CONTROLE SISTÊMICO DE ATIVIDADES DE TRATAMENTO DE DADOS NO *COMPLIANCE* DA LEI GERAL DE PROTEÇÃO DE DADOS EM CLÍNICA MÉDICA

Renata Salgado Leme
Universidade Santa Cecília (Unisanta), São Paulo.
renataleme@aasp.org.br

Marcelo Blank
Universidade Santa Cecília (Unisanta), São Paulo.
mablankg@gmail.com

Resumo: Trata-se de análise descritiva e explicativa da Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados - LGPD, no tocante ao impacto no tratamento de dados de pequenas e médias empresas, em especial no atendimento dos requisitos previstos no estatuto, no preenchimento dos documentos e relatórios obrigatórios, que devem ser gerados pelas organizações durante o ciclo operacional das mesmas e da importância do uso de ferramentas sistêmicas para o controle de todas as fases do processo com a finalidade de adequação à Lei. A pesquisa é de cunho exploratório, de caráter bibliográfico e documental, com base em livros, artigos, legislações e documentos. A investigação examinou o processo de adaptação de uma clínica médica à LGPD, descrevendo as suas etapas para adequação das áreas de Recepção, Administrativa, Financeira e Recursos Humanos, priorizados esses departamentos por apresentarem um elevado número de tratamentos de dados em desconformidade com a LGPD. O estudo utilizou uma ferramenta sistêmica, desenvolvida com exclusividade, que simplifica e agiliza as tarefas de mapeamento de atividades de tratamento de dados e organiza a manutenção das informações atualizadas durante o trabalho de *compliance*[1] desenvolvido na clínica médica.
Palavras-chave: Proteção de Dados. LGPD. Tratamento de Dados. Sistema. Clínica Médica

Systemic control of data processing activities in compliance with the Brazilian General Data Protection Law in internal medicine

Abstract: This is a descriptive and explanatory analysis of Law nº 13.709/18, known as the General Data Protection Law - LGPD, regarding the impact on the data processing of small and medium-sized companies, in particular in meeting the requirements set forth in the statute, in completing the mandatory documents and reports, which must be generated by the organizations during their operational cycle and the importance of using systemic tools to control all stages of the process in order to comply with the Law. The research is exploratory, bibliographical and documental in nature, based on books, articles, legislation and documents. The investigation examined the process of adapting a medical clinic to the LGPD, describing its stages for adapting the Reception, Administrative, Financial and Human Resources areas, prioritizing these departments because they present a high number of data processing in non-compliance with the LGPD. The study used a systemic tool, developed exclusively, which simplifies and streamlines the

[1] Departamento interno nas empresas ou serviço contratado que tem a função de verificar se as condutas praticadas pelos atores da empresa estão ajustadas às normas dos órgãos de regulamentação.

tasks of mapping data processing activities and organizes the maintenance of updated information during the compliance work carried out at the Clinic.
Keywords: Data Protection. LGPD. Data Processing. System. Medical clinic

INTRODUÇÃO

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), publicada em 14 de agosto de 2018, tem como base a *General Data Proctection Regulation ("GDPR")*, Regulamento de Proteção de Dados, da União Europeia, aprovado em 2016 e com vigência a partir de março de 2018, e no dia 10 de fevereiro de 2022, foi promulgada pelo Congresso Nacional a Emenda Constitucional 115, que inclui a proteção de dados pessoais como cláusula pétrea da Constituição Federal, no rol de garantias e direitos fundamentais do artigo 5º. O texto ainda determina competência privativa da União para legislar sobre o tema.

O principal objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Trata-se de análise descritiva e explicativa da Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados - LGPD, no tocante ao impacto no tratamento de dados de pequenas e médias empresas, em especial no atendimento dos requisitos previstos no estatuto, no preenchimento dos documentos e relatórios obrigatórios, que devem ser gerados pelas organizações durante o ciclo operacional das mesmas e da importância do uso de ferramentas sistêmicas para o controle de todas as fases do processo com a finalidade de adequação à Lei.

A pesquisa é de cunho exploratório, de caráter bibliográfico e documental, com base em livros, artigos, legislações e documentos.

1 IMPORTÂNCIA DA ADEQUAÇÃO À LGPD

A LGPD vale para todos. Empresas de todos os setores, de todos os portes tratam dados pessoais. Mesmo que a empresa não trate dados pessoais, provavelmente negocia ou fornece produtos e serviços para empresas que tratam, e necessitam que seus fornecedores estejam em *compliance* com a Lei para também estarem em conformidade com a mesma.

Todos os departamentos das empresas manipulam dados pessoais: RH, Marketing, Logística, Tecnologia da Informação, Sistemas, Financeiro, Contabilidade, Vendas, Compras, Jurídico, *Compliance*, apenas como exemplos. Além disso, o tratamento de dados pessoais somente poderá ser realizado se estiver em conformidade com uma das bases legais[2] previstas na Lei.

O referido estatuto legal apresenta princípios para nortear o tratamento de dados pessoais, como finalidades (propósitos legítimos), adequação (compatibilidade), necessidade (mínima coleta de dados) e transparência na utilização dos dados coletados.

As empresas devem adotar medidas de segurança, governança e boas práticas no tratamento de dados.

A Lei será fiscalizada pela Autoridade Nacional de Proteção de Dados, ANPD, com responsabilidade de verificar o cumprimento e aplicar sanções no caso de violação.

[2] Hipóteses previstas em lei para a proteção de dados (art. 7º da Lei nº 13.709/18)

A LGPD define as responsabilidades e os direitos de todos na chamada Economia Digital, movida e orientada por dados. E em todas as atividades, online e offline. É uma lei técnica, fazendo com que os conceitos e definições apresentados, que até pouco tempo eram de domínio de especialistas envolvidos com direito digital e tecnologia da informação, sejam importantes para a correta interpretação da Lei.

A LGPD tem como objetivo regulamentar o tratamento de dados pessoais pelas empresas, vez que os dados pessoais ganharam grande importância na economia moderna, pois permitem fazer predições, analisar perfis de consumo, opinião, definir políticas públicas, entre outras atividades.

O conceito de dado pessoal (artigo 5º, I) é bastante abrangente, sendo definido como a "informação relacionada a pessoa identificada ou identificável". Isso quer dizer que um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa natural por trás do dado, como por exemplo: nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, Carteira de Trabalho, passaporte e título de eleitor), endereço residencial ou comercial, telefone, *e-mail*, *cookies* e endereço IP[3].

Os dados pessoais sensíveis (artigo 5º, II) são uma subcategoria que, por sua relevância e importância, demandam mais proteção do que um dado pessoal comum. São estes dados 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.

Quando temos um dado que não pode identificar, de forma direta ou indireta, um indivíduo, temos o que a Lei chama de dado anonimizado. Em tempos de *Big Data*[4], em que os dados, estruturados e não estruturados, vêm das mais variadas fontes e são tratados dentro dos mais diversos sistemas, é essencial que as empresas redobrem a atenção com a segurança e a idoneidade das informações (CHIAVEGATTO FILHO, 2015, 325-332).

Tratamento (artigo 5º, II) é 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, modificação, comunicação, transferência, difusão ou extração;

Titular (dos dados) é a pessoa natural a quem se referem os dados pessoais que são objetos do tratamento. Controlador é pessoa natural ou jurídica, de direito público ou privado, responsável por tomar decisões referentes ao tratamento de dados pessoais. Operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador. Agentes de tratamento (de dados) são o controlador e o operador; Encarregado (D.P.O) é o responsável (dentro da empresa) por fiscalizar o cumprimento da legislação.

Consentimento é a livre manifestação, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Bloqueio é suspensão temporária de qualquer operação de tratamento de dados.

Transferência internacional de dados é transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro e uso compartilhado de dados é comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento

[3] **Internet Protocol** é um número identificador dado ao seu computador, ou roteador, ao conectar-se à rede. É através desse número que seu computador pode enviar e receber dados na internet.

[4] Informações produzidas em ambiente digital, a partir de ações dos usuários, que são organizadas e compiladas com base em algoritmos matemáticos.

compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais.

2 REGIME LEGAL DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A Lei define que o tratamento de dados pessoais deve observar a boa-fé e os princípios da Finalidade, Adequação, Necessidade, Livre Acesso, Qualidade dos Dados, Transparência, Segurança, Prevenção, Não Discriminação e Responsabilização e Prestação de Contas.

Desta forma, a realização do tratamento deve estar vinculada à propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, limitadas ao mínimo necessário para a realização de suas finalidades.

Devem ser adotadas 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, com demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção (DONEDA, 2005, P. 160-161).

A LGPD, em seu artigo 7º, lista as hipóteses taxativas permitidas para tratamento de dados pessoais.

A primeira forma é o consentimento pelo titular através de manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma determinada finalidade (artigo 7º, I). É a hipótese mais utilizada, por sua facilidade de obtenção, e a mais frágil das hipóteses de tratamento, e somente deverá ser obtida quando nenhuma das demais opções tenham cabimento.

Uma prática comum em sites e aplicativos, que são as opções de consentimento pré-selecionadas[5], não são consideradas manifestações de consentimento inequívoco, bem como a ausência de manifestação do titular, que não pode ser entendida como anuência para o tratamento. O controlador deve demonstrar de forma clara que foi o titular que manifestou o seu consentimento.

O consentimento dado pelo titular pode ser revogado em qualquer tempo, de forma tão simples como foi a do consentimento, gratuitamente, não implicando a eliminação dos dados coletados de forma automática, o que deve ocorrer após pedido expresso do titular.

Continuando, no artigo 7º da LGPD, são previstas outras hipóteses de tratamento de dados, que independem do consentimento do titular para que o tratamento seja considerado válido: (II) para cumprimento de obrigação legal ou regulatória pelo controlador; (III) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos, respaldadas em contratos, convênios ou instrumentos congêneres; (IV) para a realização de estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (V) para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (VI) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (VII) para a proteção da vida ou da incolumidade física do titular ou de terceiros; (VIII) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de

[5] Caixa de opções (**checkbox**) existentes em formulários digitais permitindo que o sistema colete alguma autorização ou consentimento do usuário.

saúde ou autoridade sanitária; (IX) quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e (X) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. Todo tratamento deve estar submetido a pelo menos uma destas bases legais.

Quando se tratar de dados sensíveis, a LGPD, em seu artigo 11, prevê exceções em que o tratamento pode ocorrer, sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para cumprimento de obrigação legal ou regulatória pelo controlador, tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis, exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, proteção da vida ou da incolumidade física do titular ou de terceiros, tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária e garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no artigos 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BIONI, 2018, p.14).

Havendo mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deve informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

2.1 Tratamentos de dados pessoais de crianças e adolescentes

Devido a importância do tema, a LGPD atribui um regramento único para o tratamento de dados de crianças e adolescentes, que independe de os referidos dados serem sensíveis ou não.

Em qualquer caso, o tratamento de dados de crianças e adolescentes deve ser realizado (i) no melhor interesse da criança ou adolescente (artigo 14, *caput*), (ii) mediante o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (artigo 14, §1º) e (iii) de acordo com a obrigação que os controladores têm de manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos do titular (artigo 14, § 2º).

As únicas exceções ao consentimento são (i) quando a coleta dos dados for necessária para contatar os pais ou o responsável legal e, mesmo nessa hipótese, os dados devem ser utilizados uma única vez e sem armazenamento, e (ii) para a proteção da criança ou adolescente, sendo que, em qualquer caso, os dados não podem ser repassados a terceiros sem o consentimento de pelo menos um dos pais ou do responsável legal (artigo 14, § 3º, LGPD).

Como acontece com outros dispositivos da Lei, a dispensa do consentimento para fins de proteção da criança ou do adolescente pode ser excessivamente ampla e ambígua, gerando desafios interpretativos.

Chama também a atenção a previsão do § 4º, segundo o qual

> "Os controladores não deverão condicionar a participação dos titulares, pais ou responsáveis em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade."

Procurando superar muitos dos inconvenientes da *take-ir-or-leave-it choice*[7], a LGPD prevê, como regra, que serviços ofertados pela internet para crianças e adolescentes não devem ser condicionados ao fornecimento de informações pessoais, salvo as estritamente necessárias à atividade.

Não bastassem as regras já existentes sobre os deveres de transparência e informação, o § 6º ainda prevê que

> "As informações sobre o tratamento de dados referidas neste artigo 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."

2.2 Instrumentos de segurança de dados pessoais, governança e boas práticas

Um ponto a destacar, para adequação da Proteção de Dados de maneira íntegra e transparente, se encontra na obrigatoriedade da implementação da Governança de Dados com a formulação de regras de boas práticas que constituam as condições de organização, a forma de funcionamento, os procedimentos adequados, o que inclui reclamações e petições de titulares, além das normas de segurança, os padrões técnicos, as obrigações específicas para os envolvidos no tratamento. Assim como também, as ações educativas e os mecanismos e controles internos de supervisão e a mitigação de riscos, além de outros aspectos relacionados ao tratamento de dados pessoais .

Para tanto, um programa de Governança em Privacidade deve ser estruturado sob os seguintes pilares: Transparência; Gestão de Riscos; Adaptação à realidade e tamanho e volume de operações da organização; Governança com Controles e Monitoramento; Remediação, Monitoramento Contínuo; Efetividade do Programa; Aplicação de Boas Práticas, Código de Conduta, Políticas e Procedimentos e Atualização periódica.

O controlador deve indicar encarregado pelo tratamento de dados pessoais.

A identidade e as informações de contato do encarregado devem ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

As atividades do encarregado consistem em: aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

De modo geral, a diferença entre controlador e operador está no poder de decisão. Enquanto o controlador é o responsável pelas informações, o operador é quem, a partir das ordens dadas pelo controlador, atua sobre os dados. Por isso, é essencial que o DPO conheça a legislação, tenha experiência em governança (ou seja, saiba quais informações a companhia detém) e entenda de segurança da informação.

A designação do D.P.O deve ser realizada em função das competências profissionais em especial dos conhecimentos avançados de proteção de dados e que este seja capaz de cumprir as tarefas relacionadas com a segurança e proteção de dados após a LGPD.

Privacy by Design [6] significa que todas as etapas do processo de desenvolvimento de um produto ou serviço de uma empresa devem ter a privacidade em primeiro lugar. A ideia de *Privacy by Default* (privacidade por padrão) significa que um produto ou serviço, ao ser lançado no mercado, deve vir com as configurações de privacidade no modo mais restrito possível por padrão.

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções licitadas do controlador. Os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos.

O controlador deve comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A comunicação deve ser feita em prazo razoável[7], e deve mencionar, no mínimo a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados.

A autoridade nacional pode determinar ao controlador que elabore Relatório de Impacto à Proteção de Dados Pessoais[8], inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos do regulamento, observados os segredos comercial e industrial.

A Autoridade Nacional de Proteção de Dados, ANPD, é o órgão da administração pública responsável por fiscalizar, em benefício da população e da privacidade, a adoção das corretas práticas de coleta, tratamento e compartilhamento de dados pessoais.

É importante esclarecer que não é necessário que haja o efetivo vazamento de dados pessoais para que as sanções sejam aplicadas. Já constitui infração e está sujeito aplicação de sanção a empresa que estiver em desconformidade com os processos/protocolos das atividades da pessoa à LGPD.

As sanções pelo descumprimento da Lei vão desde advertências, passando por obrigação de divulgação do incidente e eliminação de dados pessoais e multa de até 2% (dois por cento) do faturamento líquido do último período (pessoa jurídica de direito privado), limitado a R$ 50 milhões, não substituindo as sanções administrativas, civis e penais previstas em legislações específicas.

A Lei prevê alguns parâmetros[9] que devem ser observados pela Autoridade Nacional para escolha do tipo de sanção que deverá ser aplicada ao caso concreto, a fim de que não se inviabilize o próprio negócio do infrator em caso de aplicação de multa.

---

[6] **Privacy by Design**, conceito criado por Ann Cavoukian, que era a Comissária de Informação e Privacidade de Ontario – Canadá, ele surgiu na década de 90.

[7] Atualmente, a ANPD recomenda o **prazo** de dois dias úteis para a **comunicação** ser feita.

[8] O RIDP – Relatório de Impacto à Proteção de Dados - não existe na Lei a obrigação de elaboração do relatório. Deverá ser apresentado quando a ANPD solicitar (artigos 10. §3º, 32. E 38. Da LGPD).

[9] Parâmetros de aplicação das sanções: o impacto do incidente e quais dados ele afeta; se existe boa-fé por parte da empresa no tratamento dos dados; o que motivou a empresa a tratar os dados; o poder econômico da empresa; se a empresa é ou não reincidente; o dano gerado; cooperação com a ANPD e com os usuários; o desenvolvimento e aplicação de medidas tecnológicas e organizacionais que auxiliem na prevenção do dano; políticas de boas práticas e governança; adoção de medidas corretivas; a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Além da multa, as empresas que não se adequarem à legislação também enfrentarão outras penalidades, bem como a dificuldade de fechar parcerias com outras empresas.

3 ETAPAS PARA ADEQUAÇÃO À LEI

Após uma breve leitura pelos principais pontos da Lei, passamos a entender a urgência da necessidade de adequação das empresas à LGPD.

As pequenas, médias empresas e *startups*[10] sentirão maior impacto na aplicação da Lei, já que até então não estavam obrigadas a se preocuparem com governança corporativa[11] e *compliance*, prática presente em quase todas as grandes empresas.

Dependendo do tamanho da empresa, quantidade de departamentos e áreas que tratam com dados pessoais, grau de sensibilidade dos dados[12], nível de maturidade de sistemas [13]e processos, comprometimento da administração e orçamento disponível, o prazo para implementação de um projeto de adequação da empresa à LGPD poderá levar de 6 (seis) até 24 (vinte e quatro) meses[14].

A adequação à LGPD é um processo que envolve toda a empresa, pois interfere na cultura de como se lida com informações pessoais. Para que este processo tenha chances de sucesso é fundamental que os executivos estejam envolvidos desde o início do plano de adequação e que a proteção de dados pessoais esteja incorporada aos valores da empresa, e assim, o tema ganhe engajamento e força necessária.

O passo seguinte é a escolha de um líder para a coordenação do plano de adequação, com identificação das principais áreas da empresa afetadas pela LGPD e eventuais legislações setoriais, mapeando os processos e os tratamentos de dados mais críticos, o estabelecimento das ações a serem tomadas e reportar o andamento do processo para os executivos da companhia.

Se viável, estruturar uma área de Proteção de Dados, com a contratação de um D.P.O interno ou externo e criar um programa de governança em proteção de dados com a elaboração de medidas e controles para o acompanhamento da implantação de padrões que estejam em conformidade com a LGPD e legislações setoriais aplicáveis. Criar um sistema de diagnóstico e registro das operações de tratamento com identificação da base jurídica que legitima os tratamentos.

No campo jurídico, elaborar e rever documentos legais com a realização de eventuais adendos aos contratos existentes para adequação aos padrões de proteção de dados, principalmente para aqueles que envolvam o tratamento e compartilhamento de dados pessoais.

Os contratos devem conter cláusulas específicas informando sobre os processos e metodologias de coleta, tratamento, finalidade de uso, prazo de utilização, armazenamento, segurança, backups e destruição dos dados.

---

[10] **Startup** é uma empresa nova, com um modelo de negócios inovador e disruptivo, repetível e escalável, em um cenário de incertezas e soluções a serem desenvolvidas. Se não houver inovação será considerada uma empresa de modelo tradicional.

[11] Governança corporativa é um conjunto das melhores práticas para gerir uma empresa. Trata-se da gestão em si, que envolve, direta e indiretamente, acionistas, diretoria e os órgãos de fiscalização.

[12] Grau de sensibilidade dos dados – público, interno e restrito;

[13] ISO 27001 – (0) Inexistente, (1) Inicial, (2) Repetível, (3) Definido, (4) Gerenciado e (5) Otimizado.

[14] Prazo para implementação – cada empresa é um caso único. No caso estudado neste documento o prazo estimado foi de 12 meses.

Realizar treinamentos internos para apresentação das novas políticas de proteção de dados pessoais e disseminação da cultura empresarial sobre o tema.

Desenvolver um controle para garantir o exercício dos direitos dos titulares, mediante confirmação da implementação de medidas técnicas e organizacionais e criar um canal de comunicação dedicado ao exercício dos direitos dos titulares e registo de violações de dados pessoais, por exemplo, um sítio eletrônico (LEME, BLANK, 2020, p. 210-224).

4 ESTUDO DE CASO: IMPLEMENTAÇÃO DE ADEQUAÇÃO DA LGPD EM CLÍNICA MÉDICA

Apresentamos a seguir um resumo do processo para a implementação da adequação da LGPD em uma clínica para tratamento oncológico, com equipe composta por médicos oncologistas, hematologistas, reumatologistas, cirurgiões oncológicos, farmacêuticos, e enfermeiros, contando ainda com parcerias em nutrição e odontologia especializados em oncologia.

A clínica atende pacientes particulares e conveniados de diversos seguros e planos de saúde nacionais. O número de circulação diário de pacientes e pessoas envolvidas no processo é grande, e para isso existe controle de câmeras de monitoramento interno e registro de visitantes e pacientes em tratamento.

4.1 O projeto de implementação da LGPD

Devido ao grande número de tratamentos de dados existentes em uma clínica e o custo de implementação de um processo de adequação à LGPD, focamos o trabalho em três áreas mais críticas, selecionadas por possuírem maior número de tratamento de dados em desconformidade com a Lei, demandando maior urgência na adequação com maiores riscos de sanções:

A área Clínica, composta de consultórios médicos e de nutricionistas, sala de atendimento multidisciplinar, sala de emergência, farmácia de manipulação especializada e área de infusão de medicamentos e quimioterapia; a área Administrativa, composta pela diretoria administrativa, gerências financeira e recursos humanos e a área da Recepção, composta pela recepção, encarregada de recepcionar clientes, fornecedores, visitantes e encaminhar documentos e pessoas aos demais departamentos da clínica, bem com receber e despachar documentos.

Após a definição das áreas, definimos quais são os departamentos e os processos mais complexos e que apresentavam mais riscos de vazamentos de dados e possibilidades de sanções, caso não estivessem em conformidade com a LGPD.

Em seguida, elaboramos o cronograma de ações, baseado nas definições das áreas, departamentos e processos e os agendamentos de reuniões e entrevistas para a fase inicial do projeto, gerando o documento de *kick-off* [15] do projeto, marco inicial do projeto.

[15] O **kick off** é uma reunião realizada na fase inicial de um projeto com o intuito de alinhar todos os detalhes entre os atores envolvidos - o cliente, o gestor do projeto e os membros da equipe, por exemplo.

4.2 Análise da situação atual

A execução de análise situacional das organizações perante a LGPD exige estabelecer um correto sequenciamento de processos para implantação das diretrizes estabelecidas na lei, que alteram e afetam o comportamento dos processos e sistemas.

O *Gap Analysis*[16] da LGPD foi divido em fases, que permitiu um melhor aproveitamento dos resultados obtidos na fase anterior, sendo composto de:

a) Estabelecimento de escopo: a organização precisa entender e aplicar as práticas da LGPD a partir de um escopo mínimo, significativo, que conduza ao desenvolvimento de uma cultura de proteção de dados pessoais, permitindo que haja uma melhor compreensão por parte das equipes envolvidas sobre as necessidades e adaptações dos processos e sistemas com o mínimo de impacto às operações do negócio.

b) Análise da base ou arcabouço legal: A aplicação da LGPD nos processos e sistemas da organização envolve muito mais que o próprio Lei[17]. A compreensão das leis e normas aplicáveis ao escopo dos processos ou sistemas que tratam dados pessoais é essencial para que possam ser desenvolvidos elementos importantíssimos da LGPD como matrizes de temporalidade e consentimento. Assim, a avaliação de todo arcabouço legal aplicável e indica as necessidades de adequação em contratos, normas, políticas e demais elementos que possam auxiliar na efetiva implantação da LGPD.

c) Análise dos dados lógicos: Utilização de métodos e ferramentas especificas para a identificação das interfaces de coleta de dados[18], conjunto de dados pessoais tratados e as bases e estruturas lógicas de armazenamento. Além da análise dos elementos tecnológicos envolvidos, são realizados mapeamentos junto aos responsáveis pelo processo e sistema para identificação de eventuais pontos de guarda física de dados pessoais, práticas adotadas para tratamento (incluindo guarda e descarte) e controles implantados, gerando assim um mapa detalhado dos dados pessoais tratados pela organização. O resultado obtido é uma documentação prática que permite aos gestores entender em detalhes todo o conjunto de dados pessoais tratados e controles já implantados e adequados às diretrizes da LGPD além do conjunto de fluxos de dados e de solicitações dos titulares de dados conforme estabelecido na lei.

d) Avaliação de controles de segurança em sistemas eletrônicos: Na grande maioria dos casos o tratamento de dados é realizado por meio de sistemas eletrônicos mantidos pela organização. Deverão ser analisados os sistemas de segurança[19] para identificação de vulnerabilidades para identificação de pontos de vazamento de informação ou riscos inerentes aos dados pessoais tratados. O resultado imediato é a identificação da existência ou

[16] Na implementação da LGPD, o **GAP Analysis** (análise de lacunas) procura encontrar práticas e processos empresariais que não estejam de acordo com os princípios da legislação. A partir desse mapeamento, o **GAP Analysis** sugere melhorias, a fim de que a empresa fique em conformidade com a lei.

[17] Aplicação de ISO 27001 (Normas técnicas de Segurança da Informação), Redes, Programação, Banco de Dados etc. além da área jurídica.

[18] Neste caso, formulários eletrônicos, geralmente na internet ou rede interna, onde os usuários inserem informações nos sistemas (como exemplo, formulário eletrônico para autorização de consultas ou exames de plano de saúde).

[19] A ISO 27001 é a norma que traz princípios e controles de sistema de segurança da informação e evidencia o compromisso da empresa com a segurança da informação.

Como a própria norma define, é seu dever prover requisitos para estabelecer, implementar, manter e melhorar, continuamente, um sistema de gestão de segurança da informação por meio da aplicação de um processo de gestão de riscos e fornecer às partes interessadas confiança de que os riscos são adequadamente gerenciados.

necessidade de implantação de controles nos códigos fonte ou na infraestrutura tecnológica de suporte ao tratamento dos dados nos sistemas da organização.

e) Elaboração do Plano de Comunicação e Resposta a Incidentes: A correta gestão de incidentes[20] envolvendo dados pessoais é um dos pontos de grande relevância da LGPD. Assim, com auxílio de ferramenta sistêmica, deverá ser elaborado o plano de comunicação e resposta a incidentes que permite às organizações gerenciar de modo prático e padronizado as questões de quebra de segurança aplicadas no contexto da LGPD. O plano é desenvolvido a partir de um fluxo adaptado aos novos papéis e funções criadas pela lei e permite que haja correto controle dos prazos e comunicações junto às partes interessadas.

f) Plano de ação: ponto culminante de todo trabalho, o plano de ação traz todas as atividades necessárias para implantação ou adequação identificados ao longo do projeto em formato adequadamente sequenciado de acordo com a realidade da organização. Também são incluídas informações de esforço e investimentos necessários para correta adequação do processo/sistema à LGPD. Com a aplicação do plano de ação as equipes são envolvidas e adaptadas para posterior ampliação do escopo e, assim, envolver todos os dados pessoais da organização em ciclos bem definidos e com resultados práticos.

4.3 Desenvolvimento do trabalho de adequação

O trabalho de adequação à LGPD foi desenvolvido em quatro frentes:

a) Levantamento de Dados: entrevistas com os responsáveis dos departamentos que efetuam o tratamento de dados pessoais e sensíveis, a fim de conhecer os titulares e as categorias de dados tratados, documentar a situação encontrada e elaborar o mapeamento dos dados por setores;

b) Levantamento dos Documentos Jurídicos: entrevistas com os responsáveis dos departamentos que efetuam tratamento de dados pessoais e sensíveis, com a finalidade de conhecer os principais documentos e contratos, documentar a situação encontrada e indicar as vulnerabilidades e as adequações;

c) Mapeamento de Dados e Definição de Base Legal: mapeamento dos dados coletados na etapa 15.3.1, definição das bases legais para cada tratamento realizado, mapeando os titulares e as categorias de dados envolvidos, avaliação dos riscos e formas de mitigação, levantamento dos sistemas utilizados, entradas e saídas de dados dos processos, os destinatários de dados, as medidas técnicas e administrativas de segurança utilizadas, os responsáveis envolvidos, identificação do papel da empresa (controlador, operador ou responsável) no tratamento das atividades e elaboração do relatório de atividade de dados;

d) *Compliance:* elaboração do plano de ação para prevenção de vazamento de dados, com implantação de medidas de *compliance*, definição de um D.P.O (*data protection officer*), interno ou externo, geração de controles de registros de solicitação de titulares, geração

[20] Plano de Respostas a Incidentes consiste em um documento interno da empresa que deve ser amplamente conhecido por todos os funcionários e que dispõe sobre as medidas que devem ser tomadas no caso de um Incidente de Segurança em Dados Pessoais.

de relatório de impacto à proteção de dados pessoais, controle da validade dos dados armazenados, eliminação dos dados desnecessários (higienização[21] de bases de dados), anonimização dos dados e definição dos processos de acompanhamento e prestação de contas das atividades executadas.

O trabalho mapeou os seguintes tratamentos de dados (sentido duplo) existentes nas áreas analisadas (recepção, administrativa, financeira e recursos humanos): a) Recepção e Clínica (Médicos, Nutricionistas, Farmácia); b) Recepção e Pacientes; Recepção e Terceiros (Fornecedores, Visitantes); c) Financeiro/RH e Contabilidade; d) Financeiro e Colaboradores; e) Financeiro e Planos de Saúde; g) Financeiro e Administrativo; h) Financeiro e Bancos e i) Financeiro e Fornecedores.

Foram aplicadas as seguintes bases legais para os tratamentos de dados: a) Consentimento do Titular; b) Interesse Legítimo do Controlador e c) Obrigação Legal / Regulatória.

Foram identificados os seguintes titulares de dados: a) Pacientes (maiores de idade); b) Pacientes (crianças ou adolescentes); c) Pacientes (incapazes); d) Acompanhantes; Médicos; e) Nutricionistas; f) Enfermeiros; g) Administradores; h) Colaboradores; i) Terceiros (zeladores, limpeza, segurança etc.) e j) Fornecedores e Visitantes.

As principais fontes de coletas de dados nos tratamentos estudados foram: a) Fichas Recepção (dados do paciente e responsáveis etc.); b) Contratos (pacientes, emprego, terceirizados, bancários etc.); c) Ficha Médica; d) Ficha Nutrição; e) Planos de Saúde (sistemas web, guias, formulários eletrônicos etc.) ; f) Bancos e g) Contabilidade e Currículos.

Os dados coletados dos titulares de dados analisados no processo, foram: a)Dados Pessoais – nome, sexo, nascimento, raça etc.; b) Dados Contatos – telefone, e-mail, redes sociais etc.; c) Dados Identificáveis – IP, geolocalização etc.; d) Dados Residenciais – endereço etc.; Dados Profissionais / Comerciais – empresa, endereço, telefone, e-mail etc.; e) Documentos Pessoais – CPF, RG, CNH, CTPS etc.; f) Dados Médicos – Ficha anamnese, doenças pré-existentes, medicação etc.; g) Dados Tratamentos Médicos – tratamentos, medicação etc.; h) Dados Psicológicos – tratamentos etc.; i) Dados Financeiros / Bancários – conta corrente, cartão de crédito, PIX etc. e j) Outros - imagens de vídeos, autorização entrada, estacionamento etc.

Os principais receptores dos dados transmitidos pela clínica para tratamento em controladores e operadores externos são: a) Planos de Saúde (sistemas web, guias, formulários eletrônicos etc.) e b) Bancos e Contabilidade e Laboratórios de Análises Clínicas.

Após análise sistêmica, foi criado o relatório de *Gap Analysis*[22] e levantados os seguintes *Gaps* Operacionais e Sistêmicos com grau de risco nível **MÉDIO –ALTO:** a) Transferências de documentos (dados) entre departamentos é feito de forma manual (papel) ou por planilhas; b) Exposição de dados pessoais e sensíveis sem controle, bastando pequenos descuidos como deixar documentos em cima de mesas, gavetas destrancadas etc.; c) Não existe controle de acesso à sala de Arquivo, e a porta fica aberta durante o dia sem monitoramento através de câmeras; d) Acesso aos sistemas dos convênios via Internet, através de senha fornecida pelos administradores dos sistemas, sem restrições claras de permissão de usuários; e) Acesso e contato com pessoas desconhecidas, sem vínculo com a clínica, facilitam obtenção de documentos deixados sobre balcão de atendimento.

[21] A higienização de dados consiste no processo de limpar, organizar e padronizar um banco de informações. Neste processo, registros repetidos, dados incompletos ou com informações erradas etc. são eliminados ou corrigidos.

[22] Na implementação da LGPD, o **Gap Analysis** procura identificar práticas e processos empresariais que não estão de acordo com as prescrições legais. A partir desse mapeamento, o **Gap Analysis** propõe melhorias e ajustes, com a finalidade da empresa se adequar à legislação.

Na área do ordenamento jurídico, levantados os seguintes *Gaps*, com grau de risco nível **Médio –Alto:** a) Ausência dos Termos de Consentimento Livre e Esclarecido e dos Termos de Consentimento (tratamentos médicos); b) Ausência de cláusulas específicas sobre LGPD nos contratos com fornecedores; c) Ausência de documento específico sobre LGPD para regular a relação da Clínica com os planos e seguros de saúde; d) Risco da Clínica sofrer demandas judiciais, pedidos de indenização, multas, bloqueio dos sistemas, etc.

O resultado do *Gap Analysis* apresentou os maiores riscos a serem considerados: a) Dados Sensíveis ou com Natureza Extremamente Pessoal; b) Combinação de Bases de Dados (planilhas); c) Decisões Manuais sem devida proteção de dados e d) Dados em papéis.

Finalizando, foram apresentadas as seguintes recomendações sistêmicas e operacionais para a adequação à LGPD: a) Criar Comitê de Segurança da Informação – CSI[23]; b) Treinar e Conscientizar o CSI; c) Avaliar a Infraestrutura de TI, Sistemas e Fornecedores; d) Mapear e inventariar os Tratamentos de Dados, os Titulares, os Dados Pessoais e Sensíveis, as Fontes de Coleta de Dados e os Receptores dos Dados; e) Elaborar o fluxograma do Ciclo de Vida dos Dados[24]; f) Planejar de Ações Prioritárias e Ajustes nas áreas de TI e Operacionais; g) Redigir Normas de Governança de Dados; h) Adotar Medidas Preventivas de Segurança[25]; i) Elaborar Plano de Contingência[26]; j) Elaboração de Documentação Legal (Relatório de Impacto de Dados) e k) Nomear um D.P.O (data protection officer).

E apresentadas as seguintes recomendações jurídicas: a) Elaboração do Termo de Consentimento Livre e Esclarecido do paciente adulto, criança e adolescente, pessoa com deficiência e idoso; b) Elaboração do Termo de Consentimento para Tratamento de Dados LGPD do paciente adulto, criança e adolescente, pessoa com deficiência e idoso; c) Elaboração do Termo de Consentimento de Tratamento de Dados LGPD empregados contratados CLT; d) Elaboração do Termo de Consentimento de Dados LGPD prestadores de serviços; e) Análise de contratos com fornecedores para adequação à LGPD e f) Elaboração de documento informando aos planos ou seguros saúde que os dados dos pacientes transmitidos/recebidos são tratados em conformidade com a LGPD.

Foram ainda listadas as seguintes ações de caráter imediato para mitigação dos riscos e recebimento de sanções por desenquadramento à Lei: a) Definir responsáveis pelas funções de gestão, controle e fiscalização relacionadas a LGPD (D.P.O); b) Elaborar Termo de Consentimento para Tratamento de Dados LGPD para coleta de assinatura nos atendimentos na Recepção; c) Gerenciar e Armazenar os Termos de Consentimento de forma digital e em papel em locais seguros, sob responsabilidade de um gestor; d) Configurar, divulgar e-mail específico para recebimento de comunicações e reclamações de titulares sobre privacidade de dados: dpo@xxxxxx.com.br e gerir comunicações recebidas; e) Criar documento de Política de Privacidade e disponibilizar no site institucional e nas Redes Sociais; f) Conscientizar e treinar cola-

[23] O Comitê de Segurança da Informação é de natureza deliberativa, possuindo poder de decisão sobre os assuntos relativos à Segurança da Informação ou riscos de TIC (Riscos de Tecnologia da Informação e Comunicação).

[24] O ciclo de vida dos dados é o processo que descreve o caminho dos dados dentro da sua organização — desde o momento em que o dado é coletado por consentimento ou outra base legal até o arquivamento ou eliminação dos mesmos.

[25] São inúmeras as medidas a serem ser adotadas, mas as mais importantes são: detectar vulnerabilidades de hardware e software, criar e manter cópias de segurança, possuir sistemas redundantes, ser eficaz no controle de acesso, elaborar política de segurança da informação, decidir corretamente pela estrutura de nuvem pública/privada/híbrida, gerir riscos de forma apropriada e trabalhar com regras de negócio bem definidas, entre outras.

[26] Plano de Contingência é um documento onde estão definidas as responsabilidades estabelecidas em uma organização, para atender a uma emergência e contêm informações detalhadas sobre as características da área ou sistemas envolvidos.

boradores e terceirizados sobre a importância de adequação à LGPD e consequências no descumprimento da legislação; g) Implementar política de "Mesa Limpa e Tela Limpa"[27] e verificação de salas, arquivos, armários e gavetas trancadas; h) Definir protocolos e regras rígidas para o processo e i) Informar os envolvidos no tratamento sobre responsabilidades no caso de vazamento de dados.

Após a conclusão das fases anteriores, foram documentadas as principais ações de adequação à LGPD, e finalizando, apresentadas as medidas mais urgentes a serem tomadas para a conformidade LGPD da clínica.

O término do projeto é marcado pelas entregas à direção da empresa dos seguintes relatórios: a) Relatório de Atividades de Tratamento de Dados, com os Mapeamentos de Dados; b) Relatório de Análise de Gaps; c) Relatório de Mapeamento de processos de negócios e definição das Bases Legais para os Tratamentos de Dados; d) Relatório com Avaliação dos dados pessoais e o Fluxo de Dados dos tratamentos de dados realizados pela clínica; e) Relatório de Identificação das situações de desconformidade com a LGPD, com indicações de níveis de risco; f) Elaboração de Política Interna de Proteção de Dados; g) Elaboração de Política de Privacidade; h) Elaboração de Política de Retenção e Descarte de Dados; i) Elaboração de Termos de Consentimentos; j) Elaboração de Aditivos específicos aos contratos vigentes com clientes, fornecedores, colaboradores, planos de saúde etc., sobre os tratamentos de dados e responsabilidades; k) Elaboração de Documentações específicas para Planos de Saúde; l) Elaboração de Documentação com Definições de Temporalidade para guarda de documentos e processos de descarte; m) Realização de treinamentos visando capacitação dos operadores de dados e D.P.O; n) Elaboração e entrega do Relatório de Impacto à Proteção de Dados aos executivos da clínica; o) Termo de Encerramento de Execução do serviço e p) Emissão de Certificado de Conformidade e *Compliance* à Lei Geral de Processamento de Dados.

CONCLUSÃO

A Lei Geral de Proteção de Dados exigirá das empresas adequação dos processos de tratamento de dados, com um efetivo mapeamento das informações pessoais armazenadas em seus sistemas, elaboração de novos contratos e revisões dos contratos existentes, obtenção de consentimento específico para coleta de dados e definição de bases legais para o tratamento.

O processo de tratamento de dados, de natureza dinâmica, exigirá uma manutenção contínua dos mapeamentos das atividades de tratamento de dados, atendimento aos titulares e prestação de informações à autoridade de dados.

Atividades complementares, como cobertura de todas etapas do ciclo de vida dos dados desde o levantamento inicial dos processos e dados coletados, análise de finalidade e sanitização das informações, mapeamento das atividades de tratamento de dados e vinculações com bases legais, titulares, categoria de dados pessoais e sensíveis, matriz de risco, sistemas e fluxo de dados, registro e controle de requisições de titulares, violação de dados e geração de relatório de impacto de dados, auditorias, gestão de alterações de contratos, documentos, fluxo de dados, agendas, lista de tarefas e controle de treinamentos até emissões de certificações de usuários e responsáveis.

[27] A Política de Mesa Limpa e Tela Limpa reúne diversas práticas de segurança que visam proteger dados e informações, em formato digital ou impresso, do acesso, divulgação ou uso não autorizados, bem como perda, fraude ou outro tipo de dano. Para isso, é recomendada uma série de ações que os usuários devem tomar sempre que deixarem sua área de trabalho, tanto por curtos períodos quanto no final do expediente. Faz parte da ISO 27001.

Devido à complexidade da tarefa de adequação à LGPD, possuir vasto e sólido conhecimento da Lei e regulamentos setoriais, suas características tecnológicas profundamente ligadas com segurança da informação e dispor de suporte (pessoas e sistemas) para o controle dos processos envolvidos é fundamental para que o resultado planejado seja alcançado.

Ainda que todo o trabalho possa ser feito de forma mais simples, com utilização de planilhas eletrônicas e controles em diversas ferramentas, a utilização de sistemas especializados[28] para *compliance* de GDPR, LGPD e outras leis de proteção de dados no mundo, que centralizam todos os procedimentos e etapas da conformidade, além de servirem como controle do processo, são uma maneira de otimizar o trabalho e angariar novos clientes e negócios.

REFERÊNCIAS

BIONI, BR. Proteção de Dados Pessoais. **A Função e os Limites do Consentimento**. Rio de Janeiro: Forense, 2018.

BLANK, M. LEME, RS. **Lei Geral de Proteção de Dados: Entendendo a Lei. Manual de Implementação**. São Paulo: Blank Sistemas Ltda. (1-22). Julho 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Brasília, DF: Presidência da República; 2018 [Acesso em 12. jun.2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

BRASIL. Medida Provisória nº 959 de 2020. **Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD** (institui regras para o auxílio emergencial e adiamento da LGPD). Brasília, DF: Presidência da República; 2020 [Acesso em 12.jun.2020]. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. **Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.** Brasília, DF: Presidência da República; 2020. [Acesso em 14.mar.2022] Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm

CHIAVEGATTO FILHO ADP. **The use of big data in healthcare in Brazil: perspectives for thenear future**. Epidemiol. Serv. Saúde, Brasília, 24 (2):325-332, abr-jun, 2015.

DONEDA, D. **Da privacidade à proteção de dados**. Rio de Janeiro: Renovar, 2005.

LEME, RS; BLANK M. **Lei Geral de Proteção de Dados e Segurança da Informação na Área da Saúde**. Cadernos Ibero-Americanos de Direito Sanitário. 2020 jul/set.; 9(3): 210-224.

[28] GDPR365, OneTrust Privacy (OneTrust), Secure Privacy, Onspring, Netwrix Auditor, Vigilant Software GDPR Manager, ManageEngine Event Log Analyzer, Audit Board, SolarWinds Access Rights Manager, LogicGate Risk Cloud, ZenGRC Really Simple Systems, ECOMPLY.io, Files.com, archTIS, etc.

MALDONADO, VN, BLUM RO. **LGPD Lei Geral de Proteção de Dados comentada**. São Paulo: Thomson Reuters Revista dos Tribunais, 1ª edição (18 março 2019).

MALDONADO, VIVIANE NÓBREGA (Org.). **LGPD Lei Geral de Proteção de Dados Pessoais: Manual de Implementação**. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.