DESAFIOS NA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NA ÁREA DA SAÚDE

General data protection law implemention challenges in healthcare

DOI 10.5281/zenodo.8102531

CHRISTIANY PEGORARI CONTE[1]; THAYS DE MELLO GIAIMO[2]; VITOR FALCÃO SOMBINI[3]

[1]Mestre em Direito da Sociedade da Informação pela FMU/SP. Doutora em Educação pela PUC Campinas. Professora da Graduação, Pós-Graduação Lato Sensu e da Extensão da PUC Campinas. Professora da ESA São Paulo, Campinas, Santos e Santo André. Professora da Especialização dos cursos PROORDEM (Santos e Goiânia); Professora da Especialização em Direito Ambiental e Agronegócio do CERS. E-mail: [chrispegorari08@gmail.com].

[2] Doutora em Direito Civil pela USP. Mestre em Direitos Difusos e Coletivos pela UNIMES. Especialista em Direito Ambiental e Bacharel em Direito pela FMU. Docente Universitária, Advogada e Parecerista. Professora do curso de Mestrado da Universidade *Veni Creator Christian University*. Professora de Pós-Graduação Lato Sensu e da Extensão da PUC Campinas e da Anima Educação, nas áreas de Direito e Negócios. Professora nos cursos técnicos do Instituto Monitor e na graduação em Direito da Faculdade Monitor. E-mail: [thaysgiaimo@hotmail.com].

[3] Advogado e Consultor em privacidade e proteção de dados pessoais. Especialista em Lei Geral de Proteção de Dados pela PUC Campinas. E-mail: [vitor@sombinispina.com.br].

RESUMO

O presente artigo tem como objetivo abordar os principais desafios da implementação da LGPD na área da saúde, muito em decorrência da sensibilidade dos dados pessoais tratados, que podem acarretar graves danos aos titulares em casos de vazamento ou uso inadequado. Para tanto, foram analisadas normas da área da saúde, normas de privacidade e proteção de dados pessoais e as boas-práticas adotadas internacionalmente. Como desafios para a adequação à LGPD na área da saúde, destaca-se a necessidade do consentimento informado dos pacientes, o respeito ao princípio da transparência, a importância da adoção de medidas técnicas e administrativas de segurança da informação, o atendimento aos direitos dos titulares de dados e a responsabilização após eventuais danos. Como resultado, são apresentados

processos e ferramentas que podem auxiliar na gestão dos projetos de adequação à LGPD, garantindo maior transparência, segurança e autonomia aos titulares de dados pessoais.

PALAVRAS-CHAVE: Dados pessoais. Saúde. Desafios. Implementação.

ABSTRACT

This article aims to address the main challenges of the LGPD implementation in healthcare, specially due to the sensitivity of the personal data processed, which can cause serious damage to data subjects in cases of leakage or inappropriate use. For this purpose, healthcare norms, privacy and personal data protection norms and the internationally adopted good practices were analyzed. As LGPD compliance challenges in healthcare, were highlighted the need for informed consent from patients, the transparency principle respect, the importance of adopting technical and administrative measures for information security, the compliance with data subjects rights and the damages liability. As a result, are presented some processes and tools that can assist in the management of LGPD compliance projects, guaranteeing greater transparency, security and autonomy to the data subjects.

KEYWORDS: Personal data. Healthcare. Challenges. Implementation.

Introdução

Considerando a indiscutível importância que o tema pertinente à proteção de dados tem ocupado nas legislações mundiais e sua respectiva implementação, globalmente, impõe-se analisar, neste artigo, as repercussões e os desafios da preservação de dados pessoais com enfoque na área da saúde.

O avanço tecnológico experimentado nas últimas décadas culminou na celeridade dos processos e informações, porém, quando interagem com tratamento de dados pessoais, as novas tecnologias relacionam-se com direitos humanos fundamentais, tornando-se imprescindível a criação de mecanismos legais hábeis a garantir a tutela da privacidade pela área do direito.

Neste escopo, direcionada à consagração de uma política de proteção de dados, a Lei Geral de Proteção de Dados - LGPD, disciplina, nos aspectos de direito material e processual, uma completa normatização visando à prevenção e à reparação decorrentes de inadequado tratamento de dados.

O presente ensaio tem por objetivo de analisar, sob um viés crítico, os dispositivos da Lei Geral de Proteção de Dados assim como na legislação esparsa, que são aplicáveis à área da saúde, na medida em que tais dados, denominados “sensíveis”, demandam especial proteção dos sistemas jurídicos.

A metodologia utilizada no desenvolvimento deste estudo pautou-se no levantamento das normas atinentes ao tema e no confronto entre as considerações doutrinárias nacionais e estrangeiras a respeito da tutela da privacidade de dados sensíveis.

Como resultados da pesquisa realizada, constataram-se os aportes teóricos que o sistema jurídico brasileiro se fundamenta, a possibilidade e forma de responsabilização nos âmbitos administrativo, civil e penal quando ocorre violação da privacidade, mas também a necessária priorização da prevenção no cuidado com os dados sensíveis tratados, porque mais eficaz na proteção, em detrimento da persecução da responsabilidade após o dano.

Finalmente, em função da amplitude de debates que a temática possibilita, a presente análise concentra-se em questões nucleares, não sendo exaustivos estudos acurados neste artigo apresentados.

1. Lei geral de proteção de dados

A Lei Geral de Proteção de Dados - LGPD (13.709/18) que regulamenta o tratamento de dados pessoais, foi sancionada em 14 de agosto de 2018, entrou em vigor no dia 18 de setembro de 2020 e as sanções administrativas passaram a ser aplicáveis a partir de agosto de 2021.

Esta lei regulamenta o uso, a proteção e a transferência de dados pessoais[1], além de criar uma autoridade reguladora, sancionadora e

[1] A LGPD define como dados: Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal 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; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

fiscalizatória (a Autoridade Nacional de Proteção de Dados - ANPD), no que tange ao cumprimento das diretrizes específicas estabelecidas na legislação.

A publicação desta normatização constitui passo importante para a proteção de dados no Brasil, pois, muito embora já existissem, nacionalmente, outras legislações e a própria Constituição Federal Brasileira de 1988, tutelando implicitamente a proteção dos dados pessoais[2], tais como o direito à privacidade, imagem, honra e dignidade, faltava ainda uma regulamentação mais específica que pudesse traçar diretrizes claras sobre a proteção de dados, especialmente no contexto tecnológico atual.

Também porque a tendência mundial concernente a esta temática se revelou através de mudanças legislativas sobre a proteção de dados em outros países e, sobretudo, após a criação e vigência do Regulamento Geral de proteção de dados Europeu (GDPR), tornou-se evidente a necessidade de uma regulamentação pelo ordenamento jurídico brasileiro, que culminou no advento da Lei Geral de Proteção de Dados.

A referida legislação constitui-se em importante regulamento pelo seu completo conteúdo que disciplina todos os aspectos concernentes ao tratamento de dados pessoais, mas também e especialmente porque, ao final, seu atendimento reforça direitos humanos fundamentais tão relevantes e constitucionalmente assegurados.

Em seu âmbito, dispõe sobre o tratamento de dados realizado por pessoas físicas ou jurídicas, de direito público ou privado, abrangendo o amplo conjunto de operações efetuadas, incluindo aquelas realizadas em meios manuais (arquivos ou fichas de papel) ou digitais.

Contudo, assim como as demais normas da estrutura jurídica pátria, a Lei Geral de Proteção de Dados, tem sua aplicabilidade condicionada a interpretação dialógica com ponderação de outras legislações correlatas nacionais, como por exemplo, dispositivos de ordem cível, criminal, consumerista, constitucional, administrativo e regras da área da saúde, não

[2] Vale lembrar que existe a proposta de emenda constitucional PEC 17/19 que tem por objetivo incluir como direito fundamental expresso, na Constituição Federal Brasileira de 1988, o direito à proteção de dados.

sendo, portanto, recomendada sua aplicação isolada e descontextualizada do arcabouço legal nacional.

Além da Lei Geral de Proteção de Dados existem, no ordenamento jurídico nacional, diversas legislações esparsas, correlatas ao tema, conforme analisaremos a seguir.

A Lei n. 13.787 de 2018 versa sobre a digitalização e tratamento dos dados do prontuário dos pacientes[3] estabelecendo procedimentos de segurança e confidencialidade aos dados sensíveis.

A Política Nacional de Proteção de Dados Pessoais no Sistema Unimed, Norma Derivada 15, de 2019, da Unimed do Brasil- UNIMED/19, revisada em 2020, estabelece regras e diretrizes que devem ser cumpridas pelos profissionais médicos cooperados e prestadores de serviços com vistas à adequação à LGPD.

A seu turno, o Conselho Federal de Medicina editou instruções[4] e portarias[5] estabelecendo recomendações, informando e estabelecendo a estrutura de Política de Privacidade no seu âmbito de atuação.

Na área da saúde, considerando a sensibilidade dos dados pessoais tratados, denominados na Lei Geral de Proteção de Dados como “dados

---

[3] Lei n. 13.787/18 - Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Art. 1º A digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente são regidas por esta Lei e pela Lei nº 13.709, de 14 de agosto de 2018. Art. 2º O processo de digitalização de prontuário de paciente será realizado de forma a assegurar a integridade, a autenticidade e a confidencialidade do documento digital.

[4] INSTRUÇÃO NORMATIVA CFM Nº 3, DE 3 DE MARÇO DE 2021. Institui a Política de Privacidade dos Dados das Pessoas Físicas no âmbito do Conselho Federal e nos Conselhos Regionais de Medicina. Art. 5º No CFM e nos CRMs, o Controlador é a autoridade máxima do órgão, o Operador considera-se como o ocupante da alta administração e o encarregado e o que será nomeado pela alta administração que realizará a comunicação entre a Autoridade Nacional de Proteção de Dados e o controlador. § 1º Deverá ser instituído um Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais para prestar suporte aos trabalhos da LGPD que será formado por uma equipe técnica e multidisciplinar, que desempenhe as funções jurídica, de segurança da informação e tecnológica, de comunicação interna e externa, de recursos humanos, de gestão documental e estratégica.

[5] PORTARIA CFM Nº 32, DE 10 de março 2021 - Instituir a composição do Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais para apoio ao encarregado pelo Tratamento de Dados Pessoais. Lei de Proteção de Dados no âmbito do Conselho Federal de Medicina.
PORTARIA CFM Nº 33, DE 10 DE MARÇO 2021 - Institui o Encarregado pelo Tratamento de Dados Pessoais - Lei de Proteção de Dados no âmbito do Conselho Federal de Medicina e dá outras providências. Conselho Federal de Medicina Código de Ética Médica: Resolução CFM nº 2.217, de 27 de setembro de 2018, modificada pelas Resoluções nº 2.222/2018 e 2.226/2019.

sensíveis", existiam, anteriormente à edição da LGPD, normativas que visavam a garantir a privacidade e a proteção de dados de pacientes.

Na Idade Antiga, Hipócrates (460 a.C.), reconhecido como o "pai da medicina", se manifestava sobre o tema da confidencialidade, conforme se nota do trecho extraído do Juramento de Hipócrates[6], a seguir transcrito: "Àquilo que no exercício ou fora do exercício da profissão e no convívio da sociedade, eu tiver visto ou ouvido, que não seja preciso divulgar, eu conservarei inteiramente secreto".

Tal recomendação se encontra difundida em diversas normativas da área médica, vejamos o Código de Ética Médica (Resolução do Conselho Federal de Medicina nº 2.217, de 27 de setembro de 2018), que determina no artigo 73, ser conduta vedada ao profissional médico "Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente".

Entretanto, as atividades de uma organização prestadora de serviços de saúde envolvem profissionais de diversas outras áreas, não se restringindo à figura do médico, mas abrange os profissionais que exercem sua função na recepção, no atendimento ao cliente e também, os que, dentre tantos outros envolvidos neste contexto, integram os quadros de colaboradores dos departamentos comercial, de faturamento e de credenciamento (responsável pela gestão de operadoras de planos de saúde e parceiros comerciais).

---

[6] Juramento de Hipócrates: "Eu juro, por Apolo médico, por Esculápio, Hígia e Panacea, e tomo por testemunhas todos os deuses e todas as deusas, cumprir, segundo meu poder e minha razão, a promessa que se segue: Estimar, tanto quanto a meus pais, aquele que me ensinou esta arte; fazer vida comum e, se necessário for, com ele partilhar meus bens; ter seus filhos por meus próprios irmãos; ensinar-lhes esta arte, se eles tiverem necessidade de aprendê-la, sem remuneração e nem compromisso escrito; fazer participar dos preceitos, das lições e de todo o resto do ensino, meus filhos, os de meu mestre e os discípulos inscritos segundo os regulamentos da profissão, porém, só a estes. Aplicarei os regimes para o bem do doente segundo o meu poder e entendimento, nunca para causar dano ou mal a alguém. A ninguém darei por comprazer, nem remédio mortal nem um conselho que induza a perda. Do mesmo modo não darei a nenhuma mulher uma substância abortiva. Conservarei imaculada minha vida e minha arte. Não praticarei a talha, mesmo sobre um calculoso confirmado; deixarei essa operação aos práticos que disso cuidam. Em toda casa, aí entrarei para o bem dos doentes, mantendo-me longe de todo o dano voluntário e de toda a sedução, sobretudo dos prazeres do amor, com as mulheres ou com os homens livres ou escravizados. Àquilo que no exercício ou fora do exercício da profissão e no convívio da sociedade, eu tiver visto ou ouvido, que não seja preciso divulgar, eu conservarei inteiramente secreto. Se eu cumprir este juramento com fidelidade, que me seja dado gozar felizmente da vida e da minha profissão, honrado para sempre entre os homens; se eu dele me afastar ou infringir, o contrário aconteça." Disponível em: https://www.cremesp.org.br/?siteAcao=Historia&esc=3. Acesso em 25/03/2023..

Nesta seara, resta evidente a quantidade de profissionais, inclusive aqueles não restritos à área da saúde, que têm acesso a dados pessoais comuns e sensíveis dos pacientes da área médica, quando, a título de exemplo, entregam um laudo, registram formulário de atendimento no sistema ou agendam consulta médica.

Por não se tratar de profissionais vinculados ao Conselho Federal de Medicina, não possuem a obrigatoriedade do sigilo médico prevista em lei, posto isto, importante sejam adotadas providências para se garantir a confidencialidade no ambiente de trabalho, recomendando-se a aplicação de treinamentos, vinculação de obrigatoriedade de cumprimento de termo de sigilo, entre outras medidas que podem compor um projeto de adequação, que passamos a tratar a seguir.

2. Projeto de adequação

O projeto de adequação consiste em instrumento eficaz para a implantação das diretrizes e regramentos da Lei Geral de Proteção de Dados, na medida em que se trata de adequada ferramenta para combater os desafios da privacidade dos dados pessoais na área da saúde.

Um projeto de adequação à LGPD eficiente e duradouro deve envolver toda a organização, desde colaboradores, gestores, alta administração, parceiros comerciais e prestadores de serviço, sendo indispensáveis para o êxito: cultura institucional direcionada, governança corporativa determinada e ambiente comprometido com o tema de conformidade à legislação de proteção de dados.

Em síntese, revisão e redesenho da estrutura da organização, com plano de acesso às informações, definição de papéis e responsabilidades e capacitação dos profissionais envolvidos no comitê de *compliance* regulatório, responsáveis por verificar as conformidades das atuações.

Neste sentido, o projeto de adequação compõe-se de três elementos indissociáveis, que consistem nos temas inerentes à Gestão de pessoas, Cultura

e governança e Revisão do Setor de Tecnologia da Informação (TI), cujos quais passaremos a especificar. Revisão e redesenho da estrutura da organização, plano de acesso às informações com definição de papéis e responsabilidades e capacitação dos profissionais envolvidos no comitê de compliance regulatório.

2.1 Gestão de pessoas

A gestão efetiva de pessoas dentro da organização possui importância incomensurável, pois ao mesmo tempo em que auxilia a empresa a definir padrões de acesso à informação, explica aos colaboradores suas respectivas atuações e obrigações na relação comercial, além de promover a estruturação dos processos e operações de tratamento de dados institucionais.

Regressando à análise sobre o necessário sigilo profissional no que concerne aos dados sensíveis dos pacientes referente às suas informações médicas, parece contraproducente a obrigatoriedade de assinatura, pelos funcionários, de um Termo de Sigilo e Confidencialidade se não houver na organização controle de acesso, ou seja, neste cenário, qualquer pessoa externa (que portanto não está atrelada ao termo de sigilo), poderia, teoricamente, acessar e fazer uso indevido de informações confidenciais.

A empresa precisa demonstrar seu compromisso com a proteção de dados, estabelecendo níveis de acesso, restringindo informações, especificamente, apenas aos profissionais necessários, capacitados e devidamente treinados sobre boas-práticas de segurança da informação, todos estes submetidos ao dever de sigilo legal ou contratual.

Enquanto agente de tratamento de dados pessoais, é imprescindível que a empresa saiba compreender suas obrigações nas suas relações comerciais que estabelece e qual o papel que ocupa na estrutura legal de agentes da relação de tratamento de dados.

Isso porque a Lei Geral de Proteção de Dados estipula funções e responsabilidades específicas às partes envolvidas nestas relações jurídicas, prevendo a figura do controlador, operador e encarregado.[7]

[7] Artigo 5 da Lei Geral de Proteção de Dados:

Portanto, caso um hospital terceirize a análise de exames clínicos a um laboratório, o hospital assumirá perante a legislação a figura de controlador e o laboratório será o operador de dados pessoais.

Sendo assim, o laboratório – como operador de dados pessoais - deverá seguir as determinações sobre a finalidade e a base legal que foram fornecidas pelo controlador de dados, ou seja, pelo hospital. Caso descumpra as determinações do controlador, o laboratório infringe a LGPD e sofrerá todas as consequências legais e administrativas.

Por isto é tão importante que as empresas participantes das operações comerciais, neste caso, todas as envolvidas com a área da saúde tenham conhecimento dos papéis que ocupam em cada serviço prestado, se controladores ou operadores de dados pessoais, e nomeiem um funcionário para exercer a função de encarregado (também conhecido por *data protection officer*)[8], que atuará como um mediador entre empresa, titular de dados e ANPD-Autoridade Nacional de Proteção de Dados[9].

2.2 Cultura e governança

A adequação à Lei Geral de Proteção de Dados deve fazer parte da estrutura da empresa, compondo a cultura organizacional de proteção de dados em todos os processos e departamentos e além disso, inafastável a necessidade de firme gestão e competente estrutura de governança que garanta o atendimento aos dispositivos legais e podem ser executadas mediante a adoção das seguintes ações:

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;
Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

[8] VIII – encarregado (DPO - Data Protection Officer): 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);

[9] Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

2.2.1 Formulação de regras de boas práticas e governança

No que se refere ao exercício de boas práticas e governança corporativa pelos profissionais da área da saúde, precede o estabelecimento de políticas empresariais, normas e códigos de conduta.

Esses parâmetros concebidos direcionarão os colaboradores dentro das diretrizes que se espera que atuem e a partir daí se torna possível a exigibilidade de conduta conforme as práticas estipuladas pela empresa e geridas pela governança.

Para que reste evidente o compromisso institucional com o tema de proteção de dados pessoais na saúde é necessário que todas as estruturas hierárquicas empresariais, inclusive o alto corpo diretivo, sigam as normas instituídas e compartilhadas, como um exemplo a ser seguido pelos demais colaboradores.

2.2.2 Normas de segurança

Ademais, precisam ser adotadas medidas técnicas relacionadas às tecnologias e controles, bem como administrativas relacionadas a políticas, processos e treinamentos de segurança da informação[10], que garantam uma proteção de ponta a ponta, nas palavras de Jimenez ao tratar de medidas de segurança:

> Ferramentas de autenticação de acesso a sistemas, mecanismos de segurança em *softwares* e *hardwares*, recursos de controle de tráfego de dados em rede, instrumentos detectores de invasões de sistemas, recursos de criptografia, segregação de servidores, ferramentas de prevenção a perda de

[10] "Os objetivos das medidas também merecem comentários. O primeiro deles é o de impedir acessos não autorizados, mantendo a sua confidencialidade de acordo com o necessário para se alcançar a finalidade do tratamento. O segundo, que, em suma, pretende preservar a integridade das informações e prevenir vazamentos, depende em boa parte do primeiro objetivo. Isso porque nem todo vazamento ou perda de informações se dá pela quebra do sistema de segurança, mas muitas vezes se dá por credenciais utilizadas indevidamente, por culpa ou dolo". COTS, Marcio & OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. p. 239.

dados, testes de vulnerabilidade, cópias de segurança, entre muitos outros.[11]

2.2.3 Ações educativas

A adequação à Lei Geral de Proteção de Dados dependerá dos treinamentos aos funcionários que precisam ser orientados e capacitados sobre o escopo da lei, objetivos da empresa e da importância da proteção de dados.

Não se limita apenas a existência ou formalização de documentos, sendo necessária instrução aos colaboradores da ocorrência prática nas ações cotidianas, importante sejam orientados e educados sobre privacidade e proteção de dados através de capacitações, palestras e campanhas internas.

2.2.4 Supervisão e mitigação de riscos

No que se refere à supervisão e diminuição de riscos, pode-se mencionar a criação ou ajuste de contratos, termos de consentimento para uso de dados, cláusulas de confidencialidade, estabelecimento de regras para uso de direito de imagem, enfim, existe uma infinidade de ferramentas de prevenção disponíveis para gerenciar a eventualidade de ocorrência de prejuízo no tratamento de dados.

Neste aspecto, aqui também se reforça o comprometimento do alto corpo diretivo na supervisão do cumprimento das políticas, normas e regras de boas-práticas e segurança da informação pelos colaboradores da organização e aplicação das sanções, quando previstas, e que inclusive, têm a finalidade de exemplificar aos demais colaboradores demonstrando a todos a importância que a empresa atribui à adequação às normas de proteção de dados.

2.2.5 Revisão contínua do fluxo de conformidade:

[11] JIMENE, Camilla do Vale. Reflexões sobre privacy by design e privacy by default: da idealização à positivação. In: MALDONADO, Viviane Nóbrega & OPICE BLUM, Renato (Coord.). Comentários do GDPR: Regulamento Geral de Proteção de Dados da União Europeia. p.329.

Para a adequação à LGPD, a empresa precisa adequar processos antigos e desenhar novos procedimentos de acordo com as regras e boas práticas de proteção de dados, por meio de um processo contínuo, visando um *compliance* efetivo, atualizado e que se mantenha no tempo.

A governança envolve a adoção de práticas de *privacy by design* (privacidade desde a concepção) e *privacy by default* (privacidade por padrão), metodologias criadas nos anos 1990 por Ann Cavoukian, comissária de informação e privacidade de Ontário (Canadá).

> O termo *privacy by design* refere-se à metodologia que visa proteger a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação ou de práticas de negócio que sejam concernentes ao ser humano. Assim, a proteção da privacidade seria o ponto de partida para o desenvolvimento de qualquer projeto, sendo incorporada à própria arquitetura técnica dos produtos ou serviços.[12]

Neste sentido, no atendimento a um paciente, a organização da área da saúde deve garantir a privacidade dos dados pessoais durante todo o ciclo de vida do dado[13], ou seja, desde o agendamento de uma consulta ou atendimento, passando por eventuais exames, laudos, compartilhamentos com operadoras de planos de saúde, médicos e laboratórios.

No que se refere ao *privacy by default*, segundo Martins e Guariento explicam que:

> O produto ou serviço deve ser entregue com a configuração de privacidade mais restritiva possível, de modo a que apenas os dados indispensáveis sejam coletados, cabendo ao próprio usuário, se assim desejar, habilitar de maneira informada e voluntária outras funcionalidades que ampliem o espectro de tratamento de seus dados pessoais. [14]

---

[12] JIMENE, Camilla do Vale. Reflexões sobre privacy by design e privacy by default: da idealização à positivação. In: MALDONADO, Viviane Nóbrega & OPICE BLUM, Renato (Coord.). Comentários do GDPR: Regulamento Geral de Proteção de Dados da União Europeia. p.174

[13] "No âmbito da promoção da segurança da informação, os processos e procedimentos devem assegurar a disponibilidade, integridade e confidencialidade de todas as formas de informação, ao longo de todo o ciclo de vida do dado". PECK, Patrícia. Proteção de dados pessoais. Comentários à Lei n. 13.709/2018 (LGPD). p.102.

[14] MARTINS, Ricardo Maffeis & GUARIENTO, Daniel Bittencourt. Privacy by design, by default e by redesign. Disponível em: [https://www.migalhas.com.br/coluna/impressoes-digitais/345919/privacy-by-design-by-default-e-by-redesign]. Acesso em: 25.03.2023.

Na prática, nos *sites* que utilizam *cookies*, estes só podem ser habilitados mediante a ativação do usuário para tal coleta de dados e caso este visitante não ative os cookies de forma voluntária, não haverá a coleta de informações pessoais do usuário, pois a Lei Geral de Proteção de Dados exige que todas as empresas que utilizem cookies os deixem inativos por padrão, para que assim, o usuário possa decidir quais dados deseja compartilhar.

2.3. Revisão do Setor de Tecnologia da Informação (TI)

Conforme mencionado a adequação à Lei Geral de Proteção de Dados leva em consideração todos os ambientes empresariais nos quais ocorra tratamento de dados pessoais, portanto, a estrutura toda deve aplicar a proteção de dados, orientada e supervisionada por profissionais capacitados, envolvendo conceitos jurídicos, de processos técnicos e de tecnologia da informação.

No entanto, destaca-se que a segurança de informações em ambiente digital deve passar por uma revisão criteriosa realizada pelo setor de tecnologia da informação, que possui conhecimento técnico para orientar sobre as melhores ferramentas disponíveis no mercado para cada situação e necessidade específica.

> Quanto maior a exposição ao risco de violação à privacidade causada pelo agente de tratamento, seja em razão da qualidade ou do volume dos dados tratados, maior deverá ser o seu comprometimento com medidas de controle e prevenção para fins de segurança da informação. [15]

No caso de empresas da área da saúde, tais como hospitais, clínicas e laboratórios, a quantidade e a sensibilidade dos dados pessoais tratados tendem sempre a serem elevadas, o que exige um zelo e consequentemente é um investimento maior por parte dessas empresas.

Entretanto, o investimento na adoção de medidas preventivas se justifica pois ínfimo quando comparado aos valores decorrentes de responsabilização

[15] CABRAL, Filipe Fonteles. Proteção de dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais, 2019.p.64.

pelo tratamento inadequado, como por exemplo, sujeição à responsabilidade administrativa prevista no artigo 52[16] da LGPD.

Além desta forma de responsabilização, citamos demais previsões legal que consistem em multas, advertências, suspensão de atividade de tratamento de dados, sanções administrativas aplicáveis pela ANPD- Autoridade Nacional de Proteção de Dados, que exerce função sancionatória, fiscalizatória e regulatória.

3. Proteção de dados, princípios e direitos dos pacientes: diretrizes da lei geral de proteção de dados - LGPD

A Lei Geral de Proteção de dados exige transparência no tratamento de dados pela empresa, que também possibilita maior controle dos usuários sobre as suas informações pessoais, estabelecendo, inclusive, que o tratamento dos dados depende do consentimento do titular.

São princípios preconizados pela LGPD e de adoção obrigatória aqueles, por exemplo, especificados no artigo 6º desta lei, a seguir pontuados.

a) Transparência: garantia ao titular dos dados sobre informações claras de como se dará o tratamento dos dados coletados.
b) Finalidade: o tratamento dos dados coletados deve atender aos propósitos que foram indicados pelo titular dos dados.

[16] Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII - (VETADO); VIII - (VETADO); IX - (VETADO). X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

c) Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
d) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
e) Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Especialmente na área da saúde, o principal ponto consiste no consentimento do paciente titular dos dados para qualquer situação e neste sentido o artigo 43 do Código de Defesa do Consumidor dialoga com o artigo 7º da Lei Geral de Proteção de Dados[17], determinando a necessidade de se comunicar ao paciente/consumidor acerca da coleta dos dados.

As empresas precisam ter certeza de que os pacientes autorizam contato, salvo em raras situações em que a lei permite a sua realização sem consentimento.

Por ocasião da pandemia desencadeada pela COVID provocada pelo coronavírus diversas tecnologias de monitoramento surgiram nesse período, permitindo-se através da coleta de dados, o rastreamento de pessoas contaminadas, ajudando no controle da disseminação da doença.

Assim como a necessidade de consentimento informado do paciente[18], igualmente importante consubstancia-se na necessária transparência de como

[17] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I- mediante o fornecimento de consentimento pelo titular; III- pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV- para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; VII -para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

[18] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; - manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5). § 3º É

a coleta e guarda dos dados é realizada, sobre a segurança desse banco de dados e a possibilidade de remoção do cadastro no banco de dados ou de não ser mais contatado.

Isto porque as diretrizes da LGPD têm por objetivo, conforme disciplinado no artigo 1º desta lei o "objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", prosseguindo, no artigo 2º com a normatização dos fundamentos da proteção de dados, pautada na privacidade, autodeterminação informativa, inviolabilidade da intimidade, entre outros[19].

A legislação protetiva[20] preocupou-se também em disciplinar o tratamento de dados pessoais de pacientes crianças e adolescentes, condicionando a sua realização ao escopo de consecução do seu melhor interesse, no mesmo sentido conferido pelo Estatuto da Criança e do Adolescente-ECA.

Este artigo, em seu *caput*, reforça que o tratamento de dados de crianças e adolescentes deverá atender ao Princípio do melhor interesse do menor, já tão enraizado em normas dispostas no ECA e no Código Civil, tratando-se de obrigação do Estado garantir medidas de proteção à criança e ao adolescente, que deverão ser acompanhadas, fiscalizadas e cumpridas pela família e comunidade.

Pela leitura objetiva do artigo e seus parágrafos, entende-se que o tratamento de dados pessoais de adolescentes deve atender a seu melhor interesse. Já para o tratamento de dados pessoais de crianças, deverá haver

vedado o tratamento de dados pessoais mediante vício de consentimento –até porque também geraria nulidade. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

[19] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I- o respeito à privacidade; II- a autodeterminação informativa – o poder de cada cidadão sobre os seus dados, III- a liberdade de expressão, de informação, de comunicação e de opinião; IV- a inviolabilidade da intimidade, da honra e da imagem; V- o desenvolvimento econômico e tecnológico e a inovação; VI- a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII- os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

[20] Artigo 14 da LGPD: O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
§ 1º 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 pelo responsável legal.

também o consentimento específico e em destaque fornecido pela mãe, pai ou responsável legal[21].

Eventualmente, diante de suposta fragilidade no tratamento de dados pessoais de adolescentes e para que não haja a desproteção desses, é possível que a Autoridade Nacional de Proteção de Dados – ANPD publique diretrizes interpretativas sobre o viés do artigo 14 da Lei.

Todavia, ao que parece, está em consonância com a GDPR (*General Data Protection Regulation*), lei de proteção de dados da União Europeia, que serviu de inspiração para a criação da LGPD nacional.

A lei não tratou sobre a eficácia de autorizações concedidas por pacientes idosos e pessoas com deficiência (PCDs), que, eventualmente, possam ter discernimento reduzido, observando-se, para tanto, a Teoria das Incapacidades, o Estatuto da Pessoa com Deficiência (13.146/2015) e o Estatuto do Idoso (10.741/2003).

É importante frisar que de acordo com o Estatuto da Pessoa com Deficiência, a curatela deverá se limitar às necessidades do curatelado, não podendo infringir sua autonomia. Sendo assim, se uma pessoa com deficiência é curatelada para a prática de atos financeiros, tendo discernimento para a prática dos demais atos existenciais ou negociais, sua autorização para o uso de seu dado pessoal deve ser considerada válida.

A discussão do consentimento de utilização de dados no que se refere aos pacientes idosos revela-se ainda mais problemática em função da dificuldade de se garantir que o idoso, diante das atuais tecnologias, tem discernimento para decidir se concorda ou não com a coleta do seu dado pessoal e ainda, outro desafio consiste em como proteger o idoso e limitar a possibilidade de seu consentimento, no seu melhor interesse, sem ultrapassar sua autonomia.

4. Direito de acesso aos dados e a anonimização

[21] Artigo 14, Parágrafo 1° da LGPD: "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 pelo responsável legal".

No que se refere aos direitos dos titulares dos dados de acessarem os dados pessoais que a empresa detém a seu respeito, todo paciente deve ter acesso viabilizado, sendo proibida a recusa de permissão de acesso ao titular do dado pessoal.

Ainda, o paciente tem direito de saber como seus dados serão utilizados, sobre eventual possibilidade de portabilidade dos dados, informações sobre compartilhamento, acesso aos dados processados e o procedimento para a revogação do consentimento fornecido, quando for o caso.

Para o caso, por exemplo, de pesquisas médicas, diante da necessidade de divulgação dos resultados obtidos para finalidade de aprimoramento científico, deve ser realizada a anonimização dos dados.

Esta consiste na utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, ou seja, a anonimização é o processo que visa a fazer com que seja impossível identificar uma pessoa a partir do dado disponível.

Esta técnica pode ser empregada de três maneiras: (a) anonimização por supressão de dado identificador da base de dados; (b) anonimização por generalização de forma que o dado pessoal quebra o vínculo direto com o titular do dado no momento em que ele fica menos detalhado do que deveria ficar; e (c) anonimização por randomização, em que o dado se torna aleatório, comum em estudos clínicos para seleção de um perfil aleatório de pacientes, contribui para que as características da amostra sejam homogêneas quanto ao sexo, idade e outros fatores prognósticos.

5. Vazamento de dados

Conforme pesquisa realizada por empresa de consultoria global de riscos, investigação empresarial e cibersegurança, com destaque para o monitoramento em tempo real, divulgada pela revista Exame[22], as empresas do setor de saúde

[22] Empresas de saúde são principal alvo de hackers no segundo trimestre. 2022. Disponível em: [https://exame.com/tecnologia/empresas-de-saude-sao-principal-alvo-de-hackers-no-segundo-trimestre/]. Acesso em: 25.03.2023.

foram os principais alvos de *hackers* no segundo trimestre de 2022, considerando-se o cenário global, registrando alta de 90% em relação aos três primeiros meses do ano.

Paralelamente, de acordo com dados da empresa de segurança Tenable, divulgados em publicação de Demartini na Canaltech[23], a saúde foi o setor mais afetado por casos de vazamento de dados, representando 24,7% do total de casos.

Sendo assim, além da importância de se evitar que um vazamento de dados ocorra, é de extrema importância que a empresa esteja preparada[24] para caso esse vazamento ocorra, mediante o desenvolvimento de um plano de resposta a incidentes de dados, RIPD[25].

Neste sentido, a LGPD estabelece que os agentes de tratamento de dados devem registrar todas as atividades de tratamento de dados pessoais[26], indicando os tipos de dados coletados, suas finalidades, tempo de retenção e as práticas de segurança da informação.

Além disso, indica que a Autoridade Nacional de Proteção de Dados (ANPD) poderá solicitar a apresentação ou determinar a elaboração do relatório de impacto à proteção de dados pessoais (RIPD)[27], "documentação que contém

---

[23] DEMARTINI, Felipe. Vazamento de dados corporativos aumentou 78% em 2021; saiba como se proteger. Disponível em: [https://canaltech.com.br/seguranca/vazamento-de-dados-corporativos-aumentou-78-em-2021-saiba-como-se-proteger-214024/]. Acesso em: 25.03.2023.

[24] "A avaliação sobre a necessidade da realização prévia de um RIPD tenha que partir não de uma solicitação da ANPD ou de uma indicação genérica para a condução desse processo em todos os casos possíveis de tratamento de dados, mas sim de uma análise do risco à privacidade envolvido na respectiva operação de tratamento, a exemplo do que ocorre no modelo europeu, com a definição de realização do RIPD quando o risco identificado for de fato elevado, seja para novas operações, seja para operações legadas. PALHARES, Felipe. Capítulo 7 – O Relatório de Impacto à Proteção de Dados Pessoais. In: MALDONADO, Viviane Nóbrega (Coord.). LGPD: Lei Geral de Proteção de Dados Pessoais: manual de implementação, 2019, p. 274-275.

[25] Quando o pior cenário se torna uma realidade, é fundamental ter o plano de resposta adequado para entrar em operação, e ter as pessoas certas nas posições de trabalho que farão frente ao cenário crítico. A resposta adequada aos incidentes de segurança é um processo complexo que requer ações assertivas das equipes envolvidas com a segurança dos dados pessoais. Entretanto, para que a empresa disponha de ações assertivas é requerido muito treinamento. ALMEIDA JUNIOR, Washington Umpierres de. Capítulo 10 – Incidente de segurança e respostas adequadas. In: MALDONADO, Viviane Nóbrega (Coord.). LGPD: Lei Geral de Proteção de Dados Pessoais: manual de implementação, 2019, p.341.

[26] Definição do art. 37 da Lei 13.709, de 14.08.2018.

[27] O RIPD tem por objetivo garantir a efetividade dos princípios formadores da LGPD, em particular, o princípio da responsabilização, aplicando em situações concretas os conceitos de gerenciamento de riscos e balanceamento de interesses. CABRAL, Filipe Fonteles. Proteção de dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais, 2019,p.77.

“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 risco”[28].

Conclusões

Um dos grandes desafios da implantação da Lei Geral de Proteção de Dados na área da saúde, a par da realização de um eficiente projeto de adequação, reside no necessário consentimento informado do paciente no que se refere à transmissão de informações claras e objetivas ao titular de dados, respeitando o princípio da transparência.

Isto porque, além dos termos técnicos inerentes à área médica demandarem conhecimentos específicos para sua correta compreensão, as políticas de privacidade e termos de uso, comumente desenvolvidas por setores jurídicos, não raramente são repletas de palavras de difícil entendimento pelo titular de dados.

Caso o paciente não entenda os termos não se pode afirmar que, ainda que tenha consentido, seu consentimento é válido, mas ao contrário disso, será anulada sua declaração de concordância, por não ser possível concordar com o que não se entende.

O mesmo ocorre com o tratamento de dados pessoais de crianças[29] e adolescentes, idosos e portadores de deficiências que, eventualmente, tenham comprometimento de sua capacidade de consentimento, devendo-se atentar, ao preconizado pelas normas da legislação para a validação das respectivas concordâncias.

[28] Definição do inciso XVII, do art. 5º da Lei 13.709, de 14.08.2018.

[29]Previsão do § 6º, do art. 14 da Lei 13.709, de 14.08.2018: As informações deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

O *visual law*[30] é uma ferramenta que vem sendo utilizada para facilitar o entendimento dos termos e políticas de proteção de dados, tornando a leitura mais fácil e interessante.

Além disso, com relação à telemedicina com interface terceirizada deve considerar a existência do *privacy by design* e demais previsões de mecanismos de segurança, principalmente no tráfego, tais como criptografia.

Sobre a adequação da atuação na área de saúde, estruturar o projeto de adequação à LGPD, prevendo a informação acerca do consentimento sobre os cookies no site, criptografia, estipulação de níveis de acesso, com *login* e senha exclusivo, para que seja possível mapear os tratamentos de dados pessoais.

Também com relação às consultas médicas por meios remotos ou envio de exames, discussão de opiniões clínicas, indica-se que não se realize desta forma, pois o acesso ao dispositivo, permitido ou decorrente de invasão, pode ocasionar a divulgação na internet ou outros meios de comunicação.

Finalmente, no que se refere ao *data center* para armazenamento dos dados, estipular requisitos de segurança para proteção do ambiente e se terceirizado, especificar em contrato a política de segurança e de privacidade dos dados, considerando já existirem *softwares*, ferramentas e recursos tecnológicos desenvolvidos de maneira adequada aos dispositivos da LGPD, facilitando, desta forma, a proteção de dados pessoais.

Referências:

ALMEIDA JUNIOR, Washington Umpierres de. Capítulo 10 – Incidente de segurança e respostas adequadas. In: MALDONADO, Viviane Nóbrega (Coord.). **LGPD: Lei Geral de Proteção de Dados Pessoais***:* manual de implementação. São Paulo: Thomson Reuters Brasil, 2019.

[30]Neste sentido, destaca-se o brilhante trabalho realizado entre Google e Mauricio de Sousa Produções, com a edição especial do gibi Turma da Mônica em Proteção de Dados Pessoais, que aposta no *visual law* e em uma linguagem mais simples para trazer conceitos básicos sobre proteção de dados para crianças. SOUSA, Maurício & GOOGLE. Turma da Mônica em Proteção de Dados Pessoais. Disponível em: [https://turmadamonica.uol.com.br/revistasespeciais/?ed=seja-incrivel-na-internet]. Acesso em: 25.03.2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Subchefia para assuntos jurídicos, Casa Civil, Presidência da República, Brasília, 1988. Disponível em: [http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm]. Acesso em: 25.03.2023.

BRASIL**. Lei n. 13.709 de 14 de agosto de 2018***.* Dispõe sobre o tratamento de dados pessoais. Subchefia para assuntos jurídicos, Casa Civil, Presidência da República, Brasília, 2018. Disponível em: [http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm]. Acesso em: 25.03.2023.

CABRAL, Filipe Fonteles. **Proteção de dados pessoais na atividade empresarial**: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019.

CFM, Conselho federal de Medicina. **Resolução CFM nº 2.217, de 27 de setembro de 2018)**. Disponível em: [https://portal.cfm.org.br/images/PDF/cem2019.pdf]. Acesso em: 25.03.2023.

COTS, Marcio & OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada.** São Paulo: Thomson Reuters Brasil, 2018.

DEMARTINI, Felipe. **Vazamento de dados corporativos aumentou 78% em 2021; saiba como se proteger**. Disponível em: [https://canaltech.com.br/seguranca/vazamento-de-dados-corporativos-aumentou-78-em-2021-saiba-como-se-proteger-214024/]. Acesso em: 25.03.2023.

ESTADÃO CONTEÚDO. **Empresas de saúde são principal alvo de hackers no segundo trimestre**. Disponível em: [https://exame.com/tecnologia/empresas-de-saude-sao-principal-alvo-de-hackers-no-segundo-trimestre/]. Acesso em: 25.03.2023.

JIMENE, Camilla do Vale. Reflexões sobre *privacy by design* e *privacy by default*: da idealização à positivação. In: MALDONADO, Viviane Nóbrega & OPICE BLUM, Renato (Coord.). **Comentários do GDPR:** Regulamento Geral de Proteção de Dados da União Europeia*.* São Paulo: Thomson Reuters Brasil, 2018.

JIMENE, Camilla do Vale. Capítulo VII. Da Segurança e das Boas Práticas. In: MALDONADO, Viviane Nóbrega & OPICE BLUM, Renato (Coord.). **LGPD** – Lei Geral de Proteção de Dados. Comentada. São Paulo: Thomson Reuters Brasil, 2019.

MARTINS, Ricardo Maffeis & GUARIENTO, Daniel Bittencourt. **Privacy by design, by default e by redesign.** Disponível em: [https://www.migalhas.com.br/coluna/impressoes-digitais/345919/privacy-by-design-by-default-e-by-redesign]. Acesso em: 25.03.2023.

PALHARES, Felipe. Capítulo 7 – O Relatório de Impacto à Proteção de Dados Pessoais. In: MALDONADO, Viviane Nóbrega (Coord.). **LGPD: Lei Geral de Proteção de Dados Pessoais:** manual de implementação. São Paulo: Thomson Reuters Brasil, 2019.

PECK, Patrícia. **Proteção de dados pessoais**. Comentários à Lei n. 13.709/2018 (LGPD). São Paulo. Saraiva Educação, 2018.

SOUSA, Maurício & GOOGLE. **Turma da Mônica em Proteção de Dados Pessoais.** Disponível em: [https://turmadamonica.uol.com.br/revistasespeciais/?ed=seja-incrivel-na-internet]. Acesso em: 25.03.2023.