

LEI GERAL DE PROTEÇÃO DE DADOS-(LGPD) NAS INSTITUIÇÕES DE ENSINO: DESAFIOS FORMATIVOS PARA SUA APLICAÇÃO E GESTÃO.

Israel Ferreira Candiani¹
Otaviano José Pereira²

RESUMO: O presente artigo trata-se da Lei Geral de Proteção de Dados Pessoais (LGPD) nas Instituições de Ensino (IEs), faz uma análise dos impactos da lei nas IEs e os desafios da mesma para se adequar à legislação. A partir de uma breve trajetória da evolução tecnológica/dos meios de comunicação/disseminação da informação, o objetivo é realizar uma descrição dos aspectos gerais da Lei 13.709/2018, trazendo para tanto as definições, conceitos e classificações existente na legislação, bem como apresentar os princípios que estruturam a LGPD. Abordamos as limitações legais ao tratamento de dados, considerando principalmente a irrecusável necessidade do consentimento para o tratamento. Sob o prisma de uma formação específica de seus quadros, focamos, de modo especial, os chamados “dados sensíveis” e as sanções decorrentes do descumprimento da legislação. Por fim será apresentado os caminhos indicados para as IEs se adequarem as exigências legais, e os desafios, passíveis de avanços e impasses, indicados para absorção de suas práticas às Tecnologias Digitais de Informação e Comunicação (TDIC), sob constantes ameaças, mesmo num cenário global de continua e irreversível evolução.

Palavra Chave: Lei Geral de Proteção de Dados (LGPD); Instituições de Ensino; Absorção da Lei;

ABSTRACT: This article deals with the General Law for the Protection of Personal Data (LGPD) in Educational Institutions (IEs), it analyzes the impacts of the law on IEs and its challenges in adapting to the legislation. Based on a brief trajectory of technological evolution/media of communication/dissemination of information, the objective is to provide a description of the general aspects of Law 13,709/2018, bringing to both the definitions, concepts and classifications existing in the legislation, as well as presenting the principles that structure the LGPD. We address the legal limitations to data processing,

¹ pós graduação lato sensu Direito Civil, Mestrando do Curso de Mestrado profissional em Educação Tecnológica do Instituto Federal de Educação, Ciência e Tecnologia do Instituto Federal do Triângulo Mineiro – Campus Uberaba, com endereço sito a Rua Olegário Maciel, nº. 117, Centro, Uberaba/MG, e-mail: contato@candiani.com.br, telefone: (34) 99694-2076.

² pós doutorado em Educação pela Uninove de São Paulo, professor do Curso de Mestrado e Doutorado profissional em Educação Tecnológica do Instituto Federal de Educação, Ciência e Tecnologia do Instituto Federal do Triângulo Mineiro – Campus Uberaba, com endereço sito a Rua Itapagipe, nº. 241, Bairro Jardim Induberaba, Uberaba/MG, e-mail: otavianopereira@iftm.edu.br, telefone: (34) 99298-1461.

mainly considering the irrefutable need for consent for processing. From the perspective of specific training of its staff, we focus, in particular, on the so-called “sensitive data” and the sanctions resulting from non-compliance with legislation. Finally, the paths indicated for IEs to adapt to legal requirements will be presented, and the challenges, subject to advances and impasses, indicated for absorbing their practices into Digital Information and Communication Technologies (TDIC), under constant threats, even in a scenario global environment of continuous and irreversible evolution.

Keyword: General Data Protection Law (LGPD); Educational Institutions; Absorption of the Law.

1. Introdução

O presente artigo foi retirado de um dos capítulos da pesquisa de mestrado intitulada *A Lei Geral de Proteção de Dados Pessoais no Instituto Federal do Triângulo Mineiro: uma Análise de sua Implantação*, em desenvolvimento junto ao Programa de Pós-Graduação em Educação Tecnológica - curso de Mestrado Profissional em Educação Tecnológica do Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro.

A Lei Geral de Proteção de Dados representa um importante marco regulatório, especialmente para as Instituições de Ensino (IEs), que lidam diariamente com uma grande quantidade de dados pessoais de alunos, prestadores de serviços e terceirizados. Com a entrada em vigor da Lei 13.709/2018, muitos são os desafios e oportunidades que essas instituições precisam, para ajustar suas práticas e políticas as garantias de direitos constitucionais das pessoas em conformidade com a nova legislação.

A proteção dos direitos fundamentais de privacidade e autodeterminação das pessoas é um dos objetivos da legislação, que impõe nova regras para coleta, armazenamento, processamento e compartilhamento de informações que possam identificar um indivíduo. No contexto das IEs, esses dados podem incluir informações acadêmicas, registros de desempenho, informações de contato e até mesmo dados sensíveis, como origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político, e que necessitam de maior proteção.

A necessidade de implementação de medidas robustas de segurança da informação e privacidade de dados deve incluir adoção de medidas substanciais de proteção de dados, designação de um encarregado de proteção de dados, responsável por garantir o

cumprimento da legislação, e a realização de avaliações de impacto à privacidade, entre outras ações.

O conhecimento das bases legais para o tratamento de dados pessoais, passou a ser uma das obrigações das IEs, que devem revisar seus processos de tratamento de dados para garantir que estejam em conformidade com a legislação. Mais do que cumprir as determinações da legislação, a importante tarefa da educação e conscientização sobre a proteção de dados entre membros da comunidade escolar também tornou-se um desafio a ser superado pelas IEs, o que inclui a formação de professores, alunos e funcionários sobre seus direitos e responsabilidades.

Em suma, a LGPD estabeleceu desafios significativos para as IEs, sendo necessário cada vez mais fortalecer práticas de proteção de dados e promover uma cultura de privacidade e segurança em seus ambientes educacionais. Neste contexto,

2. A Lei Geral de Proteção de Dados - (LGPD): Percepções iniciais.

O século XXI vem sendo marcado por profundas e céleres mudanças propiciadas pelas Tecnologias Digitais de Informação e Comunicação (TDIC). Com a popularização dos computadores, *smartphones*, e maior acesso às tecnologias digitais e à internet, permitiu-se que um grande volume de informações chegasse a um número cada vez maior de pessoas, causando significativas mudanças comportamentais, baseada em redes de comunicação.

Nesse sentido, Castells (2013, p.11) destaca que uma nova “economia de dados” seria como um “sistema nervoso eletrônico”. A Internet seria o meio de comunicação e processamento de informações em que todos os dados pessoais e econômicos, coletados, tratados e armazenados são interligados em uma rede de forma organizacional. Por sua vez Levy (1999, p. 54), ao discorrer sobre a capacidade de processamento automático de todos esses dados, do alto grau de precisão, da celeridade e da escala quantitativa possível, destaca que: “(...) nenhum outro processo a não ser o processamento digital reúne, ao mesmo tempo, essas quatro qualidades. A digitalização permite o controle das informações e das mensagens ‘bit a bit’, número binário a número binário, e isso na velocidade de cálculo de computadores”.

Em razão dessa rápida evolução tecnológica e da globalização, foram criados desafios em matéria de proteção de dados pessoais, passando-se a exigir uma legislação

rigorosa quanto a proteção dos dados pessoais, reforçando a segurança jurídica dos cidadãos. Desse modo, A Lei 13.709, foi criada em 14 de agosto de 2018, denominada de Lei Geral de Proteção de Dados Pessoais, cuja sigla foi fixada como LGPD, com a finalidade de disciplinar a proteção de dados pessoais em âmbito nacional. Nesse sentido é importante destacar que a LGPD serve apenas para o tratamento de dados pessoais, ou seja, não atinge diretamente os dados de pessoas jurídicas. A referida lei é um marco legislativo brasileiro que modificou significativamente a forma de coleta e tratamento indiscriminado de dados pessoais, coletando e tratando o que somente é o necessário. A LGPD traz consigo os fundamentos que enfatizam a proteção de direitos e garantias da pessoa natural, tais como: autodeterminação informativa, à liberdade de expressão, o respeito à privacidade, à inviolabilidade da intimidade, ao desenvolvimento econômico e tecnológico, além da livre iniciativa e respeito aos direitos humanos (Brasil, 2018).

A legislação é eufônica aos direitos fundamentais e à proteção da dignidade da pessoa humana, e sofreu grande influência do Regulamento Geral de Proteção de Dados da União Europeia (UE). É importante ressaltar ainda, que a LGPD é aplicada também a dados em estado físico ou *offline*, migrando ou não esses dados para o meio digital. Em síntese a Lei visa proteção dos titulares de dados pessoais sobre documentos armazenados em nuvens, servidores, em memória de computadores, ou mesmo em *pen drives*, além de fichas físicas, livros de atas, formulários, prontuários em papel. Visa a proteção de direitos e garantias fundamentais da pessoa natural, através da harmonização e atualização de conceitos de modo a diminuir riscos e estabelecer regras para o tratamento dos dados pessoais.

Com advento da Lei Geral de Proteção de Dados, rompemos um paradigma de coleta e tratamento indiscriminado de dados pessoais (dados que identifiquem a pessoa natural), para um modelo que passará a coletar e tratar somente os dados necessários. O artigo 2º da LGPD, estabelece um conjunto de princípios que deverão ser observados para o tratamento dos dados, sendo um deles o respeito à privacidade, bem jurídico cujo a inviolabilidade é elevada ao *status* de direito fundamental por nossa Constituição Federal, visam inibir qualquer ato capaz de afetar a intimidade e a vida privada da pessoa natural. Ferraz Júnior (2005, p. 28), entende como privacidade:

a vida privada compõe, porém, um conjunto de situações que, usualmente são informadas sem constrangimento. São dados que, embora privativos – como nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc., condicionam o intercâmbio humano em sociedade, pois

constituem elementos de identificação que tornam a comunicação possível, corrente e segura.

Assim, a utilização de dados pessoais, análises de comportamentos em redes sociais, registros de acesso a aplicações, informações de geolocalização ou de consumo de energia podem estabelecer parâmetros para identificar e traçar perfis de indivíduos, seja para direcionar produtos e serviços, validar uma contratação profissional, ou mesmo para identificar um potencial criminoso, por essa razão o que o indivíduo faz ou pode fazer com dados pessoais de terceiros, deve ser determinado pelo titular de seus dados, e passou a ter proteção à privacidade como fundamento da LGPD (MALDONADO, 2022, p. 29).

Estabelece ainda em seu inciso II do artigo 2º, o princípio da autodeterminação informativa, que é o direito de controle pessoal sobre o trânsito de dados relativo ao próprio titular. A autodeterminação informativa constitui-se no “direito do indivíduo controlar seus dados pessoais”, no sentido de “poder escolher o que será feito de suas informações” (Bioni, 2014).

A ausência de controle e autoridade sobre os seus próprios dados pessoais, no caso de o indivíduo não conseguir identificar quais informações suas são utilizadas, para quais propósitos, e como isso interfere e influencia em sua vida, demonstra o tolhimento da autodeterminação informativa.

O inciso III do artigo 2º da LGPD, estabelece o princípio da liberdade de expressão, de informação, de comunicação e de opinião. Tais liberdades descritas no artigo estão inseridas na Constituição Federal e categorizadas como direitos e garantias fundamentais, prevista no artigo 5º, inciso IX da CF/88. Cumpre destacar que a liberdade de expressão, de informação, de comunicação e de opinião não são direitos absolutos, e são vedados o anonimato justamente para responsabilizar aqueles que extrapolam em sua liberdade (liberalidade desregrada e irresponsável) e causem danos à imagem, à honra, à intimidade e à privacidade de outrem, garantindo-se o direito de resposta e indenização no caso de abusos.

Importante ressaltar que a LGPD excluiu a sua aplicabilidade ao tratamento realizado para fins exclusivamente jornalísticos e artísticos ou acadêmico; veda o tratamento de dados para fins discriminatórios; exige qualidade, finalidade, adequação, necessidade e transparência no tratamento; determina que o tratamento de dados pessoais, cujo acesso é público, considere a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização (MALDONADO, 2022. p. 38).

O inciso IV do referido artigo, trata da inviolabilidade da intimidade, da honra e da imagem, e da mesma forma como a LGPD enfatiza como fundamento a privacidade, também o faz com a inviolabilidade da intimidade, da honra e da imagem, direitos igualmente fundamentais, previsto no artigo 5º, inciso X da CF/88.

Segundo Costa Júnior (2007, p. 49), o direito a intimidade é o direito de o indivíduo não ser arrastado para a ribalta contra sua vontade, de subtrair-se à publicidade e de permanecer recolhido na sua intimidade, o direito de manter olhos e ouvidos indiscretos afastados dessa esfera de serviço, bem como o direito de impedir a divulgação de palavras, escritos e atos realizados nessa esfera de intimidade. A honra pode ser afetada, quando dados pessoais são utilizados sem o consentimento, inclusive ofendendo o livre desenvolvimento da personalidade da pessoa natural. Por sua vez, o direito à imagem faculta ao titular de dados pessoais proibir sua utilização de forma abusiva, enfim contrária à lei.

A Declaração Universal de Direitos Humanos, em seu artigo 12, estabelece que ninguém sofrerá intromissões arbitrárias na sua vida privada, respaldando todas as pessoas de ataques ou intromissões com a proteção da lei. Atento a tal normativa, o Conselho de Direitos Humanos da ONU publicou dispositivo para a promoção, proteção e fruição dos direitos humanos na *internet*, dispondo sobre a importância da privacidade *on-line*, como elemento fundamental para realização do direito de liberdade de expressão e de ter opiniões sem interferência. (ONU, 2016)³. Zanon (2013, p. 156) defende inclusive, que a proteção de dados pessoais seja uma nova espécie de direitos da personalidade, assegurando, à pessoa, a dignidade, a paridade, a não discriminação e a liberdade.

A LGPD, ao fundamentar sua existência no livre desenvolvimento da personalidade e na dignidade da pessoa humana, demonstra sua preocupação na proteção da personalidade do ser humano, haja vista que a proteção de informações íntimas do titular atinge o seu direito da personalidade. Nesse sentido é importante frisar, que o tratamento de informações de cunho íntimo e pessoal, associado à personalidade de um indivíduo específico é capaz de identificar e revelar muito a respeito desse indivíduo, a ponto de impactar seu próprio exercício de cidadania (Maldonado, 2022).

³ ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Human Rights Council. Thirty-second session. Disponível em: [http://www.un.org/ga/search/view_doc.asp?symbol=A/HCR/32L.20]. Acesso em: 20.01.2023.

2.1 Definições, Conceitos e Classificações – um olhar mais

O artigo 5º cumpre o importante papel de especificação dos termos utilizados na norma, deixando expresso o que é considerado dados pessoais, como “[...] a proteção de dados é uma das facetas do conceito maior de privacidade, e que brotou e floresceu por decorrência do desenvolvimento tecnológico ocorrido nas últimas décadas.” (MALDONADO, 2018, p. 86-87). Enfim, através da proteção de dados pessoais as garantias que antes relacionavam-se com o direito à privacidade, são tratados de forma mais específica, em razão da manipulação de dados. Por essa razão podemos destacar que o direito a proteção de dados surge como instrumento de proteção da pessoa titular das informações pessoais.

A legislação cuidou de definir os dados pessoais como sendo toda “informação relacionada a pessoa natural, identificada ou identificável”, conforme estabelece o artigo 5º, inciso I da Lei. Em outras palavras, significa dizer que dados pessoais são todas aquelas informações que se referem a determinada pessoa viva, capaz de ser identificada.

Por sua vez, o inciso II do mesmo artigo, definiu os dados sensíveis, que são dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Cumpre informar que a motivação da conceituação dessa categoria especial de dados pessoais é fruto da necessidade de estabelecer obrigações diferenciadas ao tratamento de dados sensíveis, o que efetivamente foi feito no artigo 11 da LGPD, conforme será demonstrado, a seguir:

O inciso VI do artigo 5º traz a definição de controlador, sendo a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Enquanto o inciso VII, traz a definição de operador, sendo pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Por sua vez, o inciso VIII, estabelece a definição de encarregado, como sendo a 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). Neste caso, a LGPD impõe maior peso jurídico ao controlador, pois o mesmo é responsável pela tomada de decisões sobre o tratamento de dados pessoais, bem como pelo cumprimento da LGPD na prática.

O encarregado se apresenta como a figura do *Data Protection Officer (DPO)*, e tem como finalidade ser o responsável por aceitar reclamações e comunicações dos titulares dos dados, prestar esclarecimentos e adotar providências; receber comunicações da ANPD e adotar providências; orientar os controladores e funcionários a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, o que torna suas funções muito mais amplas do que simplesmente estabelecer a comunicação entre o controlador, os titulares dos dados e a ANPD.

A referida Lei ainda trouxe importante esclarecimento em seu inciso X, artigo 5º, ao definir o que é tratamento, como sendo 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. Sendo assim verifica-se que a definição de tratamento é ampla, engloba desde a coleta até as inúmeras possibilidades de manuseio dos dados, independente do meio utilizado. A importância dessa abrangência de definição do termo tratamento se dá, em razão do dever do agente que realiza o tratamento manter o registro de todas suas operações.

A definição de consentimento, também foi informado no inciso XII, sendo a manifestação livre, informada e inequívoca, pela qual o titular concorda com o tratamento de seus dados pessoais para sua finalidade determinada. Importante ressaltar que o consentimento para tratamento de dados sensíveis, de crianças ou para transferências internacionais, além de livre, informado e inequívoco, para uma finalidade determinada, deverá ser realizado de forma específica e em destaque. Ademais o consentimento deverá ser para finalidade específica, sendo nulas as autorizações genéricas para o tratamento de dados. Sendo assim, a autorização deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade, e nos casos em que o tratamento seja para fins múltiplos, deverá ser conferido consentimento para cada um desses fins.

No que diz respeito ao relatório de impacto à proteção de dados pessoais, o inciso XVII, define o mesmo como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos. Segundo a doutrina de Vainzof (2022), o relatório de impacto à proteção de dados (RIPD) é um instrumento, de responsabilidade do controlador, objetivando anotação de Cadernos da Fucamp, v.27, p.31-52/2024

qualquer tratamento de dado pessoal, que possa gerar riscos às liberdades civis e aos direitos fundamentais, contendo a descrição dos processos para diminuir os riscos e responsabilidades. Tendo em vista que o RIPD tem como finalidade a mitigação dos riscos no momento do tratamento dos dados pessoais, o mesmo deverá ser realizado antes do início do tratamento dos dados, estabelecendo uma visão completa de todo o ciclo de vida dos dados, dessa forma o controlador poderá observar com clareza os principais fatores que poderão impactar nas liberdades civis e direitos fundamentais, podendo, a partir de então, implementar medidas e mecanismos que demonstrem o cumprimento da LGPD.

Por fim, a definição de autoridade nacional, prevista inciso XIX, como órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

2.2 Princípios da LGPD

Os princípios que estruturam a LGPD, estabelecidos no artigo 6^a, são as bases para que se evite o cometimento de infrações, dos quais destacamos: a finalidade, necessidade, consentimento, transparência, segurança e responsabilidade e prestação de contas, conforme exposto na Figura 1 a seguir:

Figura 1 - Princípios que estruturam a LGPD



Fonte: Elaborada pelos autores (2024)

Cadernos da Fucamp, v.27, p.31-52/2024

Os três primeiros princípios dispostos na LGPD (finalidade, adequação e necessidade), formam um conjunto que garante a transparência, o fundamento dessa norma jurídica, determinante para o respeito da proteção dos direitos fundamentais de liberdade, de privacidade e de livre desenvolvimento da pessoa natural. O quadro 1 a seguir traz de forma didática o significado de cada princípio:

Quadro 1 – Princípios dispostos na LGPD

Finalidade	Garante ao titular dos dados a fronteira de legalidade do tratamento de seus dados, delimitando os propósitos do tratamento para mitigar o risco de uso indevido e sem o conhecimento e consentimento do titular dos dados.
Necessidade	Tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
Adequação	Estabelece que o tratamento de dados pessoais seja realizado somente quando houver compatibilidade com as finalidades informadas ao titular.
Consentimento	O tratamento de dados pessoais deve ser realizado com consentimento do titular dos dados, exceto nos casos previstos em lei.
Transparência	As organizações públicas e privadas, devem informar de forma clara e transparente como os dados serão tratados, incluindo quem terá acesso a eles e para quais finalidades.
Segurança	Devem ser adotadas medidas técnicas e organizacionais para proteger os dados pessoais contra acesso não autorizados, perda ou destruição.
Responsabilidade e Prestação de contas	As IES devem ser capazes de comprovar que estão em conformidade com a LGPD e serem responsabilizadas por eventuais violações.

Fonte: Elaborado pelos autores (2024)

Por meio destes princípios, o objetivo da legislação é garantir os direitos fundamentais, como privacidade e o livre desenvolvimento da personalidade, através do tratamento ético, responsável e seguro dos dados pessoais. O titular dos dados deverá ter ampla informação sobre o tratamento dos seus dados para que consiga verificar a legalidade, a legitimidade e a segurança do tratamento de seus dados, respeitado o propósito, adequação e a necessidade. Como medida de segurança, a legislação estabelece os seguintes critérios:

- (a) utilização de medidas técnicas e administrativas qualificadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou

difusão; (b) prevenção, compreendendo a adoção de medidas para prevenir a ocorrência de danos por causa do tratamento de dados pessoais; (c) não discriminação, que sustenta que o tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos. A segurança dos dados pessoais é um dos princípios de grande relevância na legislação, devendo os agentes de tratamento utilizar as medidas técnicas e administrativas aptas a proteger os dados pessoais de eventuais violações, tanto em eventos dolosos, como em acidentes (BRASIL, 2018).

As medidas de segurança para proteção dos dados devem ser observadas desde a fase de concepção do produto ou serviço até a sua execução, através de sistemas estruturados de forma a atender aos requisitos de segurança, padrões de boas práticas e de governança. O tratamento irregular dos dados, decorrente da violação da sua segurança, fará com que o controlador ou o operador que deixar de adotar as medidas de segurança, previstas e adequadas, respondam pelos danos decorrentes da violação da segurança.

É aconselhável que os agentes mantenham um registro contendo a descrição das medidas técnicas e organizativas de segurança dos dados. A ANPD (Autoridade Nacional de Proteção de Dados) poderá dispor sobre os padrões técnicos mínimos, de acordo com a natureza dos dados (dados pessoais e dados sensíveis), as características específicas do tratamento e o estado atual da tecnologia.

É importante destacar que a legislação indica que os agentes poderão estipular regras de boas práticas e de governança criando condições de organização, funcionamento, procedimento, padrões técnicos, obrigações específicas para os envolvidos no tratamento, ações educativas, mecanismos internos de supervisão e mitigação dos riscos relacionados ao tratamento dos dados pessoais. Nesse sentido, o controlador poderá implementar programa de governança em privacidade e demonstrar a efetividade de seu programa de governança, quando solicitado pela ANPD ou outra entidade responsável por promover o cumprimento de boas práticas ou código de conduta.

2.3 Limitações legais ao Tratamento de Dados

A legislação estabelece as hipóteses legais que legitimam o tratamento dos dados pessoais, as quais são taxativas e estabelecidas no artigo 7º e seus incisos. A licitude e regular exercício da atividade de tratamento de dados pessoais supõe o atendimento das hipóteses previstas nos incisos do artigo 7 da LGPD. O quadro 2 a seguir torna mais pedagógico o entendimento das hipóteses legais de limitação ao tratamento de dados:

Quadro 2 – Hipóteses Legais de Limitação ao Tratamento de Dados

1) Consentimento	a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
2) Cumprimento de Obrigação Legal	atividade destinada ao cumprimento de dever imposto ao controlador. Não cabe ao agente de tratamento, discricionariedade sobre o atendimento do dever. Existindo dever decorrente de norma válida, é de observância obrigatória.
3) Tratamento pela Administração Pública	poderá realizar o uso compartilhado de dados, desde que tal se dê com o estrito objetivo de executar políticas públicas expressamente previstas em lei
4) Estudos por órgãos de pesquisa	o tratamento de dados para realização de estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. Estando-se diante de órgão de pesquisa, a entidade pública ou privada poderá realizar, com o uso de dados pessoais, pesquisas de caráter histórico, tecnológico ou estatístico.
5) Execução de Contratos	Trata-se de hipótese em que os dados pessoais necessariamente precisem ser tratados para a execução de obrigações contratuais firmadas
6) Exercício regular de direito	hipótese legal que autoriza o tratamento de dados pessoais, conforme previsão do artigo 7º, inciso VI da Lei. Assim, nas situações em que se entender que os dados pessoais servirão como elemento para exercício de direitos em demandas em geral, eles poderão ser armazenados enquanto subsistir tal necessidade.
7) Proteção da vida ou incolumidade física	relacionadas a questões graves, e que ponham em risco a vida ou a integridade física do titular.
8) Finalidade exclusiva de saúde	os profissionais da área de saúde e as entidades que são membros do SNVS (Sistema Nacional de Vigilância Sanitária) poderão se valer dessa base legal para o tratamento de dados, desde que com o objetivo específico de tutela da saúde, sendo vedado qualquer outro uso que desvirtue essa finalidade.
9) Legítimo Interesse	conceito que exige redobrar cuidados na determinação de seu significado, em vista da natureza da atividade do controlador e a finalidade do tratamento.
10) Finalidade de proteção de Crédito	trata-se de hipótese de licitude, prevista no artigo 7º, inciso X, da LGPD, visa informações sobre adimplência e inadimplência, sobre determinado titular podendo ser utilizadas, a fim de se tomar decisão acerca da concessão ou não de crédito.

Fonte: Elaborado pelos autores (2024).

Vale ressaltar que o consentimento informado será atingido quando, antes da coleta dos dados pessoais, os titulares forem amplamente informados acerca do ciclo de vida do tratamento dos seus dados, respeitando assim os princípios da finalidade e transparência,

devendo ser apresentado de forma clara e ostensiva as informações para os titulares dos dados, quais sejam:

(i) finalidade específica do tratamento; (ii) forma e duração do tratamento; (iii) identificação, (iv) informações de contato do controlador; (v) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (vi) responsabilidade dos agentes que realizarão tratamento e direitos do titular (BRASIL, 2018).

O Parágrafo 4º do artigo 7º, trata da hipótese de dispensa da exigência do consentimento previsto no inciso I do artigo, na hipótese de o próprio usuário tornar público seus dados pessoais, não sendo necessário a obtenção do seu consentimento para tratamento dos mesmos dados, sendo fundamental observar que, mesmo nessa hipótese, não será totalmente livre a utilização dos dados que somente poderá ocorrer se resguardados os direitos e os princípios previstos em lei.

Quanto aos interesses legítimos do controlador ou de terceiros, ou simplesmente “legítimo interesse” previsto no artigo 7, inciso IX, deve ser observado com cautela o uso de interesse legítimos como base legal para o tratamento de dados a ser realizado por terceiros, que não diretamente o controlador, diante dessa indefinição que existe na legislação.

2.4 Consentimento para Tratamento de Dados Pessoais

A legislação em seu artigo 8º indica que o consentimento, previsto no artigo 7º, inciso I da Lei, deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Segundo Cots e Oliveira (2018, p. 115);

[...] o importante é que a manifestação da vontade seja: (i) preservada e inequívoca; (ii) inteligível, isto é, deve ser compreensível caso precise ser comprovada, especialmente perante as esferas judiciais; e (iii) esteja adequadamente atrelada aos termos do tratamento de dados, vale afirmar que é necessário comprovar que determinado consentimento se deu sobre determinado tratamento.

O consentimento fornecido por escrito, deve ainda constar de cláusula destacada das demais cláusulas contratuais. Referida determinação judicial, contida no parágrafo 1º, do artigo 8º tem o intuito de alcançar maior transparência.

De acordo com parágrafo 2º, do artigo 8º da LGPD, caberá ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na legislação. Em razão desse parágrafo, é fundamental que se utilize somente mecanismos de

Cadernos da Fucamp, v.27, p.31-52/2024

coleta de consentimento que permitam a geração de evidências de sua obtenção, bem como que referidas evidências fiquem armazenadas durante o período de tratamento dos dados, independentemente da finalidade. Nesse sentido, Tepedino e Teffé (2020, p. 98), ponderam:

[...] não se deve confundir a validade do consentimento, especialmente de seus requisitos formais, com a sua prova. Todavia, é aconselhável ao agente de tratamento que tenha registrado em documento escrito o consentimento dado pelo titular. Isso porque, como dispõe o artigo 8º, §2º, da LGPD, caberá ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na lei, o que é influência direta do princípio da responsabilização e prestação de contas.

Em eventual solicitação da Autoridade Nacional de Proteção de Dados, das evidências quanto ao cumprimento da exigência de obtenção de consentimento válido, é importante que o controlador tenha se atentado quanto a obrigação de armazenamento da evidência da obtenção do consentimento, sob pena de graves consequências estabelecidas no artigo 52 da LGPD.

O parágrafo 3º, do artigo 8º, da LGPD, veda o tratamento de dados pessoais mediante vício de consentimento. Ou seja, diante da ausência de base legal que autorize o tratamento de dados, e tendo o consentimento qualquer vício, o tratamento não poderá ser realizado. Cordeiro (2020, p. 174) destaca que “[...] a manifestação de vontade não será válida se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado”

Por sua vez, o Código Civil Brasileiro, estabelece de forma cristalina as hipóteses de vício de consentimento, que podem decorrer de:

(i) erro, conforme artigo 138 e 139 do CC/02; (ii) dolo, conforme artigo 145 do CC/02; (iii) coação, conforme artigo 151 do CC/02; (iv) estado de perigo, conforme artigo 156 do CC/02; (v) lesão, conforme artigo 157 do CC/02; (vi) fraude contra credores, conforme artigo 158 do CC/02; e, (vii) simulação, conforme 167 do CC/02. (BRASIL, 2002).

A legislação estabelece ainda, em seu parágrafo 4º, artigo 8º, que o consentimento deverá referir-se às finalidades determinadas, e às autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas. Sendo assim o documento formulado para colher o consentimento do titular dos dados deverá ser elaborado de forma a demonstrar transparência, finalidade especificada e inequívoca, conforme exige a LGPD.

Portanto, é importante ressaltar que qualquer circunstância que altere o modo, a duração, a forma ou qualquer outra característica do tratamento para o qual se consentiu

Cadernos da Fucamp, v.27, p.31-52/2024

deverá ser prontamente informado ao titular dos dados, que poderá revogar o consentimento em razão da alteração na finalidade subjacente à manifestação de vontade, conforme previsão expressa do artigo 8º, §6º da LGPD.

2.5 Dados Pessoais Sensíveis

Já o tratamento de dados pessoais sensíveis, previstos na Lei, seção II, orienta que os dados pessoais sensíveis somente poderão ser utilizados nas hipóteses que legitimam o tratamento de ambas as modalidades de dados pessoais, que são semelhantes.

O artigo 5º, inciso II, da LGPD estabelece um rol exemplificativo de dados sensíveis, que são dados que versam sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos.

As hipóteses tratadas no artigo 11 da LGPD para o tratamento de dados pessoais sensíveis são semelhantes às hipóteses estabelecidas no artigo 7º da LGPD, ou seja:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) Cumprimento de obrigação legal ou regulatória pelo controlador; b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) Proteção da vida ou da incolumidade física do titular ou de terceiros; f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (BRASIL, 2018).

Uma leitura comparativa do artigo 11 da Lei mantém várias bases já previstas no artigo 7º, para o tratamento de dados pessoais, deixando de fora do tratamento de dados sensíveis as hipóteses de atendimento aos interesses legítimos do controlador ou de terceiros e de proteção do crédito.

Deve ser destacado que todos os cuidados previstos no artigo 11 da LGPD para o tratamento dos dados deve ser aplicado de forma mais intensa e rigorosa, já que para os dados sensíveis se espera um padrão ainda mais rigoroso de proteção técnica e jurídica.

Com relação ao tratamento de dados pessoais de crianças e de adolescentes, a legislação estabeleceu em seu artigo 14, que o tratamento de dados pessoais somente deverá ser realizado se levar em conta o melhor interesse, e a necessidade de proteção integral, conforme disciplina a legislação pertinente (Estatuto da Criança e do Adolescente – ECA). Nesse sentido ainda, o parágrafo primeiro do artigo 14 da LGPD estabelece que o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal. Por sua vez, o parágrafo segundo do artigo 14, da LGPD, estabelece que os dados tratados em seu parágrafo primeiro, deverão manter pública a informação sobre os tipos de dados coletados pelos controladores, a forma de sua utilização e os procedimentos para o exercício dos direitos estabelecidos no artigo 18 da LGPD.

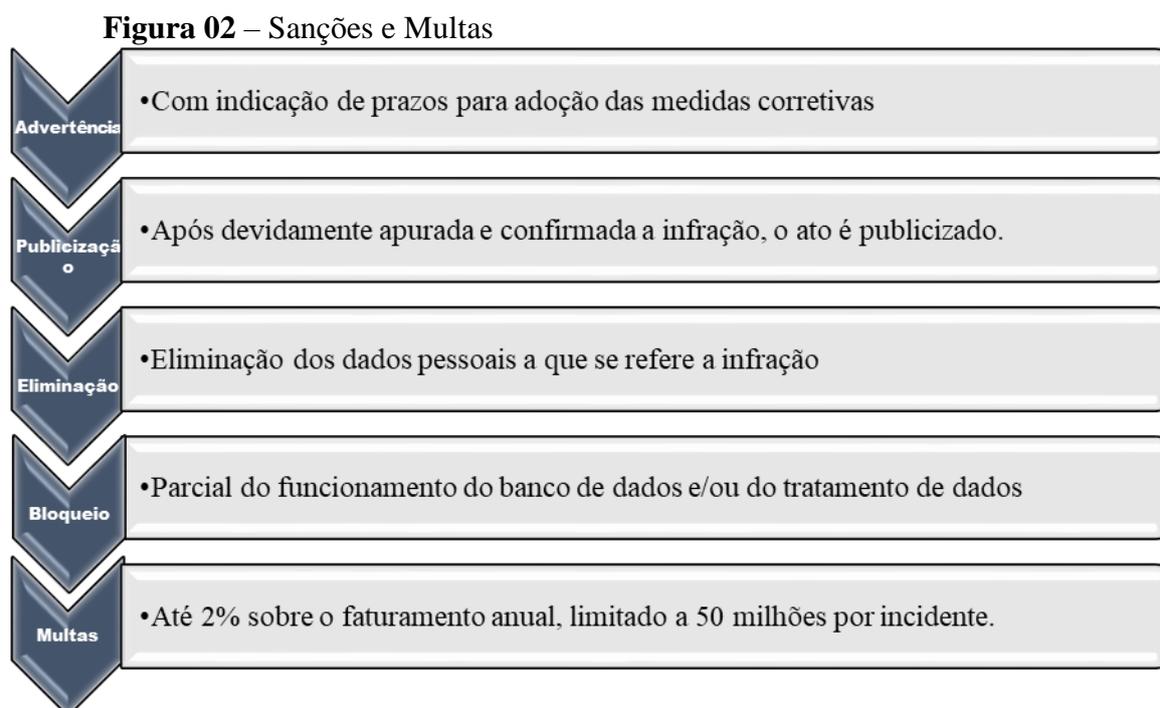
O consentimento específico que a legislação estabelece deve ser entendido como o detalhamento sobre o ciclo de vida do tratamento dos dados pessoais, com referência objetiva e clara sobre todos os limites e as finalidades em relação a quais dados serão tratados. Já o consentimento em destaque, estabelecido pela legislação, será alcançado quando for clara a identificação do usuário em relação ao tratamento que será realizado com seus dados pessoais. Nesse sentido, um documento que contemple outras autorizações, deverá ser realçado o trecho referente ao tratamento de dados pessoais em relação às demais partes do texto.

A legislação determina, ainda, que os dados pessoais de crianças só poderão ser coletados sem consentimento a que se refere o parágrafo primeiro, quando a coleta for necessária para contatar os pais ou responsável legal, utilizados uma única vez e sem armazenamento.

2.6 Sanções Administrativas

A LGPD, apresenta em sua íntegra sanções para possíveis violações, em face de uma proposta rebuscada por regras estabelecidas em meio a um conjunto de aspectos disciplinares de autoridade nacional, orientados pela fixação de hipóteses para a coleta dos dados, com categorias que detalham minuciosamente as especiais condições para o tratamento, o armazenamento e os direitos dos titulares de dados sensíveis, além de circunscrever os ditames para o armazenamento dos dados de empresas (com suas obrigações), de indivíduos e de seus segmentos.

A legislação em toda a sua extensão, estruturada pela Art. 1º ao Art. 65º, apresenta um conjunto de sanções como forma de se assegurar possíveis violações das regras previstas no capítulo VIII, seção I, Art. 52, que estabelecem, desde advertência, a multas, bloqueios dos dados, eliminação dos dados, até a suspensão parcial do funcionamento do banco de dados, suspensão parcial do exercício da atividade de tratamento dos dados e a proibição parcial ou total do exercício de atividades relacionadas a tratamento dos mesmos. Figura 02 a seguir ilustra melhor as sanções e multas:



Fonte: Elaborado pelos autores (2024).

Nos possíveis casos de violação das regras previstas no Art. 52º, merece destaque a advertência, cabendo nessa medida a correção de ações, o que não deixa de ser menos importante a previsão de “[...] *bloqueio dos dados pessoais a que se refere a infração até a sua regularização*” (Brasil, 2018), previsto no inciso V do mesmo artigo, além da proibição total e/ou parcial de atividades voltadas ao tratamento do banco de dados, caso as ações apresentem relação específica com irregularidades.

3. Os Impactos da Lei Geral de Proteção de Dados nas Instituições de Ensino

A LGPD, pela sua natureza, considera um direito de todo cidadão a proteção de dados pessoais, sensíveis ou não. Pela normativas dadas pela Lei, as IEs brasileiras, Cadernos da Fucamp, v.27, p.31-52/2024

independentemente da sua área de atuação e/ou porte, deverão atender aos aclames da Lei, bem como seguir orientações para a coleta, tratamento, processamento e compartilhamento de dados.

O uso de dados nas escolas públicas e privadas sempre foi frequente na prestação de serviços. A coleta e armazenamento de informações, tais como endereço do aluno, condições de saúde e boletim de avaliação fazem parte dos processos de uma instituição de ensino. Não é segredo que as IEs, assim como outras organizações, públicas e privadas, estão passando por um processo de digitalização, adotando, para tanto, novas tecnologias da informação e comunicação em seu cotidiano laborativo. Isto implica em afirmar que as ferramentas tecnológicas devem ser adaptadas às propostas pedagógicas, derivadas de discussões avaliativas internas sobre as condições e o alcance de seu uso, bem como aos processos administrativos, - neste caso diretamente relacionados à Lei em foco -, e a comunicação sobre suas potencialidades e efeitos com a comunidade escolar e seu entorno.

A propósito, segundo Borelli (2020) as IEs preparadas para os desafios propostas pela era digital, são aquelas que conseguem perceber os riscos e prejuízos do compartilhamento ou o vazamento de dados pessoais, e quão invasivos e violador podem ser esses episódios. Os riscos de eventuais vazamentos de dados e os prejuízos vão além da violação de direitos fundamentais, como direito à privacidade, situação que pode se agravar, sobretudo quando se tratar de dados forem sensíveis, dado a importância de referidos dados.

Não há dúvidas que os processos internos de coleta, tratamento e compartilhamento de dados pessoais e sensíveis realizado pelas IEs, deverão observar os preceitos estabelecidos na LGPD, e para tanto torna-se imprescindível a adequação, organizacional e tecnológica, dessas instituições, encarregadas de zelar pela segurança de alunos, professor, servidores e da própria comunidade do entorno, mormente as famílias. Há de considerar que a LGPD veio por sinal até mesmo um pouco tardia, se considerarmos o potencial tanto benéfico quanto maléfico da revolução comunicacional que vivemos, de modo irreversível, em toda a humanidade.⁴

Os desafios não são poucos. Diante do que foi estabelecido pela legislação, será necessário que as IEs realizem uma análise das condições atuais da instituição, sua própria

⁴ A título de exemplo citamos o caso da Escola Base de São Paulo, ocorrido em 1.994, em que os proprietários foram acusados injustamente de abuso sexual. Disponível em: https://pt.wikipedia.org/wiki/Caso_Escola_Base. Acesso em 18 abril 2024. Cadernos da Fucamp, v.27, p.31-52/2024

capacidade (expertise de formação e gestão) de absorção da Lei e elabore um plano de ação para garantir o cumprimento das demandas da legislação vigente, desde 2018.

Há de considerar que os tempos (atuais) são outros e requerem um desdobramento muito diferenciado e vigilante à sua aplicação, sob o permanente risco de vazamento de informações, notadamente de dados pessoais invioláveis. A LGPD, normatiza no art. 6º, inciso VI, a questão da transparência como” [...] garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento” (BRASIL, 2018), de dados pelo fato de que as IEs coletam periodicamente um grande volume de dados pessoais regulares, o que faz com que a LGPD, exija que seja dada uma maior transparência no tratamento de dados pessoais.

Contudo, mais do que a transparência no tratamento dos dados, será necessário ter o consentimento informado e específico dos titulares dos dados, antes de coletar e processar suas informações, sob uma verdadeira cruzada contra acessos não autorizados, vazamentos e perdas. Vale dizer, a premente necessidade de incluir criptografia, controle de acesso, auditorias de segurança e protocolos de segurança dos dados.

Juntamente às medidas de segurança as IEs deverão se adequar as inovações organizacionais, através da designação de um encarregado da proteção de dados (diuturnamente em cada IEs), que deverá supervisionar a conformidade com a LGPD, e atuar como ponto de contato para questões relacionadas a privacidade, chamado de *Data Protection Officer* – cuja sigla é DPO.

Não se trata, entretanto, de uma centralidade no apuro técnico e tecnológico no campo da revolução comunicacional (Sociedade em rede) de nosso tempo. Mais do que a formação para lidar com todo este aparato, tão novo ainda na idade da própria humanidade, há de considerar uma poderosa “cultura emergente”, no que o pensador da comunicação Pierre-Lévy chama de Cibercultura - num inédito e desmedido “campo” em aberto: Ciberespaço. A propósito, outro autor, entre nós, Crespo (2021), destaca que o maior desafio imposto às IEs, consiste na mudança cultural da instituição e de seus servidores ante a necessidade de tratamento de dados pessoais, já que a transformação cultural em qualquer instituição, demanda tempo e investimento em divulgação, treinamento e sensibilidade da comunidade envolvida.

No investimento em formação e trato com suas práticas, as IEs, ao constituir os membros responsáveis pela captação de dados gerais, dados sensíveis e/ou informações, como *conditio sine qua non*, deverão receber treinamento específico e atualização das

normativas previstas na Lei Geral de Proteção de Dados - LGPD, bem como conhecer suas implicações na internalização dessa poderosa cultura da rede. O quadro 3 abaixo, sintetiza os principais cuidados inerentes à aplicação da Lei nas IEs.

Quadro 3 – Cuidados inerentes à Aplicação da Lei

a) Garantia dos direitos dos titulares dos dados	As IEs devem criar mecanismos para que os titulares dos dados possam exercer seus direitos, de acesso, correção, exclusão e revogação de consentimento para o tratamento de seus dados.
b) Criação de políticas de retenção de dados	Também está nas obrigações da IEs para cumprirem as determinações da LGPD, sendo necessário definir prazos para que os dados armazenados não sejam mantidos por mais tempo do que o necessário na base de dados das instituições.
c) Avaliações de Impacto de privacidade (AIPD)	Atividade que envolvam riscos significativos à privacidade, objetivando identificar e mitigar possíveis riscos, também se encontra dentre as obrigações das IEs.
d) Acesso aos Dados pelos Titulares	Garantir, através de contratos, que os fornecedores e parceiros das IEs que tenham acesso aos dados pessoais, também cumpram com os requisitos elencados pela LGPD, estabelecendo contratualmente as responsabilidades para proteção dos dados
e) Monitoramento contínuo e auditoria	Para identificação de possíveis falhas e garantia de cumprimento da LGPD, passa a ser uma obrigação das IEs preparadas para demonstrar o cumprimento das obrigações estabelecidas na lei.

Fonte: Elaborado pelos autores (2024).

Se antes, a preocupação das IEs, estavam voltadas ao atendimento de requisitos legais, regulatórios e normativos (o que não os invalidam), agora se voltam para o uso ético⁵ e seguro dos dados pessoais. Mais que um processo polêmico e burocrático, a LGPD, visa o direito de proteção da personalidade e da privacidade. As IEs necessitam, já com inadiável urgência, se adequar às demandas (éticas) da referida Lei, buscando ferramentas tecnológicas disponíveis, metodologia própria de formação teórico-prática e apoio jurídico, como forma de assegurar os direitos dos dados e, por necessidade, seus titulares, conforme as novas diretrizes dadas pela LGPD.

Considerações Finais

⁵ Ética de absorção crítica da Lei, a ser discutido em outro artigo, para além do simples ajuste, com base na formação não apenas técnica.

O objetivo do artigo foi trazer os aspectos mais relevantes da Lei Geral de Proteção de Dados, a partir da análise dos principais artigos estabelecidos na LGPD, e os impactos trazidos (e respectivos desafios) nas IEs, que deverão se amoldar à nova legislação.

A proteção de dados pessoais nos meios digitais, estabeleceu-se como direito fundamental através da EC 115, que acresceu o inciso LXXIX, ao artigo 5º da Constituição Federal (CF), objetivando processamento de dados pessoais de forma ética, segura e responsável, garantindo ao indivíduo controle de seus dados.

Conforme pode se verificar da análise realizada dos principais aspectos da LGPD e dos caminhos que devem ser percorridos pelas IEs para se ajustar as exigências legais, a observância das medidas dispostas nos quadros 1 e 3, que perpassam pelo mapeamento dos dados, elaboração da política de privacidade, identificação da base legal para tratamento do dado, obtenção do consentimento informado, implementação de medidas para segurança dos dados, nomeação do encarregado de proteção de dados (DPO), treinamento dos funcionários, estabelecer políticas de retenção de dados, realizar avaliações de impacto de privacidade, realizar o monitoramento e auditoria dos dados, e estabelecer uma comunicação transparente, todas essas medidas necessárias para o cumprimento da legislação.

O cumprimento da LGPD pelas IEs exigirá uma abordagem contínua à proteção de dados, para garantir que as instituições estejam preparadas para adequar suas práticas as novas tecnologias e ameaças que permanecem em constante evolução. A hora é agora!

Referências

BIONI, Bruno Ricardo. O dever de informar e a teoria do diálogo das fontes para aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo “Lulu”. **Revista de Direito do Consumidor**, v. 94, p. 283-324, São Paulo, jul./ago. 2014.

BORELLI, Alessandra. O tratamento de dados de crianças e adolescentes no âmbito da lei geral de proteção de dados. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 179-190, jan. mar./2020. Disponível em; https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_8_o_tratamento_de_dados.pdf?d=637250348921212362. Acesso em: 20 out. 2023.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 19 out. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 20 out. 2023.

CASTELLS, Manuel. **A galáxia da internet:** reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2013.

CORDEIRO, A. Barreto Menezes. **Direito da Proteção de Dados:** à luz do RGPD e da lei n. 58/2019. Coimbra: Almeida, 2020, p. 174.

COSTA JÚNIOR, Paulo José de. **O direito de estar só:** tutela penal da intimidade. 4 ed. São Paulo: Revista dos Tribunais, 2007. p. 49).

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada.** São Paulo: Thomson Reuters Brasil, 2018, p.115).

CRESPO, Marcelo. Proteção de Dados Pessoais e o poder público: noções essenciais. *In:* CRAVO, Daniela Copetti; CUNDA, Daniela Zago G. da; RAMOS, Rafael (org). **Lei Geral de Proteção de Dados e o poder público.** Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, Porto Alegre, 2021.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito a privacidade e os limites à função fiscalizadora do Estado. *In:* PIZOLIO, Reinaldo; GALVADÃO JÚNIR, Jayr Viégas (coord.). **Sigilo fiscal e bancário.** São Paulo: Quartier Latin, 2005. p. 28.

LÉVY, Pierre. **Cibercultura.** São Paulo: Editora 34, 1999.

MALDONADO, Viviane Nobrega. Direitos dos Titulares de dados. *In:* MALDONADO, Viviane Nobrega; BUM, Renato Opice (coord.). **Comentários ao GDPR:** regulamento geral de proteção e dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 86-87.

MALDONADO, Viviane Nobrega. Dos Direitos do Titular. *In:* MALDONADO, Viviane Nobrega; BUM, Renato Opice (coord.). **Lei Geral de Proteção de Dados Comentada.** 4. Ed. São Paulo: Thomson Reuters Brasil, 2022. p. 233-264.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil - RBDCivil**, Belo Horizonte, v .25, p. 83-116, jul./set. 2020, p. 98.

VAINZOF, Rony. *et al.* Disposições preliminares. *In:* MALDONADO, Viviane Nobrega; BUM, Renato Opice (coord.). **Lei Geral de Proteção de Dados Pessoais Comentada.** 4. ed. São Paulo: Revista dos Tribunais, 2022. p. 21-191

CANDIANI, I. F.; PEREIRA, O. J.

ZANON, João Carlos. **Direito à proteção dos dados pessoais**. São Paulo: Revista dos Tribunais, 2013. p. 156.