

**O COMPLIANCE COMO INSTRUMENTO PARA EFETIVAÇÃO DA LEI GERAL DE
PROTEÇÃO DE DADOS EM SAÚDE***Melissa Daandels¹***RESUMO**

O direito à privacidade dos dados pessoais tem se revelado como constante preocupação, especialmente em assuntos associados à saúde. A Lei Geral de Proteção de Dados, ao passo que estabelece direitos e deveres relacionados ao tratamento e compartilhamento de dados pessoais em geral, estipula ainda maior proteção àqueles considerados como sensíveis, que são os dados que versam sobre saúde, em razão do elevado risco que a sua coleta, transferência ou divulgação indevidos podem causar aos indivíduos. Nesse contexto, a implementação de proteção de dados nas políticas de conformidade, mediante a análise rigorosa de riscos, a criação de políticas de privacidade específicas e o monitoramento constante, invade os caminhos de modo a inovar e alinhar a imagem da instituição da saúde aos direitos fundamentais do paciente, objetivando a excelência na prestação de serviços e gerando benefícios às instituições de saúde que as implementam.

Palavras-chave: Lei Geral de Proteção de Dados. Saúde. Dados Sensíveis. Tratamento. Políticas de conformidade.

ABSTRACT

The right to privacy of personal data has been shown to be a constant concern especially in matter associated with health. The General Data Protection Law, while establishing rights and duties related to the treatment and sharing of personal data in general, provides even greater protection those data considered to be sensitive which deal with health, due to the high risk that its undue collection, transfer or improper disclosure can cause to persons. In this context, the implementation of data protection in compliance policies through risk analysis, the creation of specific privacy policies and constant monitoring, innovate and align the image of the health institution to fundamental rights of the patient, aiming for excellence in the provision of services and providing benefits to the health institutions that implement them.

Keywords: General Data Protection Law. Health. Sensitive data. Data processing. Compliance policies.

¹ Currículo resumido: Graduada em direito; Pós Graduada em Direito Processual Civil; Pós Graduada em Direito Médico; MBA em gestão jurídica na área da saúde e hospitalar. Cursanda em Compliance em proteção de dados

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

1 INTRODUÇÃO

O setor da saúde vivencia constantes e efetivas transformações na atualidade, notadamente em virtude da velocidade em que o conhecimento e as práticas médicas e assistenciais avançam e tecnologias e novas soluções para o tratamento e o cuidado dos pacientes se incorporam em ambientes organizacionais neste setor.

Considerando-se que a figura do paciente é o foco central em meio aos diversos stakeholders² do setor da saúde, bem como a proteção dos dados pessoais que versam sobre esta área se traduz como um grande desafio, já que se tratam de dados sensíveis, a existência de programas de compliance³ efetivos e que garantam o direito à privacidade mediante o tratamento de dados, em conformidade com a Lei Geral de Proteção de Dados, gera benefícios às instituições de saúde que os implementa, contribuindo para a redução ou até mesmo inibição do tratamento indevido de dados de saúde.

Isso porque, os dados pessoais dos pacientes, que são os titulares de direitos, se não forem tratados e protegidos adequadamente, podem se tornar passivos jurídico, econômico, financeiro e reputacional para a instituição de saúde, especialmente porque se tratam de dados a quem a lei reservou ainda mais proteção, reputando-os como dados sensíveis, de modo semelhante às normativas europeias de proteção de dados.

De fato, em agosto de 2018, o Brasil deu um passo importante ao aprovar a primeira legislação específica à proteção de dados pessoais do país, a Lei 13.709 – Lei Geral de Proteção de Dados (LGPD), embora o tema da privacidade de dados já era anteriormente discutido na Constituição Federal, no Código de Defesa do Consumidor e no Marco Civil da Internet, dentre outros.

A referida Lei, inspirada no General Data Protection Regulation (GDPR) da União Européia, foi promulgada com o objetivo de regulamentar o tratamento de dados pessoais,

² Segundo FREEMAN (1984), “*stakeholders* são indivíduos ou grupos que podem influenciar ou serem influenciados pelas ações, decisões, políticas, práticas ou objetivos da organização”. De um modo geral, são os atores que fazem parte da cadeia do setor da saúde, sofrendo influência e/ou influenciando as organizações, com diferentes interesses e objetivos, como, por exemplo, pacientes, profissionais da saúde, operadoras de planos de saúde, entre outros inseridos nesta cadeia.

³ Segundo Sarlet IW, Saavedra GA (2020, p. 32) “compliance consiste em um estado dinâmico de conformidade a uma orientação normativa de comportamento com relevância jurídica por força de contrato ou lei, que é caracterizado pelo compromisso com a criação de um sistema complexo de políticas, de controles internos e de procedimentos que demonstrem que a empresa está buscando ‘garantir’, se mantenha em um estado de compliance”.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

visando à proteção dos direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. Da própria definição legal do Art. 5º, inciso II da LGPD é possível verificar que os dados relativos às informações de saúde, genéticos ou biométricos, dentre outros, devem ser considerados como sensíveis e, portanto, ser alvos de proteção específica, notadamente revelada na regra geral de que seu uso só possa ser permitido quando haja livre consentimento informado por parte do seu titular, a não ser em hipóteses excepcionais taxativamente descritas pela lei.

De fato, a adequação das instituições de saúde à Lei Geral de Proteção de Dados é obrigatória para todas as empresas em saúde e o tratamento dos dados dos pacientes deve ser realizado em conformidade com as bases legais previstas na própria LGPD, e mediante padrões adequados de proteção e segurança de dados, durante todo o ciclo de vida e circulação de dados pessoais: desde a coleta, conservação, armazenamento, processos de anonimização, até a eliminação, quando aplicável, já que tanto o armazenamento como o manuseio e a transmissão de dados tem acentuado a necessidade desta proteção.

Nesse cenário, compatibilizar as operações de tratamento de dados no setor da saúde em conformidade com as normas previstas na LGPD tem se mostrado uma tarefa desafiadora e a implementação de políticas de compliance em proteção de dados fundamental, não somente para minimizar e evitar situações de violação de dados pessoais, mas, também, para servir como atenuantes em possíveis atribuições de responsabilidade e aplicação de sanções, e potencialmente, garantir valor à imagem da instituição de saúde perante a sociedade como um todo.

1.1 A LGPD E O TRATAMENTO DE DADOS SENSÍVEIS EM INSTITUIÇÕES DE SAÚDE

As instituições de saúde, onde se estabelecem as mais complexas relações entre os profissionais e com os mais diversos atores neste setor, por sua própria natureza, tratam dados pessoais sensíveis, que demandam maior atenção pela Lei Geral de Proteção de Dados Pessoais, assim como acontece com legislações internacionais sobre o tema, em razão do elevado risco que a sua coleta, compartilhamento ou divulgação indevidos podem causar aos indivíduos.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

Com efeito, a preocupação dos mais diversos estabelecimentos de saúde com este compartilhamento de dados sensíveis do paciente, que são coletados pelo controlador e disponibilizados para o tratamento pelo operador, se potencializam neste setor, mormente porque se tratam de “dados pessoais que, por sua natureza, são mais propícios a serem utilizados de forma discriminatória e lesiva ao seu titular”, conforme ensina Guanaes (2018, p.6), a teor do indicado no Art. 5º, inciso II da Lei Geral de Proteção de Dados Pessoais.

Nas palavras de Dallari (2021, p.118), os dados em saúde “representam a extensão da personalidade do indivíduo, extremamente importantes na privacidade, na construção da identidade e fundamentais para a fruição de direitos de cidadania”, cujo tratamento irregular pode acarretar danos incalculáveis para o paciente titular de dados, patrimoniais ou morais, por conta do conteúdo altamente discriminatório e preconceituoso.

Isso porque, em um ambiente hospitalar, os dados pessoais dos pacientes registrados, por exemplo, em exames laboratoriais e de imagem, cuja realização tenha sido feita dentro da própria instituição hospitalar ou em determinada clínica médica diagnóstica e em um determinado laboratório, são acessados pelo médico assistente e por toda a equipe assistencial do hospital, inclusive pelos próprios planos de saúde, o que não é incomum.

Para além disso, algumas instituições hospitalares comportam o setor de pesquisa clínica com seres humanos ou mantem relações diretas com clínicas especializadas nesta área, cuja essência demanda “a coleta e o processamento de dados pessoais sensíveis de saúde e seu compartilhamento para a comprovação científica da segurança, eficácia e qualidade de um produto médico, para que este possa ser comercializado”, leciona DALLARI (2019, p. 188).

Nesse cenário, qualquer inobservância quanto à coleta e o tratamento de dados pessoais e de dados pessoais sensíveis nessas instituições de saúde e/ou a não conformidade com uma política de proteção de dados em saúde, pode impactar diretamente não somente na sua situação financeira, mas também, na sua própria reputação perante os órgãos fiscalizadores, demais instituições e profissionais da área de saúde e, especialmente, perante os próprios pacientes.

Para Dallari (2021, p. 127), “o acesso ilimitado a dados clínicos dispostos em prontuário, por médicos e por outros profissionais da área da saúde, sem envolvimento direto com a assistência do paciente e titular de dados, seja armazenado de forma física, seja em sistema informatizado para a sua guarda, representa tratamento irregular sob os preceitos da LGPD,

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

bem como um potencial incidente de segurança, além de representar violação ao Código de Ética Médica”.

No entanto, é preciso pontuar que as informações pessoais dos titulares dos dados, ao passo que são recebidas por diversas fontes da complexa cadeia de saúde, necessitam e devem trafegar dentro dela, com o escopo de garantir a melhor assistência aos seus titulares, que são os pacientes. Nesse sentido, todas as operações de dados pessoais dos pacientes, definidos no Art.5º, inciso I da Lei 13.709/2018 como informações relacionadas a pessoas naturais identificadas ou identificáveis, precisam e devem ser efetivamente realizadas.

Para tanto, o tratamento dessas informações deve ser operacionalizado de forma segura e sigilosa, porquanto incluem etapas desde a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, até a difusão ou extração, a teor do disposto no Art. 5º, inciso X do referido normativo legal.

A Lei Geral de Proteção de Dados Pessoais, visando ao tratamento dos dados sensíveis dos paciente, estabeleceu autorizações legais, dentre as quais se destacam a tutela da saúde em procedimentos realizados por profissionais da saúde e o consentimento do titular, nos termos do disposto no Artigo 7º, inciso VII e Art.11º, inciso I da referida Lei, respectivamente.

No que se refere ao consentimento do titular para o tratamento de dados pessoais sensíveis, o art. 11 da LGPD estabelece que este somente poderá ocorrer nas seguintes hipóteses: quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas (inciso I, c.c. art. 7º, I), ou sem fornecimento de consentimento do titular, nas hipóteses especificadas no artigo 11, (inciso II).

Nesse sentido, a exceção à coleta do consentimento inequívoco do titular dos dados somente se justifica para a tutela da saúde e para a proteção da vida ou da incolumidade física do mesmo ou de terceiros, nos casos de tratamento da saúde ou continuidade de sua assistência, e desde que em benefício dos pacientes e titulares dos dados, conforme evidencia o artigo 11 da LGPD.

A privacidade, a confidencialidade e a integridade, uma vez centrais e inerentes à saúde, salientam Garcia, Saavedra (2020, p. 184), foram beneficiadas e protegidas pela LGPD em

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

graus de proteção ainda maiores. Primeiramente, “porque a tutela da saúde se configura como uma das bases legais, sem prescindir dos direitos dos titulares, que se fundamentam na autodeterminação informativa”, que prevê que o titular, a qualquer tempo, solicite um relatório de impacto sobre o acesso da empresa aos dados, quando e com quem compartilhou e quais os tratamentos foram realizados.

Para além disso, todas as informações pessoais dos pacientes estão protegidas pela LGPD, ainda que se tratem de documentos físicos, podendo os pacientes, inclusive, na condição de sujeito e objeto de seus dados, exigirem que os seus dados sejam alterados, corrigidos, apagados ou bloqueados, total ou parcialmente. “Entender o caminho percorrido pelo dado que está sendo utilizado em qualquer tratamento foi permitido somente pela LGPD, como inovação legislativa”, continuam os autores.

A toda evidência, existem exceções legais para o tratamento destes dados sem o consentimento do paciente, mas estas, segundo Schafer (2020, p. 196) “devem ser interpretadas restritivamente, também em respeito aos demais princípios da legislação, especialmente”.

Afinal, sustenta Aragão (2020, p. 698), “se o mote geral do discurso relacionado à proteção de dados reserva atenção especial à privacidade e à intimidade do indivíduo, quando a discussão volta-se ao universo dos dados em saúde, a análise extrapola, em muito, a mera tutela individual de direitos”.

No mesmo sentido, Doneda (2019, p. 29) destaca que o paciente, na condição de titular de seus dados, mesmo que ocorra a revelação dos dados para a finalidade de seu tratamento, não deixa de se conectar a eles, exatamente porque “os dados pessoais integram a privacidade que, por sua vez, está vinculada à personalidade do indivíduo e ao seu desenvolvimento”.

Por essas razões, esclarece Dallari (2021, p. 122), que “o tráfego de dados de saúde com a dispensa do consentimento é a exceção, e não a regra. É autorizado quando se tratar de profissionais da saúde, serviços de saúde ou autoridade sanitária, ou quando se tratar de uso econômico, nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, e para permitir transações financeiras e administrativas resultantes do uso e da prestação desses serviços”.

No entanto, independentemente do consentimento do titular dos dados pessoais, deve-se ter cuidado para que esses dados sejam tratados exclusivamente para fins terapêuticos, de diagnóstico e para a garantia do atendimento e da assistência à saúde, não se permitindo afastar

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

o consentimento do paciente sempre que possível, tampouco o dever de transparência nas informações sobre o tratamento de dados pessoais, inclusive quando forem transmitidos sem seu consentimento, como nos casos de urgência ou emergência médica.

A aplicação da LGPD no ambiente hospitalar deve, pois, caminhar a par e passo com as ferramentas de segurança da informação, tornando-se imprescindível esclarecer e mapear, cuidadosamente, o fluxo de informações entre o titular de dados, o seu médico assistente, sua operadora de planos de saúde e a instituição hospitalar, uma vez que deverá sempre ocorrer de forma ágil e com a finalidade específica de assegurar a não interrupção do tratamento assistencial sem um ônus financeiro adicional ao paciente.

1.2 A IMPORTÂNCIA DA CONSTRUÇÃO DE UMA CULTURA DE PROTEÇÃO DE DADOS SENSÍVEIS NAS INSTITUIÇÕES DE SAÚDE

Com a entrada em vigor da LGPD e os impactos da pandemia pelo novo coronavírus em nosso país, as instituições de saúde vem enfrentando grandes desafios de adequação às regras da nova legislação protetiva dos dados pessoais, notadamente pelo fato de que o tratamento de dados restou por ser inerente às atividades hospitalares, clínicas e consultórios médicos.

Uma vez que, atualmente, o encontro entre o paciente e o profissional médico ocorre nesses ambientes de saúde cada vez mais complexos, onde estão presentes todos os stakeholders do sistema de saúde, é neste ambiente que se faz necessária a definição e disseminação das regras e limites exigidos e definidos pela Lei Geral de Proteção de Dados Pessoais.

Afinal, os relacionamentos entre todos esses atores na área da saúde são extremamente importantes e necessários, não somente para a promoção da saúde, mas para que efetivamente aconteçam em prol dos pacientes, bem como para que mecanismos de controle e tratamento de dados para o monitoramento e detecção de eventuais desvios de privacidade de seus titulares sejam criados.

Com efeito, pondera Johnsen (2012) que, em virtude da sujeição de todos os profissionais da área da saúde e os próprios pacientes a diferentes influências de padrões da comunidade e demais profissionais, das normas legais, das políticas governamentais e institucionais, dos métodos computadorizados de armazenamento e recuperação de

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

informações médicas, da relação entre pesquisa e prática, bem como de outros fatores, a implementação de políticas de privacidade de dados em um ambiente hospitalar se revela fundamental.

Com o advento da lei e, por meio de uma implementação de política de privacidade de dados efetiva em uma instituição de saúde, pautada em regras claras e exemplificativas referentes ao objeto de proteção e a forma como esta deve ser implementada, facilita-se a criação internamente, no meio empresarial, desta cultura que até então não é natural e que, portanto, precisa ser inculcada em cada um dos indivíduos responsáveis pelo tratamento de dados.

Efetivamente, as políticas de privacidade em uma instituição hospitalar com princípios e valores estabelecidos, revela-se fundamental para a construção de uma cultura ética e de proteção de dados neste setor da saúde, na medida em que influenciam o comportamento e a tomada de decisão de todos os seus colaboradores, definindo os comportamentos esperados destes e defendidos pela organização hospitalar, especialmente pautando a forma como a maioria deles irá se posicionar frente ao tratamento dos dados de seus titulares: os pacientes.

Para uma efetiva gestão dos conflitos no processo decisório, salientam Johnsen(2012), devem ser considerados fatores relacionados à estrutura da organização, ao contexto social no qual a decisão se insere e à qualidade dos relacionamentos interpessoais na equipe. Para além disso, pontuam os autores que as instituições devem ter uma política e um programa claros em relação a sua missão, à diversidade de serviços, à melhoria continuada de qualidade na atenção aos pacientes, à orientação em problemas clínicos difíceis e processos para a resolução de litígios.

Para tanto, a Lei Geral de Proteção de Dados, em seu artigo 50, §2º, inciso I, alínea “c”, dispõe que o controlador poderá implementar um programa de governança em privacidade de dados, o que deve ser feito em conformidade com estrutura, escala e volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade de gravidade de danos para o titular de dados.

A referida legislação também assevera que esta política de privacidade, uma vez implementada pela instituição de saúde, deve atender a requisitos específicos que demonstrem não somente o comprometimento do controlador em adotar políticas internas que garantam o cumprimento de normas e boas práticas, a teor da alínea “a” do referido artigo, mas, também,

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

estabeleça relação de confiança com o titular dos dados, por meio de uma atuação transparente e que assegure mecanismos de participação do titular, conforme disposto na alínea “e” do referido artigo legal.

De fato, com a importância cada vez maior conferida à proteção dos dados, as instituições de saúde tiveram que se adaptar a esta nova realidade de proteção a dados sensíveis, mediante a implementação da Lei Geral de Proteção de Dados em suas políticas de compliance em segurança de dados pessoais, as quais devem se dar de forma ampla e abrangente de todos os setores que ofereçam possibilidades de risco.

Afinal, uma instituição que possui um programa de compliance em proteção de dados implementado de forma eficaz promove uma gestão em que os seus riscos são conhecidos, controlados e mitigados, contribuindo para o desenvolvimento sustentável da sociedade e para a melhoria da saúde e da população. “Transformar a mentalidade para que os dados sejam protegidos de forma contínua, durante o ciclo de vida das empresas e impedir novas ações pode fazer com que a empresa atinja novo patamar de maturidade em ética, transparência e cuidado com o paciente”, pontuam GARCIA, SAAVEDRA (2020, p. 186).

Na esteira do reconhecimento da importância em se criar uma cultura de compliance voltada à proteção de dados, Ustaran (2014) pontua que, por meio da implementação destas políticas de privacidade de dados pessoais à luz da LGPD, a instituição encara os custos envolvidos pela ótica dos benefícios que obterá, seja porque protege os direitos fundamentais envolvidos, seja porque pode também tirar vantagens econômicas deste tratamento de dados ético e legalmente adequado.

Por essas razões, a implementação de um programa de *compliance* em proteção de dados deve não somente considerar o cenário em que uma instituição de saúde está inserida e seus riscos, mas também contemplar a realidade de cada ambiente deste setor, seja ele um hospital, uma clínica médica, um setor de pesquisa clínica ou um consultório médico, bem como a sua capacidade de aplicação de recursos ao programa para implantação de controles e ações educativas, ponderando-se a prioridade dos riscos a serem tratados, de modo a observar-se o seu potencial de impacto e vulnerabilidade no caso concreto.

Observam Saavedra, Garcia (2020, p. 186) que, “assimilar a soberania do titular, garantir que todos os seus direitos sejam possíveis de serem executados, fundamentar todos os tratamentos de dados existentes em bases legais de forma sólida e estruturada são ações

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

complexas que não poderiam ser apenas parte de uma política ou discurso de liderança”, devendo permear todos os stakeholders da cadeia de saúde.

Os programas de compliance em proteção de dados tem como foco a promoção de espaços de reflexão entre os profissionais da saúde, a fim de proporcionar padrões que normatizem as condutas éticas nas instituições que os implementam. Por isso, salienta Frago (2017), investir em práticas de *compliance* tem se mostrado um caminho sem volta para a longevidade dos negócios.

Nesse cenário, implementar políticas de privacidade é fundamental não apenas para demonstrar à Autoridade Nacional de Proteção de Dados o comprometimento da instituição hospitalar com a legislação protetiva de dados e com os direitos dos titulares dos dados sensíveis, mas especialmente para criar uma cultura efetiva em proteção de dados que, no âmbito hospitalar, conscientize todos os atores em saúde.

Dessa forma, o *compliance* ajuda a gerar valor para a organização de saúde e para a sociedade, na medida em que, tendo processos bem controlados, ela se torna uma instituição mais confiável e atraente quanto à credibilidade e investimentos, além de se posicionar de forma mais atrativa para os próprios pacientes e terceiros, uma vez que tende a prestar uma assistência mais segura e ter um relacionamento mais transparente com eles.

A adoção de programas de compliance robustos, pontua Frazão (2019, p. 711), “além de garantir o cumprimento das normas de proteção dos dados, contribui para a construção de ambiente de confiança entre os titulares - essencial em um mundo em que o disseminado uso de dados pessoais aparenta ser processo irreversível – e representa diferencial competitivo”.

A conformidade das empresas com a legislação brasileira não é um empecilho aos negócios, mas uma chance de mostrar destaque e confiança ao seu público-alvo e ao mercado, deixando evidente que a empresa está de acordo com as melhores práticas, participando da construção de uma sociedade digital equilibrada, saudável e pautada pela ética.

Portanto, a implementação de uma cultura de proteção de dados pela própria instituição de saúde, a toda a cadeia deste setor, inclusive terceiros, é fundamental para que todos os atores na área de saúde, possam identificar as situações que envolvem dados pessoais do paciente e serem capazes de refletir novas situações que venham a lidar com o tratamento de dados, prevendo riscos e possibilidades de enfrentá-los adequadamente, o que se mostra ainda mais

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

necessário em um mundo de inovações tecnológicas constantes e potencialmente entrelaçadas com o tratamento de dados.

2 CONSIDERAÇÕES FINAIS

Com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), o Brasil passou a contar com uma legislação específica sobre o tratamento de dados pessoais, tanto em meios físicos quanto em meios digitais. Para a referida Lei, os dados de saúde são caracterizados como sensíveis, categoria esta que exige mais segurança e privacidade em estabelecimentos de saúde devido à potencialidade de riscos associados ao trânsito dos dados sensíveis, quando do compartilhamento e tratamento de dados.

Em que pese todas as regras quanto ao tratamento de dados pessoais sensíveis do paciente na LGPD, não há uma transparência total quanto aos limites para tanto, especialmente porque a informação ao paciente e o consentimento estão diretamente interligados, haja vista que não há consentimento sem a adequada informação.

De acordo com o regramento legal, prioriza-se, então, a exigência do consentimento informado e esclarecido do titular dos dados do paciente para fins de tratamento pelos agentes em finalidades específicas, porquanto essas operações tem como um de seus objetivos principais assegurar direitos inerentes à personalidade dos titulares e direitos fundamentais constitucionalmente previstos, incluindo privacidade, intimidade, honra, imagem, liberdade, autodeterminação e não discriminação.

No entanto, o fluxo de dados em saúde nem sempre terá por prioridade o consentimento informado e especificado do paciente, titular dos dados pessoais, a teor do disposto no artigo 11 da LGPD, hipóteses legais em que os dados sensíveis podem ser tratados ainda que não haja o prévio e específico consentimento, porquanto a LGPD também estabeleceu como base legal o tratamento de dados pessoais para a tutela da saúde, devendo os profissionais de saúde, hospitais, clínicas, centros de diagnóstico, prestar assistência à saúde e, por questões éticas, zelar pela privacidade e intimidade dos pacientes.

Nesse cenário, o novo texto dado à LGPD pontua que a exceção para se tratar dados de saúde sem o consentimento do titular e viabilizar o cruzamento de informações proporcionadas

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

pelo tratamento desses dados poderá ser aplicada por toda a cadeia do setor da saúde, valendo-se para isso da definição “serviços de saúde” constante na lei 8.080/90 (Lei do SUS).

A análise contextual é de extrema relevância para a verificação acerca de determinado dado pessoal ser considerado também um dado relacionado à saúde do titular e, portanto, um dado de categoria sensível. O tratamento de dados pessoais sensíveis requer a identificação de uma base legal específica para tanto, dentro de possibilidades mais restritas do que aquelas previstas para o tratamento de dados comuns e que estão dispostas no artigo 11 da LGPD.

Fato é que o compartilhamento e o tratamento de dados em estabelecimentos de saúde é extremamente necessário, desde a realização das atividades que hoje já constituem uma rotina no atendimento médico e da assistência à saúde, até as novas demandas em saúde. Para que haja continuidade, segurança e legitimidade do tratamento de dados, em busca de excelência no cuidado da saúde do paciente, que é o titular dos dados pessoais e dos dados pessoais sensíveis, as informações deverão trafegar o seu caminho dentro das instituições de saúde, desde que de forma sigilosa e objetiva.

De fato, programas de *compliance*, se bem estruturados e geridos por meio de seus pilares estabelecidos, são uma ferramenta de monitoramento e controle para garantir um ambiente mais seguro e justo para a assistência ao paciente, evitando perdas e danos e contribuindo para o aumento da confiabilidade e a valorização das organizações prestadoras de serviços de saúde.

Deveras, a implementação destas políticas de privacidade devem atender a requisitos específicos que demonstrem o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas (artigo 50, §2º, inciso I, alínea a) e que objetive o estabelecimento de uma relação de confiança com o titular, por meio de uma atuação transparente e que assegure mecanismos de participação do titular (artigo 50, §2º, inciso I, alínea e).

Muito embora o sigilo e a privacidade de dados pessoais não sejam novidade na área da saúde, a LGPD trouxe novas responsabilidades, direitos e deveres, cuja observação faz parte quando da implementação de um programa de *compliance* em matéria de proteção de dados. Para além da mudança das práticas, o que é fundamental, é preciso alterar a cultura e a forma de pensar, mediante um processo contínuo e adaptações diárias.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

E, para que essa imagem possa ser sólida, deve haver um alinhamento com a alta diretoria que, por sua vez, deve ser observado pelos diversos setores da empresa. Se não houver o comprometimento de toda a instituição, o compliance se torna inviável, mormente porque o mesmo é uma ferramenta indispensável para garantir e evidenciar a adoção de melhores práticas para o tratamento de dados de maneira compatível com a finalidade informada ao titular dos dados.

De fato, a implementação de políticas de privacidade como um instrumento de compliance em proteção de dados mostra-se relevante ao demonstrar uma preocupação efetiva da instituição de saúde em estar em conformidade com as normas que determinam as políticas de proteção de dados que devem ser implementados, ao passo que contribui, ainda, para a criação de uma cultura empresarial de proteção de dados, permitindo a efetivação de sua execução internamente e contribuindo para a educação dos funcionários, garantindo, dessa forma, maior eficácia da lei.

Para além disso, a adoção de programas de compliance em privacidade de dados efetiva, pelas instituições de saúde, representa uma mitigação de riscos e de potenciais danos, ultrapassando a certeza de que todos os colaboradores tenham conhecimentos dos aspectos formais das políticas ou programas de compliance, mais do que isso, a compreensão da relevância de uma atuação ética e efetiva no tratamento e compartilhamento de dados pessoais do paciente na área da saúde.

A gestão de dados sensíveis é um desafio, uma vez que o relacionamento entre empresas e profissionais da saúde é de extrema importância para esses avanços. Contudo, a solução não é banir ou impedir o relacionamento, mas garantir que sejam pautados por interesses primários para o melhor tratamento e segurança do paciente, com o objetivo de efetivamente promover a saúde e a proteção de dados dos titulares.

Parece, portanto, não haver uma solução única, mas lidar com segurança de informações, a fim de reduzir as chances de falhas de ordem técnica, bem como o fator humano, requer a implementação de programas de *compliance* específicos nas instituições de saúde, de modo criar e potencializar uma efetiva mudança de cultura organizacional do estabelecimento de saúde, mediante a incorporação, por todos os agentes de tratamento, das normas protetivas e políticas de privacidade.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAGÃO, Suéllyn Mattos de. SCHIOCCHET, Taysa. **Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde**. Revista Eletrônica de Comunicação, Informação e Inovação em Saúde, v.14, n.3, 2020, pp.692-708, p. 698.

CRESPO, Marcelo Xavier de F. **Compliance no Direito Digital**. V3. São Paulo: RT, 2021.

DALLARI, Analluza B.; MONACO, Gustavo Ferraz de C. **LGPD na Saúde**. São Paulo: Thomas Reuters Brasil, 2021.

DALLARI, Analluza B. **Contrato de Pesquisa Clínica: aspectos práticos e jurídicos**. São Paulo: Thomas Reuters Brasil, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de dados pessoais**. 2.ed. São Paulo: Thomson Reuters Brasil, 2019.

FRAGOSO, Ronaldo Perez. **O real valor dos investimentos na busca por transparência**. In: Governança corporativa e integridade empresarial: dilemas e desafios. Organização Carlos Eduardo Lessa Brandão, Joaquim Rubens Fontes Filho, Sérgio Nunes Muritiba. 1.ed. São Paulo: Saint Paul Editora, 2017.

FRAZÃO, Ana. **Nova LGPD: O Término do Tratamento de Dados**. Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-termino-do-tratamento-de-dados-10102018>>. Acesso em: 12fev2021.

FREEMAN, Edward R. **Strategic management: a stakeholder approach**. Boston: Pitmann, 1984.

GARCIA, Lara R.; SAAVEDRA, Giovani A. **Privacidade e proteção de dados na área da saúde**. In: Compliance na área da saúde. Coordenadores CARLINI, Angélica; SAAVEDRA, Giovani A. Indaiatuba: Editora Foco, 2020.

GUANAES, Paulo; SUZA, Allan Rocha de; DONEDA, Danilo; NASCIMENTO, Francisco José Tavares do. **Marcos Legais nacionais em face da abertura de dados para pesquisa em saúde: dados pessoais, sensíveis ou sigilosos e propriedade intelectual**. Rio de Janeiro: Fiocruz, 2018.

JONSEN, Albert R.; SIEGLER, Mark; WINSLADE, William J. **Ética Clínica**. Abordagem prática para decisões éticas na medicina clínica. 7.ed. Porto Alegre: AMGH Editora Ltda, 2012.

PORTO, Éderson Garin. **Compliance & Governança Corporativa: uma abordagem prática e objetiva**. Porto Alegre: Laboratory, 2020.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

SARLET, Ingo W.; SAAVEDRA, Giovanni Agostini. **Judicialização, Reserva do Possível e Compliance na Área da Saúde.** R. Dir. Gar. Fund, Vitória, vc.18, n.1, p. 257-282, jan/abr, 2017. Disponível em: <file:///D:/DADOS/Downloads/858-2782-1-PB.pdf>. Acesso em 14.01.2021.

SCHAEFER, Fernanda; GONDIM, Glenda Gonçalves. **Telemedicina e Lei Geral de Proteção de Dados Pessoais.** In: ROSENVALD, Nelson; MENEZES, Joyceane Bezerra de; DADALTO, Luciana. Responsabilidade Civil e Medicina. Indaiatuba: Editora Foco, 2020.

USTARAN, Eduardo. **Howto Encourage Privacy Compliance.** Managing Intellectual Property, vol.244, p. 36-37, 2014.