Revista Científica
O DIREITO PENSA
v.3 n.2
ISSN 2675-844X

LEI GERAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO DE *COMPLIANCE* NA SAÚDE

LAW OF GENERAL DATA PROTECTION AS AN INSTRUMENT OF COMPLIANCE IN HEALTH

Carla Ayume Ayabe Pereira[1]

Resumo: Na pesquisa realizada se analisa os impactos da Lei Geral de Proteção de Dados, na qual se buscou entender se ela pode vir a atuar como um novo instrumento de *compliance* nas organizações de saúde. Para tanto utilizou-se do método hipotético-dedutivo. Primeiramente, no estudo do *compliance* aplicado às organizações da saúde. Em seguida, examinando-se o que seriam dados pessoais, dados pessoais sensíveis e o seu tratamento. Por seguinte, como as entidades da saúde podem estar em conformidade com a LGPD e, por fim, se a mesma proporciona uma nova camada de *compliance* na saúde.

Palavras-chave: legislação.integridade.medicina.

Abstract: The survey analyzed impacts of the General Data Protection Law, which sought to understand whether it could act as a new *compliance* in health associations. For that, the hypothetical-deductive method was used. First, in the study of *compliance* applied to organizations. Then, examining what would be personal data, specific personal data anda their treatment. Next, how health entities can be in *compliance* with LGPD and, finally, whether they offer a new layer of health *compliance*.

Keywords: legislation.integrity.medicine.

1. Introdução

Em um mundo altamente globalizado, onde as informações trafegam em uma velocidade e quantidade nunca antes vista, os dados pessoais e dados sensíveis passaram a ter em nossa sociedade um alto valor agregado, revelando preferências de consumo, características peculiares do usuário e, na saúde, podem ter uma importância muito maior, ao explicitar dados genéticos e também possibilitar posturas de discriminação contra os titulares dos dados colhidos.

É nesse contexto que a Lei Geral de Proteção de Dados surge para regulamentar e proteger os dados pessoais do uso e tratamento indevidos, trazendo em suas disposições todo um arcabouço no intuito de estruturar a licitude do tratamento de dados. Mas a LGPD traça um desafio as instituições como um todo, e em especial as ligadas a saúde, que pela intrínseca

[1] Pós Graduada em Direito Civil pela Universidade Estadual de Maringá; Servidora Pública; Maringá; Paraná; Brasil; carlapereira89@outlook.com.

complexidade de sua estrutura e por ser grande responsável na colheita de dados sensíveis podem ter mais dificuldades em estar em conformidade com a lei.

Um caminho para estar essa conformidade poderia ser as instituições equiparem sua estrutura com um programa de *compliance* efetivo. Sendo que, dada a generalidade e alcance da LGPD que afeta toda a envergadura das organizações, se indaga se a LGPD poderia ser considerada com um novo instrumento de *compliance* nas instituições de saúde? Procura-se responder essa pergunta através do desenvolvimento do presente trabalho, destrinchando o tema através do estudo do que seria o *compliance* nas organizações de saúde, o que são dados pessoais, dados pessoais sensíveis e o seu tratamento na LGPD, os meios das quais as organizações de saúde podem se utilizar para estar em conformidade, dos métodos adequados para proteção de dados, e mais especificamente, tratando da LGPD e o *compliance* nas organizações da saúde. Sendo que, toda a pesquisa realizada foi estruturada pelo método hipotético dedutivo, através de extensa leitura de livros, artigos e reflexão.

2. O *compliance* e as organizações

A importância de um programa de *compliance* nas instituições tem cada dia mais se tornado essencial, pois ele tem como sua principal característica a prevenção de riscos (CARLINI,2020, p.33). Tendo se mostrado uma área de forte adaptação devido aos diversos avanços tecnológicos e alterações comportamentais ocorridos em sociedade.

O *compliance* vem sendo aplicado no Brasil desde a década de 1990, como meio de mitigar riscos em diferentes áreas, em especial no combate à corrupção. Tanto é que veio se tornar objeto de diversas leis, como na lei nº 8.429/1992, pela lei nº 9.613/1998, pela lei nº 12.683/2012, que ampliou os setores obrigados a criar um sistema de *compliance* (DUARTE, 2020, p. 147). Mas o destaque veio com a promulgação da Lei nº 12.846/2013 a chamada "Lei Anticorrupção", ao dispor que dentre os fatores considerados para aplicação de sanções a adoção pela entidade de um programa de *compliance* efetivo que poderia influenciar positivamente na dosimetria da pena (DUARTE, 2020, p. 147).

Apesar dos avanços legislativos ocorridos na última década em torno da obrigatoriedade e efetividade dos programas de conformidade, o fato é que a legislação ainda é esparsa e não o estrutura de forma sistemática (DUARTE, 2020, p. 147). Pois, não existe concretamente uma norma que dê unidade, capaz de servir de verdadeiro guia no sentido de orientar todas as organizações que têm atribuições de *compliance* (DUARTE, 2020, p. 156).

Pois adotar um programa de *compliance* não se resume apenas a estar em conformidade com as leis, porque ele é dotado de uma metodologia de aplicação toda própria, que se embasa em avaliar e definir um conjunto de medidas que permita frente a um cenário de possíveis riscos delimitar como a organização deve estruturar sua atividade de modo que se mantenha num nível aceitável de risco, mitigando o quanto possível os danos advindos de suas ações, estruturando todo um sistema (DUARTE, 2020, p. 149). E, caso o ilícito já tenha ocorrido, deve propiciar o imediato retorno ao contexto de normalidade e legalidade (CARLINI, 2020, p.32).

O *compliance* se aplica a todos os tipos de organização, visto que o mercado tem exigido a adoção de condutas éticas e legais em suas transações, que devem buscar a lucratividade de forma sustentável (RIBEIRO; DINIZ, 2015, p. 88). Mas cada programa deve ser personalizado para cada instituição, contendo sua estrutura, aplicação e atualização de acordo com as peculiaridades e riscos das atividades de cada pessoa jurídica, que deve também zelar pelo refinamento e adaptação contínua do programa, visando torná-lo efetivo (CARLINI, 2020, p.33).

Assim, cada programa de *compliance* é próprio, não existindo um formato uno que possa ser replicado de forma satisfatória em todas as entidades, mas a maioria deles traz alguns pontos em comum, como os cinco pilares do Programa de Integridade elaborado pela Controladoria Geral da União, que resumidamente, dita a necessidade do comprometimento da alta direção com a criação de um programa de integridade, instituindo uma instância responsável por ele que analise de forma sistêmica perfil e riscos da organização, elaborando regras, instrumentos e formas de sanção. E, quando criado e operante passe ser objeto de monitoramento contínuo no intuito de identificar e tratar vulnerabilidades encontradas (BRASIL, CGU, 2015).

Um dos objetivos básicos do *compliance* é implantar um sistema de gestão na instituição que possibilite que ela atue dentre dos níveis aceitáveis de riscos de sua atividade, para isso é imprescindível que esse sistema concretize as obrigações de *compliance* que podem estar contidas em diversos materiais como: “previstas em normas externas (leis, regulamentos, instruções normativas, emanadas da administração pública e de agências reguladoras), e /ou normas internas (códigos de ética e conduta, políticas e procedimentos” (SAAVEDRA, 2020, p. 52).

É por meio do “Código de Ética que a empresa expõe seus valores, comunica-os aos funcionários e à sociedade e define o padrão ético-comportamental que deles de espera” (CREDIDIO, 2018, p. 88). No qual deve ser escrito de forma clara e objetiva para que possa

facilmente ser incorporado e seguido por todos os funcionários e terceiros que a organização possui relacionamento, especificando as condutas desejáveis e as penalidades para os que não observarem seu conteúdo (KONIG,2018, p. 21). E, também que inspirem confiança nos funcionários que caso denunciem alguma irregularidade, entendam que não haverá qualquer tipo de represália contra aqueles que se utilizem dos canais de denúncia (KNOEPKE, 2019, p.16).

Assim, o programa de *compliance* passa por sua formulação, implantação, assimilação por parte das pessoas envolvidas, equilíbrio de sua aplicação e aprimoramento de seus regulamentos. Ademais, deve-se lembrar que todo sistema de *compliance* tem a necessidade de passar por monitoramento e melhorias contínuas para que tenha capacidade de eliminar ou minorar os riscos da organização. Ainda mais, quando os avanços tecnológicos, e as mudanças de comportamento na sociedade, levam a criação de diversos riscos tanto internos quanto externos, fazendo que com a todo momento novas ameaças passem a incidir sobre a organização (SAAVEDRA, 2020, p. 54).

2.1 O compliance e o setor da saúde

Um dos fundamentos de um sistema de *compliance* é possuir a capacidade, se bem aplicado, de antever situações que possam causar danos para as partes envolvidas na atividade da organização. Assim, a prevenção é a palavra chave no *compliance* e tem na área da saúde sua importância majorada, devido aos riscos que permeiam a prestação de serviços que possuem alta lesividade e impactos irreversíveis (SAAVEDRA, 2020, p. 53).

O *compliance* na saúde deve pautar-se tanto nas normas internas e externas, e quanto a estas últimas ele possui uma extensa gama de normas protetivas, começando pelo tratamento constitucional. Ilustra-se em seus art. 197 a 199 a importância dada à saúde como direito fundamental de todo o ser humano e dever do Estado. E, a assistência à saúde do brasileiro é prestada por meio público (mediante o Sistema Único de Saúde) ou pelo sistema de saúde privado por meio da contratação de planos de saúde ou contratação direta de serviços por meio de prestadores de saúde.

Sendo que, o sistema privado de saúde tem sua regulação mediada por três órgãos, quais sejam: a Agência Nacional de Vigilância Sanitária (Anvisa), a Agência Nacional de Saúde (ANS) e, por fim, o Sistema Brasileiro de Defesa da Concorrência (SBDC), que atuam no intuito de regular econômica e sanitariamente o mercado de compra e venda de insumos

hospitalares, atuando no fluxo financeiro de serviços entre operadoras e garantindo a competitividade no setor, respectivamente (FAVERO, 2021, p. 172).

Portanto, o *compliance* na saúde precisa estar atento as disposições dos órgãos referidos, que determinam como a saúde no Brasil deve estar moldada e quais parâmetros as organizações devem se pautar. Além disso, para que uma organização sobreviva ao mercado a longo prazo, se faz necessário que alinhe seu programa de *compliance* aos objetivos estratégicos, missão e valores que propaga, se tornando algo realmente efetivo, e não apenas papel (CREDIDIO, 2018, p. 88).

Soma-se, ainda, as normas emitidas pelo Conselho Federal de Medicina extremamente importantes no *compliance* na saúde, um exemplo claro disso, é quando se aborda sobre o prontuário médico, que pode ser definido como:

> Documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo (CONSELHO FEDERAL DE MEDICINA, 2002)

Assim, por meio do prontuário médico que tem como principal função conservar o histórico do paciente, se possibilita o conhecimento do histórico de saúde, do uso de medicamentos durante o tratamento, do resultado de exames já realizados e o diagnóstico de outros profissionais, tornando-se um instrumento necessário para prestar o melhor atendimento possível e a continuidade do tratamento ao paciente, possibilitando a comunicação com os demais profissionais envolvidos na atenção ao paciente, evitando interrupções e falhas no decorrer do atendimento. Sendo que, a partir da Resolução nº 1639/2002 do CFM, o prontuário médico teve sua estrutura devidamente estabelecida, e refinada pela Resolução2.218/2018, na qual se dispôs sobre medidas de segurança e utilização de certificação digital para a feitura de tais documentos, dando mais exatidão, garantia e integridade (COSTA, 2021, p. 93).

Ademais, a Carta Magna de 1988 dispõe sobre a garantia da inviolabilidade da intimidade, da vida privada, da honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação. Essa norma atua como embasamento ao sigilo médico, regulamentado na Resolução CFM nº 1605/2000, que proíbe o médico de revelar conteúdo do prontuário ou da ficha médica sem o consentimento do paciente, constituindo ato ilícito punível de acordo com o Código Penal. Posteriormente, a Resolução CFM nº 2.217/2018 contém previsões sobre a questão do sigilo profissional, proibindo o médico de permitir o manuseio e o conhecimento do prontuário por pessoas não obrigadas ao sigilo profissional

quando sob sua responsabilidade. Soma-se, o Código de Ética Médica e o Código de Ética da Enfermagem, que preveem a proibição de se difundir fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento do paciente, por escrito (DALLARI; MARTINS, 2021, p.126).

A prestação da saúde na complexidade brasileira é um desafio, pois ambas as redes pública e privada são intrinsicamente ligadas, necessitando para um melhor atendimento, de normas, procedimentos, parâmetros que são encontrados em diversas disposições. Sejam desde as contidas na Carta Magna até as importantes resoluções emitidas pelo conselhos profissionais da saúde, que tem possibilitado às organizações criarem de acordo com suas peculiaridades programas de *compliance*, que devem propiciar ao paciente um tratamento efetivo, sempre no intuito de minorar riscos e danos ao longo do seu tratamento.

3. Dados pessoais, dados sensíveis e o tratamento na lei geral de proteção de dados

A tecnologia que vivencia-se hoje possibilita grandes avanços na saúde, ainda mais em termos de disseminação de informações, nas quais o acesso a dados médicos de pacientes por meio de prontuários eletrônicos e bases de dados estruturadas faz-se com que haja um tratamento médico mais assertivo e contínuo, porém, há os riscos inerentes aos tratamentos de dados pessoais, em especial, de dados sensíveis (COSTA,2021, p. 90).

Há que se ter em vista que:

> Dados de saúde trafegam e precisam trafegar dentro da cadeia de modo a garantir a melhor assistência do paciente e titular de dados. Exames de sangue e imagem realizados em um certo laboratório podem ser acessados pelo médico e pela equipe assistencial de um hospital para impedir a repetição desnecessária desses exames, tudo para uma adequada tutela da saúde do paciente. Dados de saúde podem ser acessados até mesmo pelo plano de saúde, desde que de forma segura e sigilosa, seja para liberar um reembolso, seja para autorizar um pagamento, seja até mesmo para evitar a exposição desnecessária à radiação, como a realização repetitiva de exames como PET-Scan, que prejudicam a saúde do paciente titular de dados (DALLARI, MARTINS, 2021, p. 121).

Porém a consulta de dados de saúde vai muito além dessas relações médico e paciente, pois são diversas as hipóteses em que os dados são tratados na saúde, como por exemplo, mediante pesquisa e desenvolvimento de produtos, tratamentos e tecnologias em saúde, prática clínica e assistencial de pacientes por profissionais ligados à saúde, atividades que envolvem controle de qualidade em indústrias farmacêuticas, dentre tantas outras que os dados de saúde trafegam (KUNG; AUN, 2021, p. 103).

Dados de saúde são relevantes pois:

> Representam a extensão da personalidade do indivíduo, extremamente importantes na privacidade, na construção de sua identidade, além de se mostrarem fundamentais para a fruição de certos direitos de cidadania. Nesse sentido, tanto o tratamento irregular como o incidente de segurança sobre dados

> de saúde podem acarretar danos incalculáveis para o paciente titular de dados, patrimoniais e morais, por conta do conteúdo sensível e do potencial altamente discriminatório e preconceituoso que o uso indevido destes dados pode representar (DALLARI; MONACO,2021, p. 5).

Ademais, tendo "o conhecimento profundo do usuário, inclusive no que diz respeito às suas fragilidades, pode ser utilizado para toda sorte de discriminações e abusos, além da manipulação de suas emoções, crenças e opiniões para os fins mais diversos, inclusive políticos" (FRAZÃO, 2019, p. 14). Se acresce que "do ponto de vista econômico, dados importam na medida em que possam ser convertidos em informações necessárias ou úteis para a atividade econômica. Consequentemente, os dados precisam ser processados para que possa gerar valor" (FRAZÃO, 2019, p.10).

Portanto, restava inconteste a necessidade de um avanço legislativo que tratasse de forma mais assertiva a questão dos dados pessoais, porque em que pese a Constituição Federal de 1988, o Código de Defesa Consumidor, o Marco Civil da Internet, e mais especificamente no setor da saúde, disposições acerca do ato médico, do Código de Ético Médico e Resoluções do Conselho Federal de Medicina auferissem certa proteção no tratamento de dados na saúde, foi somente com a Lei Geral de Proteção de Dados de 2018 com forte inspiração no GDPR europeu (FRAZÃO, 2019, p.10), que a situação jurídica de proteção da privacidade e proteção de dados encontrou um diploma específico e atualizado (SAAVEDRA; GARCIA, 2020, p.181).

A LGPD faz uma distinção entre dados pessoais que são tidos como toda informação relacionada a pessoa natural identificada ou identificável daqueles que são considerados dados pessoais sensíveis, que são caracterizados, como aqueles que trazem informações sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes a saúde ou à vida sexual, dados genéticos ou biométricos, todos vinculados a uma pessoa natural (DALLARI; MONACO,2021, p. 6). Assim, informações genéricas não se enquadram na definição trazida pela lei, como também as pessoas jurídicas ou quaisquer outras coletividades de fato estão fora do alcance dela. Ademais, dado pessoal pela lei não se caracteriza como uma simples informação, mas tem de haver um vínculo desta com uma pessoa natural em concreto (COSTA, 2021, p. 90).

É importante ter ciência que quando a LGPD faz alusão a dados relacionados a saúde, não se trata apenas de dados que claramente são de saúde, como um resultado de um exame de sangue ou os dados descritos numa receita ou prontuário médico, mas também qualquer informação que se relacione a pessoa natural, identificada ou identificável, que permita concluir

sobre os aspectos relacionados à sua saúde, a exemplo de uma dieta especial recomendada por conta de uma restrição alimentar (PALHARES, 2021, p. 303).

O tratamento de dados é conceituado na Lei Geral de Proteção de Dados no seu artigo.5º, X como:

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

A caracterização em tratamento de dados não depende de qualquer alteração da informação, podendo somente ser qualquer ação, digital ou analógica que tenha por objeto quaisquer dados (COSTA, 2021, p. 90).

Para a proteção do dados pessoais a LGPD determina que quando houver tratamento, todo o processo deve se pautar na boa-fé, e também, se ater a finalidade, adequação, necessidade, transparência, segurança e prevenção, no intuito de assegurar que o tratamento seja limitado ao mínimo de informações necessárias para se atingir finalidades legítimas, no qual necessita adotar medidas efetivas para prevenir danos e proteger os dados contra acessos indevidos e vazamentos de informações (KUNG; AUN,2021, p. 105).

Não obstante, a LGPD (BRASIL, 2018) estabelece em seu art. 7º as hipóteses que legitimam o tratamento de dados, como mediante o consentimento do titular, para obrigação legal ou regulatória do controlador, para realização de estudos por órgão de pesquisa, quando necessário para a proteção da vida do titular ou da sua incolumidade ou de terceiros, dentre outras hipóteses legitimadoras. Porém, caso os dados sejam considerados sensíveis, como são os dados da saúde, as hipóteses que autorizam o tratamento que se encontram no art. 11 da citada lei são mais restritivas, pois o tratamento irregular desses dados podem ocasionar danos mais graves ao titular.

Na saúde, dentre as bases legais que são usadas com mais frequência para justificar o tratamento de dados pessoais e dados sensíveis são os que envolvem consentimento, cumprimento de obrigação legal e regulatória, exercício de direitos, realização de estudos por órgãos de pesquisa e tutela da saúde (KUNG; AUN,2021, p. 106).

4. Lei geral de proteção de dados na saúde e possíveis meios para estar em conformidade

A LGPD possui uma aplicabilidade extensa, pois ela se refere às operações de tratamento de dados pessoais realizadas no Brasil, ou em relação a dados coletados no Brasil ou, ainda,

que sejam de titularidade de indivíduos localizados no País, é o que dispõe o artigo 3º da citada lei (DONDA, 2020, p. 17).

Assim, soma-se ao desafio de as organizações de saúde estarem em conformidade com a lei pela própria extensão da aplicabilidade dela, bem como pela dificuldade no tratamento dos dados pessoais e dados sensíveis, que devem se situar dentre as bases legais trazidas pelos art. 7º e 11 da LGPD. Obstáculos que podem ser minorados pela aplicação de um programa de *compliance* na saúde bem executado, que possam moldar como os dados possam ser tratados na conformidade com a lei e evitando possíveis riscos, como acessos não autorizados e vazamentos de informações.

A própria LGPD dita sobre a criação de um programa de *compliance* em seu art. 50, §2º ao dispor sobre a elaboração de um programa de governança em privacidade, que necessita ser executado de acordo com a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados (SANTORO, 2021, p. 252).

Essa política de privacidade deverá dispor de todos os aspectos essenciais de sua aplicação, sendo claramente formulados, desde a identificação e classificação de seu objeto de proteção, na qual necessita explicitar quais são os dados passíveis de proteção, estipulação de regras e enquadramentos legais para seu tratamento, bem como dispor sobre seu acesso, proteção, compartilhamento, políticas de segurança e, também a previsão de consequências para o descumprimento das referidas regras (SANTORO, 2021, p. 253). Ainda mais, deve incluir como poderão ser feitas as "reclamações e petições dos titulares, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento, ações educativas, mecanismos de supervisão internos e mitigação de riscos" (DALLARI; MARTINS, 2021, p. 128).

Ademais, será necessário para a feitura da política de privacidade o mapeamento de toda a cadeia de dados pessoais e sensíveis que circulam na organização, identificando todas as formas de coleta, etapas de tratamento, agentes envolvidos em cada uma delas e, em especial, identificar possíveis falhas de segurança. (DALLARI; MARTINS, 2021, p. 129). Em seguida, deverá ser elaborado um relatório inicial, que conterá uma avaliação dos potenciais riscos identificados, que serão considerados para a correta determinação de quais os instrumentos necessários a garantir a segurança informacional (DALLARI; MARTINS, 2021, p. 134). Posteriormente, deverá ser executada a capacitação de todos os profissionais envolvidos no

tratamento de dados. Além disso, a política de privacidade deverá ser revisitada, sendo objeto de monitoramento, reavaliações, atualizações, pois não é algo perfeito e acabado, mas sim que deve evoluir de acordo as constantes demandas empresariais e tecnológicas.

Além de possibilitar o tratamento de dados mais assertivo, evitando perdas de informações, acessos indevidos, e também uma clara visualização da circulação de dados em uma organização, um programa de *compliance* efetivo poderá evitar ou abrandar a aplicação das robustas multas descritas na LGPD pelo tratamento irregular de dados pessoais e dados pessoais sensíveis, pois a "adoção de medidas adequadas, será inclusive, um dos critérios orientadores para a autoridade nacional de proteção de dados na avaliação da gravidade dos incidentes de segurança" (KUNG; AUN, 2021,p.113). As medidas apropriadas segundo a LGPD incluem "medidas que garantam maior segurança nas operações de tratamento de dados, incluindo métodos de anonimização, pseudonimizaçao, técnicas adequadas de eliminação e conservação dos dados em arquivo" (KUNG; AUN, 2021, p.113) e a correta colheita do consentimento do titular de dados.

4.1 Anonimização, pseudonimização e consentimento

A anonimização, segundo o art. 5º, IX da LGPD (BRASIL, 2018) consiste na "utilização de meios técnicos razoáveis e indispensáveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação direta ou indireta, a um indivíduo", quando esse processo não pode ser revertido com a utilização de esforços razoáveis, o dado anonimizado não é considerado mais um dado pessoal, saindo da esfera de proteção da LGPD (KUNG; AUN, 2021, p.107).

Ainda, a pseudonimização diz respeito "a um processo que também protege e oculta dados pessoais, mas pode ser reversível por meio de informações detidas pelo controlador, por vezes chamada de chave de acesso" (KUNG; AUN, 2021, p. 107). Por ser um processo reversível, dados pseudonimizados ainda são resguardados pela LGPD.

Ademais, como preceitua a LGPD em seu art. 5º, XII "consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018). Ainda, o consentimento do titular autorizando o tratamento de dados não implica a transferência da titularidade dos dados para os agentes de tratamento, que passam a ter restrições para essas operações (GUEDES, 2019, p. 125).

A anonimização e a pseudonimização possibilitam uma maior segurança aos dados pessoais e aos dados pessoais sensíveis ao camuflar uma associação direta do dado com um indivíduo concreto, e o consentimento livre é uma das bases legais autorizadoras do tratamento de dados, no entanto:

> Ele apenas é considerado como efetivamente livre e inequívoco caso o titular, no momento de sua aceitação, esteja concreta e totalmente informado sobre todos os possíveis usos dos seus dados, as suas finalidades, tempo de armazenamento, possibilidade de compartilhamento e demais informações completas e necessárias para que a manifestação do seu consentimento possa de fato ser considerada livre e inequívoca (COSTA, 2021, p. 95).

Esses três pontos: a necessidade da anonimização, da pseudonomização e como será feita a comprovação do consentimento na colheita de dados, são medidas de segurança incidentes sobre os dados pessoais e sensíveis que serão decididas pelo controlador e executadas pelo operador dos dados pessoais e sensíveis. Essas figuras são centrais na proteção de dados pessoais e sensíveis, ditando como serão os processos, o trâmite dos dados na organização, e pontuando quem serão as pessoas dentro dela que terão acesso os dados de saúde, pois somente quem está relacionado ao cuidado do cidadão deverá ter acesso às informações de saúde de seu paciente (PRICOLA; PIZZO, 2021, p. 147).

A necessidade de proteção de dados na LGPD "não se restringe ao meio virtual, mas a todos os meios pelos quais os dados podem ser coletados e utilizados. Entretanto, também não há dúvida de que é no meio virtual que se concentram as maiores preocupações e os maiores desafios da proteção de dados" (FRAZÃO, 2019, p.12). Assim é fundamental que as organizações invistam cada vez em segurança da informação, como a exemplo:

> Detecção de vulnerabilidades de hardware e software e outros controles de rede; efetuar backups periódicos e realizar controles de acesso, tanto físico quanto lógico (controles de acesso com travas especiais, firewall, antimalware e intrusion prevention system atualizados, dupla criptografia de disco aplicada para notebooks, tablets e smartphones. Pode contar ainda com monitoramento externo a partir de centros de segurança (Security Operation Center-SOC) para detecção de vulnerabilidades, e security penetration test, ou pentest, para simular ataques cibernéticos e um adequado plano de recuperação contra desastres (PALHARES, 2021, p. 320).

Mais ainda do que investir em segurança da informação, é imprescindível que a importância do sigilo das informações seja reforçada aos profissionais envolvidos no tratamento da saúde.

Todas essas medidas de segurança ficarão em boa parte à cargo das figuras do controlador, operador e encarregado, que sob a vigilância da ANPD deverão prestar contas e se responsabilizar em caso de incidentes, demonstrando de forma efetiva quais as medidas efetivas foram tomadas no sentido de comprovar a observância das normas de proteção de dados pessoais.

5. A lei geral de proteção de dados e o *compliance* na saúde

Em 2018 um aplicativo E-Health disponibilizado pelo Ministério da Saúde, teria exposto por meses, dados pessoais de milhares de brasileiros usuários do Sistema Único de Saúde, que tiveram informações como Cartão Nacional do SUS, dados do titular como informações médicas, histórico de medicamentos e agendamentos acessados indevidamente (ROSA; SILVA; BÔAS; AVOGLIA, 2021, p.281). Esse exemplo de incidente de segurança, como é denominado pela LGPD em seu art. 46, pode ser definido como a violação das medidas de segurança adotadas pelos agentes de tratamento, que resultam em acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado (SOUZA, 2019, p. 251).

Assim, além do evidente dano verificado no exemplo anterior, se verifica que o custo envolvido em um vazamento de dados de saúde são maciços, uma vez que se acumulam por conta do pagamento de atividades voltadas ao gerenciamento da crise, contratação de pessoal especializado, interrupção de negócios, perdas de clientes, pagamento de indenizações, multas regulatórias, perdas na imagem da entidade, entre outros. Ainda, inequívoco os danos aos titulares dos dados vazados, pois:

> No que concerne à falta de segurança no tratamento de dados, a máxima adotada é aquela de acordo com a qual é 'melhor prevenir do que remediar', pois não há como recuperar informações acessadas por terceiros não autorizados. Tal questão explica-se pelo fato de que dados, entre os quais dados pessoais, sejam estes sensíveis ou não, são bens intangíveis e, portanto, inapropriáveis e inapreensíveis de reprodução com facilidade *ad infinitum*, sendo inúteis, portanto, as ações de busca e apreensão para fins de reparação dos dados in natura (TOMASEVICIUS FILHO, 2021, p. 212)

Esses incidentes muitas vezes ocorrem, porque as medidas de segurança adotadas pelas organizações não acompanham a velocidade em que novas fraudes e brechas nos sistemas são descobertos, e também, pela própria falha nas entidades de aplicar medidas eficazes de proteção e acompanhá-las devidamente.

Em pesquisa realizada no ano de 2019 pelo Serasa Experian, revelou que apenas 8,7% das organizações ligadas à saúde estão em conformidade com a LGPD (PECK, 2019). Se soma, pesquisa realizada pelo Centro de Estudos para o Desenvolvimento da Sociedade da Informação, com dados históricos colhidos entre 2014 a 2019, que demonstram ser de somente 27% as instituições ligadas à saúde que detém uma política de segurança da informação (TIC SAÚDE, 2017). Esses dados revelam o tamanho do desafio de se proteger dados pessoais e dados pessoais sensíveis com foco em dados da saúde no cenário brasileiro.

Apesar do grande obstáculo envolvido em estar as organizações ligadas à saúde em conformidade com a LGPD, é inegável a sua imprescindibilidade. Pois de um lado, se encontra os "inúmeros benefícios do fácil acesso a dados médicos de pacientes por meio de prontuários eletrônicos e bases de dados estruturadas e, de outro, os riscos inerentes ao tratamento de dados sensíveis" (COSTA, 2021, p. 89). Além disso, com a informatização da saúde se busca a otimização de processos, recursos e a redução de prejuízos, bem como o aumento da qualidade do serviço prestado e da experiência do paciente com determinado produto ou serviço (ROTHBARTH, 2021, p. 295).

Cabe lembrar que:

> As raízes da proteção de dados estão ligadas aos direitos da personalidade contidos na Constituição Federal, no Código Civil e perpassam pela Lei do Habeas Data, pelo Código de Defesa do Consumidor, pela Lei de Acesso à Informação, pela Lei do Cadastro Positivo e pelo Marco Civil da Internet. Com efeito, o Brasil foi desenvolvendo um sistema de proteção de dados, que também se refletiu na atuação dos tribunais superiores e órgãos da Administração Pública (OLIVEIRA; LOPES, 2019, p. 29).

Porém, a LGPD teve a importante missão de ser o instrumento normativo que compilou importantes obrigações de privacidade e sigilo, previstas nessas legislações e também em resoluções do CFM que disciplinam sobre o Prontuário Médico e Sigilo Médico.

Todavia, a LGPD inovou trazendo novas responsabilidades, direitos e deveres, que devem ser cumpridos quando da implementação de um programa de *compliance* que tenha por escopo a proteção de dados (DALLARI; MARTINS, 2021, p.137), o que resta claro é que o objetivo da LGPD "é o de conferir uma ampla proteção ao cidadão e às situações existenciais mais importantes que são afetadas pelo tratamento de dados" (FRAZÃO, 2019, p. 48). Ainda, impôs novas e gravosas sanções advindas do irregular tratamento de dados pessoais e sensíveis, bem como novas hipóteses autorizadoras de seu tratamento.

Ainda, a LGPD possibilitou que:

> O mercado tratava os dados coletados como ativo próprio, que poderia ser livremente utilizado e comercializado por quem dele se apropriasse. Agora a perspectiva é inversa: os dados coletados continuam a pertencer às pessoas que se referem, de modo que o coletor dos dados deve prestar contas do uso que deles é feito. As prerrogativas, os direitos e princípios contidos na LGPD se reconduzem a essa ideia básica: dever de prestar contas, já que o agente de tratamento de dados lida com bens alheios e de extrema relevância. Esse dever fundamentalmente é gratuito e envolve também a obrigação de retificar informações para que os dados reflitam a realidade e não obstem o exercício de direitos fundamentais da pessoa natural (FRAZÃO; OLIVA; ABILIO, 2019, p. 374).

Além do mais FRAZÃO recorda que:

> É possível apontar três fatores para robustecer o papel dos mecanismos de compliance no âmbito da proteção de dados pessoais. Em primeiro lugar, o amplo escopo de incidência da LGPD (decorrência, como visto, do conceito de dado pessoal, de tratamento e de banco de dados) torna necessária a adaptação não apenas de atividades centralizadas de coleta de dados, mas também de

> qualquer operação que perpasse, ainda que indiretamente, a utilização de informações relacionadas a pessoas naturais. À luz do conceito de dado pessoal, até mesmo as mais simples atividades terão que se adequar à lei, vez que demandam, em alguma medida, o armazenamento de informações tuteladas pela lei – basta cogitar das informações atinentes aos empregados ou, ainda, das listas de clientes. Mesmo operações laterais- como a que ocorre nos condomínios edilícios ao coletarem e armazenarem dados de condôminos, visitantes, funcionários-também se sujeitam à LGPD (2019, p. 374).

Isto posto, a LGPD pode ser utilizada como novo instrumento a ser aplicado nos programas de *compliance* no setor de saúde, pois através do cuidado em se proteger os dados pessoais e dados pessoais sensíveis, toda uma cadeia de mapeamento de dados, de processos, de ferramentas de segurança, de interações entre os diversos atores presentes no setor de saúde é discutido e revisitado, no intuito de se preservar a integridade do paciente que se encontra sob seus cuidados e que é o verdadeiro detentor da titularidade de suas informações. É um grande desafio que a LGPD impôs as organizações ligadas à saúde estar em *compliance* com suas normas, mas um obstáculo que se vencido colocará a entidade em um lugar muito confortável em relação às suas obrigações e certeza da qualidade do serviço de saúde prestado à comunidade brasileira.

6. Conclusão

Em um mundo cada vez mais conectado, ter informação rapidamente e com facilidade é imperioso para uma prestação de serviço mais assertiva, e no contexto da saúde, essa presteza ganha ainda mais importância, ao dispor o profissional de saúde de dados completos sobre o paciente aos seus cuidados, para garantir um atendimento adequado e contínuo. Porém, mesmo com esses benefícios, o tratamento dos dados pessoais trazem também ônus para as organizações de saúde, o qual podem se destacar o acesso de indevido dos dados pessoais e sensíveis, perda ou adulteração dos mesmos e ainda, o vazamento de milhões de dados em ataques de hackers.

Nesse contexto, surgiu a necessidade de se ter uma legislação mais efetiva que possibilitasse de fato uma proteção maior aos dados pessoais e sensíveis, emergindo a Lei Geral de Proteção de Dados de 2018 dessa demanda. No qual dispôs sobre o tratamento devido que deve ser destinado aos dados pessoais e sensíveis, regulamentando bases legais, atribuindo responsabilidades e sanções. Porém, para que a norma seja dotada de efetividade, imprescindível se faz com que as organizações de saúde, que tem responsabilidade elevada por tratar de dados sensíveis em larga escala, terem em sua estrutura um programa de *compliance* que dê concretude as disposições da lei.

No entanto, se indaga se a Lei Geral de Proteção de Dados atuaria como um novo instrumento de *compliance* nas organizações? A resposta após ampla análise desenvolvida no presente trabalho é positiva, pois que apesar de muitas organizações já terem um programa de *compliance*, a LGPD fez com que houvesse a necessidade de uma nova sistemática nesses programas já em execução, e para as que ainda não o tinham, a inevitabilidade de criá-los. Pois apesar de a legislação brasileira já dispor na Carta Magna, no Código Civil sobre privacidade, intimidade e as próprias resoluções do Conselho Federal de Medicina regrarem sobre o segredo médico, fato é que a LGDP possibilitou uma estruturação de todas essas disposições. Além de inovar, atribuindo novas responsabilidades, novas bases legais de tratamento de dados e colocando o titular dos dados pessoais como verdadeiro titular de seus dados, no intuito de proteger direitos fundamentais tão valiosos. Conclui-se, também, que a LGPD pela sua alta aplicabilidade dada pelo conceito de dado pessoal tornou necessária a adaptação as suas normas não apenas de atividades centralizadas de coleta de dados, mas também a toda operação que transite em algum tempo sobre dados pessoais.

7. Referências

_____. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros-TIC SAÚDE**. Disponível em: https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comum cacao-nos-estabelecimentos-de-saude-brasileiros-tic-saude-2017/. Acesso em: 06 out. 2021.

BRASIL, 2018. Lei nº 13.709, de 14 de agosto de 2018. **Diário Oficial**,2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 out. 2021.

BRASIL. Controladoria Geral da União. **Programa de Integridade: diretrizes para empresas privadas.** Brasília, 2015. Disponível em: https://www.gov.br/cgu/pt-br/centrais-deconteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf. Acesso em: 06 out. 2021.

CARLINI, Angélica. A saúde suplementar no Brasil-Importância do *compliance* em todos os seguimentos do setor. *In*: CARLINI, Angélica; SAAVEDRA, Giovani Agostini (org). ***Compliance* na área da saúde**. São Paulo: Editora Foco, 2020, p.33.

CONSELHO FEDERAL DE MEDICINA. **Resolução nº 1.638, de 10 de julho de 2002.** Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Disponível em: http://www.rio.rj.gov.br/dlstatic/10112/5125 745/4209117/RESOLUCAO CFMN1.638DE10DEJULHODE2002.pdf. Acesso em: 06 out. 2021.

COSTA, José Augusto Fontoura. Tratamento e transferência de dados de saúde: limites ao compartilhamento de dados sensíveis. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.93.

CREDIDIO, Simões Guilherme. O *compliance* como ferramenta de redução da corrupção. **Revista CEJ.** Brasília, v. 22, n.74, p. 85-90. jan/abr.2018. Disponível em: https://revista cej.cjf.jus.br/cej/index.php/revcej/article/view/2289/2240. Acesso em: 06 out. 2021.

DALLARI, Analluza Bolivar; MARTINS, Amanda Cunha e Mello Smith. Proteção e compartilhamento de dados entre profissionais e estabelecimentos de saúde. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.126.

DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos. Apresentação. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.7.

DONDA, Daniel. **Guia prática de implementação da LGPD**. São Paulo: Labrador, 2020, p. 17.

DUARTE, Clarice Seixas. O *compliance* como instrumento de garantia da efetividade de políticas públicas de saúde no Brasil. *In*: CARLINI, Angélica; SAAVEDRA, Giovani Agostini (org). ***Compliance* na área da saúde**. São Paulo: Editora Foco, 2020, p.147.

FAVERO, Walquiria Nakano Eloy. Proteção e compartilhamento de dados na saúde complementar. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.172.

FRAZÃO, Ana. Fundamentos da proteção de dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de proteção de dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p.10.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p.48.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p.374.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Venceslau. Término do tratamento de dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p.125.

KNOEPKE, Luciano. O sistema de *compliance*: notas introdutórias. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR.** Curitiba, v. 4, n. 2, p. 16. out.2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/10/revista-esa-10-cap-05.pdf. Acesso em: 06 out. 2021.

KONIG, Evelin. Programa de compliance. *In*: _____. **Cartilha de *compliance***. São Paulo: Editora IASP, 2018, p. 21. Disponível em: https://www.iasp.org.br/produto/cartilha-de-compliance/. Acesso em: 06 out. 2021.

KUNG, Angela Fan Chi; AUN, Nicole Recchi. Conservação, anonimização e eliminação de dados na área da saúde: obrigação legal e regulatória, viabilidade técnica e observância da LGPD. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.103.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e a sua otimização pela lei nº 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p.29.

PALHARES, Felipe. Vantagem econômica no compartilhamento de dados da saúde: interpretação do artigo 11, §4º, da LGPD. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.303.

PECK, Patricia. **LGPD e saúde: os fins justificam os meios?** Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude. Acesso em: 06 out. 2021.

PRICOLA, Lilian Cristina; PIZZO, Vladimir Ribeiro Pinto. Segurança da informação na saúde: requisitos para coleta e tratamento de dados na área da saúde. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.147.

RIBEIRO, Marcia Carla Pereira; DINIZ, Patrícia Dittrich Ferreira. *Compliance* e lei anticorrupção nas empresas. **Revista de Informação Legislativa**. Brasília, v. 52, n.205, p. 87-105. jan/mar. 2015.

ROSA, Helena Rinaldi; SILVA, Marlene Alves da; BÔAS, Eliéte Ferreira Villas; AVOGLIA, Hilda Rosa Capelão. Bancos de dados de saúde e pesquisa: prós e contras da LGPD. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.281.

ROTHBARTH, Renata. Monetização de dados de saúde à luz da LGPD: interpretação do artigo 11, §3º. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.295.

SAAVEDRA, Giovani Agostini. Governança corporativa e fundamentos do *compliance* na área da saúde. *In*: CARLINI, Angélica; SAAVEDRA, Giovani Agostini (org). ***Compliance* na área da saúde**. São Paulo: Editora Foco, 2020, p.52.

SAAVEDRA, Giovani Agostini; GARCIA, Lara Rocha. Privacidade e proteção de dados na área da saúde. *In*: CARLINI, Angélica; SAAVEDRA, Giovani Agostini (org). ***Compliance* na área da saúde**. São Paulo: Editora Foco, 2020, p.181.

SANTORO, Raquel Botelho. A LGPD como ferramenta de *compliance* na área da saúde: política de privacidade e relatório de impacto à proteção de dados pessoais. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.252.

TOMASEVICIUS FILHO, Eduardo. Responsabilidade civil na LGPD na área da saúde. *In*: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (org). **LGPD na saúde**. São Paulo: Thomson Reuters Brasil, 2021, p.212.