do trabalho, tendo assim uma ideia geral do tema trabalhado no artigo. Além disso, com a leitura dos resumos, selecionamos os potenciais trabalhos a serem posteriormente analisados com maior critério, excluindo os que não atendiam aos critérios pré-estabelecidos.

Atendidos os critérios, passamos à leitura dos objetivos, com o propósito de verificar a proposta do trabalho apresentado, uma vez que nele se resume sua ideia central. Por conseguinte, foi realizada a leitura dos resultados da pesquisa. Em razão disso, foram selecionados os artigos que tiveram como objetivo relacioná-los, de modo que foi delineado o referido estudo.

No entanto, vale destacar que não foram encontrados trabalhos que tratam da análise técnica da LGPD no setor público. Os artigos encontrados trouxeram-nos uma visão geral dos trabalhos a respeito do tema. Na Figura 3 foi demonstrado, por meio de infográfico, o caminho percorrido e a seleção dos estudos contemplados para a pesquisa.

Após a leitura dos artigos previamente selecionados, apenas 5 tiveram relação direta com o tema proposto. É importante frisar que a base de dados do Google Scholar indexa outras bases de dados, obtendo vários estudos repetidos.

Objetivando automatizar o processo de descarte de artigos repetidos, utilizamos o programa Zotero (2019), um gerenciador de referências bibliográficas em que podemos importar as buscas nas bases de dados das bases de selecionadas no formato *bibtex*. Com isso, automatizamos o processo de exclusão de artigos duplicados através do botão “*deteção duplicada*”.

Dessa forma, diminuimos significativamente o trabalho de análise de artigos. Todos os artigos que trouxeram o contexto serviço público e proteção de dados pela nova LGPD foram analisados.

Dado o exposto e analisando de forma sintética os artigos, verifica-se uma inclinação por parte dos pesquisadores a projetar suas pesquisas não na parte técnica, e sim em discussões acerca das definições dos termos e comparação com a *General Data Protect Regulation – GDPR*.

Resultados e discussões

Dos atores envolvidos no processo

Para melhor entendimento da legislação, é importante ressaltar e destacar a ação de cada ator envolvido no processo. Dessa forma, podemos analisar sob a ótica técnica como será o comportamento dos envolvidos.

O titular dos dados

Segundo o art. 5º, V, pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Semelhante ao *GDPR* na União Europeia, a LGPD assegura ao titular dos dados pessoais o direito de obter do controlador, a qualquer momento e mediante requisição, o que se segue.

Confirmação e acesso aos dados

É garantido o direito de confirmação da existência de tratamento e, por consequência, o de acessar todos os dados pessoais de sua titularidade que estão sendo coletados pelo controlador, fornecendo assim informações de existência de tratamento ou o acesso aos dados pessoais imediatamente ou no prazo de 15 dias contados da data do requerimento do titular.

Segundo dados extraídos da Plataforma Nilo Peçanha (2019), o IFTO possui cerca de 14.000 (quatorze mil) alunos matriculados, distribuídos espacialmente nos *campi* (Tabela 1).

Tabela 1 – Quantidade de estudantes no IFTO em 2018

Unidade	Percentual	Matrículas
Araguaína	7,9%	1.124
Araguatins	13,8%	1.970
Colinas do Tocantins	6,1%	863
Dianópolis	5,0%	709
Formoso do Araguaia	1,6%	228
Gurupi	5,4%	770
Lagoa da Confusão	3,1%	438
Palmas	36,3%	5.190
Paraíso do Tocantins	9,7%	1.377
Porto Nacional	8,3%	1.180
Pedro Afonso	2,8%	415
Total		14.264

Fonte: Plataforma Nilo Peçanha (2019)

Para que seja atendida a exigência de confirmação de dados prevista em lei, todos os sistemas da instituição deverão ser integrados em um *Data Warehouse* (DW), com o intuito de centralizar os dados. Na Tabela 1 é mostrada a quantidade de alunos distribuídos por *campi* no IFTO.

Os dados pessoais devem ser armazenados em formato que favoreça o direito de acesso, bem como o da portabilidade dos dados pessoais, cabendo ao controlador viabilizar mecanismos que garantam o fornecimento por meio eletrônico ou sob a forma impressa.

Retificação

Os titulares possuem o direito de corrigir os dados incompletos, inexatos ou desatualizados que lhes digam respeito. Segundo informações retiradas do portal do IFTO (2020), existem inúmeros sistemas descentralizados que tratam de dados pessoais e muitas vezes o dado cadastral de um sistema não corresponde ao dado de outros — dessa forma, a confirmação dos dados pelo titular se dá por todos os sistemas informatizados da instituição, excluindo-se a coleta de dados através de formulários web, como o Microsoft Forms e o Google

Forms, gerando uma infinidade de sistemas de coleta, cadastro e manipulação de dados pessoais.

Restrição de tratamento

Os titulares possuem o direito de restringir o tratamento de dados pessoais por meio da recusa em fornecer o consentimento.

Cancelamento ou exclusão

Os dados desnecessários, após feito o tratamento, devem ser excluídos, mas como realizar essa exclusão de forma que não se atinja diretamente os dados necessários para o armazenamento de informações? A exclusão da qual a lei trata não é apenas a mudança de status como ativo ou inativo, e sim a exclusão definitiva do banco de dados.

Encarregado pelo tratamento dos dados pessoais

O *Data Protection Officer (DPO)* é o controlador responsável pelo tratamento. De modo geral, esse novo profissional é um especialista em proteção de dados que fará o papel de monitoramento para garantir que eles estejam em *compliance* com regras e boas práticas do setor. Ele será o intermediário entre a empresa e o titular dos dados.

Em consulta direta, hoje, não há nenhum servidor com esse perfil. Da mesma forma o art. 37 da GDPR a figura do DPO é necessária sempre que o tratamento for feito por órgãos ou autoridades públicas (com exceção de tribunais), a empresa lida com dados especiais e sensíveis como informações sobre etnia, religião e condenações penais ou faça um monitoramento em larga escala.

Em linhas gerais, o encarregado pela proteção de dados dentro da instituição deverá ser um profissional de formação e conhecimentos múltiplos, expertise em legislação de proteção de dados, tecnologia da informação e gestão de processos, desempenhando assim um papel muito importante dentro da organização e estando apto para agir em prol do cumprimento da lei.

Considerações finais

Em suma, no presente artigo foi proposta uma análise qualitativa que tem como objetivo a compreensão, descrição e geração de hipótese sobre o tema proposto. Diante da universalidade de dados pessoais existentes no Instituto Federal do Tocantins e das várias formas de tratamento, desde inserção em sistemas complexos até um simples formulário impresso, surgem novos desafios, especialmente para os analistas de Tecnologia da Informação, que deverão se adequar aos ditames da Lei nº 13.709, de 2018.

Nesse sentido, vale ressaltar a importância do presente estudo, que tem o intuito de refletir sobre o tema prático em um ambiente real, para adequação à nova legislação por parte não só das pessoas jurídicas de direito privado, mas também das pessoas jurídicas de direito público.

Inicialmente, apresentou-se a ideia do *compliance digital* como meio de garantir a correta aplicação da lei.

Em seguida, restou demonstrada a complexidade na manipulação e adequação à nova lei pelos sistemas informatizados do IFTO, visto que eles não estão interligados, uma vez que cada sistema utiliza seu próprio banco de dados. Assim, caso o titular dos dados peça alguma alteração, deverá este, formulando o pedido, indicar em quais sistemas excluí-los, tornando assim ineficaz o seu pedido diante da manipulação dos dados de forma compartilhada.

Por fim, analisando a figura do *Data Protection Officer*, que recai sobre o encarregado, pessoa física que será responsável pela proteção dos dados pessoais, atuando também como intermediador entre o controlador, os titulares e a autoridade nacional de proteção de dados (ANPD), instituída pela Lei nº 13.853, de 2019.

Muitos desafios irão surgir ao longo da adequação do fato à norma. Empresas manipulam diariamente dados e registros, contudo os primeiros passos para a efetiva proteção se mostram perceptíveis à medida que as instituições públicas e privadas buscam o melhor entendimento

da lei, aplicando-a em seu ambiente corporativo. Com a vigência da norma, a atuação para a conformidade deve ser imediata.

Referências

AGUIAR, V. **A transformação digital no governo e órgãos públicos**. Disponível em: <https://transformacaodigital.com/setor-publico/transformacao-digital-no-governo-e-orgaos-publicos>. Acesso em: 23 abr. 2020.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 28 abr. 2017.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 23 abr. 2020.

BRASIL. **Ministério da Educação**. Plataforma Nilo Peçanha. Disponível em: https://public.tableau.com/views/PNP2019V_II/Capa?:embed=y&:showVizHome=no. Acesso em: 26 abr. 2020.

BRASIL. **Instituto Federal do Tocantins**. Sistemas Acadêmicos Administrativos. Disponível em: <http://www.ifto.edu.br/aceso-a-sistemas/aceso-sistemas>. Acesso em: 26 abr. 2020.

CÂMARA DOS DEPUTADOS. **Representação brasileira no parlamento do Mercosul**. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-mistas/cpcms/siglas/siglar2/s/SERPRO.html>. Acesso em: 25 abr. 2020.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

IBGE. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal**. Brasil: IBGE, 2018. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 23 abr. 2020.

KANT, I. **Fundamentação da metafísica dos costumes e outros escritos**. Tradução: Leopoldo Holzbach. São Paulo: Martin Claret, 2011.

KORKMAZ, M. R. D. C. R. **Dados sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**. Juiz de Fora/MG: Fundação Getúlio Vargas, 2019.

MONTESQUIEU. **Do espírito das leis**. Tradução: Jean Melville. São Paulo: Martin Claret, 2009.

NEGROPONTE, N. **A vida digital**. Tradução: Sérgio Tellaroli. São Paulo: Cia. das Letras, 1995.

NUNES, M. G. **Jurimetria: como a estatística pode reinventar o Direito**. São Paulo: Revista dos Tribunais, 2016. v. 2.

REALE, M. **Filosofia do direito**. São Paulo: Editora Saraiva, 1999.

ROUSSEAU, J. J. **O contrato social**. Porto Alegre: LP&M Pocket, 2007.

SALVADOR, Â. D. **Métodos e técnicas de pesquisa bibliográfica, elaboração e relatório de estudos científicos**. 9. ed. Porto Alegre: Sulina, 1981.

SERASA. **LGPD e a definição de dados pessoais - Serasa Experian**. Disponível em: <https://www.serasaexperian.com.br/blog/lgpd-e-a-definicao-de-dados-pessoais>. Acesso em: 23 abr. 2020.

SERPRO. **Glossário LGPD**. Lei Geral de Proteção de Dados Pessoais. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd>. Acesso em: 23 abr. 2020.

SOUZA, T. P. V. de. **A proteção de dados pessoais como direito fundamental e a (in)civilidade do uso de cookies**. Uberlândia/MG: Universidade Federal de Uberlândia, 2018.

UNIÃO EUROPEIA. **General Data Protection Regulation**. Disponível em: <https://gdpr.algolia.com/pt/gdpr-article-37>. Acesso em: 26 abr. 2020.

ZOTERO.ORG. **Zotero. Your personal research assistant**. [s.l: s.n.].