DOI 10.1344/rbd2021.54.36005

Revista de Bioética y Derecho
Perspectivas Bioéticas
www.bioeticayderecho.ub.edu – ISSN 1886 –5887

ARTÍCULO

La Llei General de Protecció de Dades i les seves implicacions per a la salut: Avaluacions d'Impacte sobre el tractament de dades en el context clínic i hospitalari

A Lei Geral de Proteção de Dados e suas implicações na saúde: as Avaliações de Impacto no tratamento de dados no âmbito clínico-hospitalar

The General Data Protection Law and its implications on Health: Impact Assessments on Data processing in the clinical-hospital scope

La Ley General de Protección de Datos y sus implicaciones para la salud: Evaluaciones de Impacto sobre el tratamiento de datos en el contexto clínico y hospitalario

MARGARETH VETIS ZAGANELLI, DOUGLAS LUIS BINDA FILHO *

* Margareth Vetis Zaganelli. Doutora em Direito pela Universidade Federal de Minas Gerais (UFMG). Professora titular da Universidade Federal do Espírito Santo (UFES). Professora colaboradora do Projeto Jean Monnet Module "Emerging 'moral' technologies and the ethical-legal challenges of new subjectivities" do Erasmus+ European Commission. Professora Visitante Mobilidade Docente Erasmus+ na Università Degli Studi Di Milano-Bicocca - UNIMIB. E-mail: mvetis@terra.com.br.

*Douglas Luis Binda Filho. Graduando em Direito pela Universidade Federal do Espírito Santo (UFES). Membro dos grupos de pesquisa "Grupo de Pesquisas em Bioética" (BIOETHIK) e "Grupo de Estudos e de Pesquisas em Migrações, Fronteiras e Direitos Humanos"(MIGRARE), ambos em parceria com a Università degli Studi di Milano-Bicocca (UNIMIB, Itália). E-mail: bindadouglas@gmail.com.

Resum
La Llei General de Protecció de Dades preveu la protecció de les dades personals i té implicacions significatives en nombrosos àmbits, inclòs el sanitari. En aquest, a causa de la quantitat rellevant de dades sensibles que contenen informació sobre salut, es requereix precaució per part dels agents de tractament, ja que és més probable que el seu processament causi un alt risc per als drets dels titulars. En aquest sentit, l'art. 35 del Reglament General de Protecció de Dades, la legislació europea en matèria de protecció de dades personals, determina que la realització d'Avaluacions d'Impacte és obligatòria, la qual cosa no és evident en la legislació brasilera. A través d'un estudi exploratori, basat en una enquesta bibliogràfica i documental, s'investiga la importància d'aquestes Avaluacions per part de les institucions de salut en el tractament de dades sensibles, a fi de certificar no només el compliment de la legislació, sinó també de les estipulacions presents en els codis deontològics que valoren el secret, la privacitat i la confidencialitat en la relació metge-pacient. Al principi, es discuteixen aspectes generals de la llei brasilera i una perspectiva comparada respecte a l'europea. En segon lloc, exposa l'associació entre el tractament de dades sensibles i la confidencialitat en l'assistència sanitària. Conclou que és important realitzar l'Avaluació d'Impacte sobre dades sensibles, ocasió en la qual es considera l'experiència europea d'una metodologia basada en riscos.
Paraules clau: dades sensibles; governança de dades; Llei General de Protecció de Dades; Reglament General de Protecció de Dades; Avaluació d'Impacte.

Resumo
A Lei Geral de Proteção de Dados dispõe sobre a proteção de dados pessoais e tem implicações significativas em inúmeras áreas, dentre as quais a saúde. Em âmbito sanitário, em virtude da quantidade relevante de dados sensíveis contendo informações sobre saúde, exige-se cautela dos agentes de tratamento, uma vez que seu processamento é mais suscetível de ocasionar alto risco para os direitos dos titulares. Nessa hipótese, o Regulamento Geral sobre a Proteção de Dados, a legislação europeia sobre proteção de dados pessoais, em seu art. 35, determina como obrigatória a realização das Avaliações de Impacto, o que não se demonstra evidente na legislação brasileira. Por meio de pesquisa exploratória, com base em levantamento bibliográfico e documental, investiga-se a importância dessas avaliações pelas instituições de saúde no tratamento de dados sensíveis, a fim de atestar não apenas o cumprimento com a legislação, mas igualmente com as estipulações presentes em códigos deontológicos que valorizam o sigilo, a privacidade e a confidencialidade na relação médico-paciente. Para tanto, são abordados, em um primeiro momento, os aspectos gerais da LGPD e uma perspectiva comparada em relação à GDPR. Em seguida, é exposta a associação entre o tratamento de dados sensíveis e a confidencialidade na assistência em saúde. Por fim, o trabalho conclui acerca da importância da realização da Avaliação de Impacto em dados sensíveis, ocasião em que se considera a experiência europeia de metodologia baseada nos riscos.
Palavras-chave: dados sensíveis; governança de dados; Lei Geral de Proteção de Dados; Regulamento Geral sobre a Proteção de Dados; Relatório de Impacto.

Abstract
The General Data Protection Law provides for the protection of personal data and has significant implications in numerous areas, including in healthcare. In the health field, due to the relevant amount of sensitive data containing information on health, it is required caution from the treatment agents, since its processing is more likely to cause a high risk to the rights of the data subjects. In this regard, the art. 35 of the General Data Protection Regulation, the European legislation on the protection of personal data, determines that the carrying out of Impact Assessments is mandatory, which is not evident in the Brazilian legislation. Through exploratory research, based on a bibliographic and documentary survey, the importance of these assessments by health institutions in the treatment of sensitive data is investigated, so as to attest not only compliance with legislation, but also with stipulations present in deontological codes that value secrecy, privacy and confidentiality in doctor-patient relationship. At first, general aspects of the Brazilian law and a comparative perspective regarding the European one are discussed. Secondly, it exposes the association between treatment of sensitive data and confidentiality in healthcare. It concludes that it is important to carry out the Impact Assessment on sensitive data, an occasion in which the European experience of risk-based methodology is considered.
Keywords: Sensitive data; data governance; General Data Protection Law; General Data Protection Regulation; Impact Assessment.

Resumen
La Ley General de Protección de Datos prevé la protección de los datos personales y tiene implicaciones significativas en numerosos ámbitos, incluido el sanitario. En éste, debido a la cantidad relevante de datos sensibles que contienen información sobre salud, se requiere precaución por parte de los agentes de tratamiento, ya que es más probable que su procesamiento cause un alto riesgo para los derechos de los titulares. En este sentido, el art. 35 del Reglamento General de Protección de Datos, la legislación europea en materia de protección de datos personales, determina que la realización de Evaluaciones de Impacto es obligatoria, lo que no es evidente en la legislación brasileña. A través de un estudio exploratorio, basado en una encuesta bibliográfica y documental, se investiga la importancia de estas Evaluaciones por parte de las instituciones de salud en el tratamiento de datos sensibles, a fin de certificar no sólo el cumplimiento de la legislación, sino también de las estipulaciones presentes en los códigos deontológicos que valoran el secreto, la privacidad y la confidencialidad en la relación médico-paciente. Al principio, se discuten aspectos generales de la ley brasileña y una perspectiva comparada con respecto a la europea. En segundo lugar, expone la asociación entre el tratamiento de datos sensibles y la confidencialidad en la asistencia sanitaria. Concluye que es importante realizar la Evaluación de Impacto sobre datos sensibles, ocasión en la que se considera la experiencia europea de una metodología basada en riesgos.
Palabras clave: datos sensibles; gobernanza de datos; Ley General de Protección de Datos; Reglamento General de Protección de Datos; Evaluación de Impacto.

1. Introdução

O surgimento de regulamentações de proteção de dados pessoais consolidou-se a partir dos anos 1990, com o modelo de negócios da economia digital, dependente dos fluxos internacionais de base de dados. Em 2013, o debate em torno do tema acentuou-se após as revelações de Edward Snowden, ex-contratado da NSA, a respeito do esquema de vigilância instaurado sobre cidadãos norte-americanos e líderes de Estado, fato que mobilizou a cultura europeia de proteção à privacidade. Antes da divulgação de Snowden, as corporações estavam moldando as regras de privacidade da Europa, mas tal situação fez com que os defensores da privacidade incorporassem suas preferências ao texto do Regulamento (UE) 2016/679, também denominado Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation – GDPR*).

O conceito de privacidade no mundo digital e a necessidade de se pensar a proteção de dados pessoais foram igualmente transformados pelo episódio de repercussão midiática ligado ao *Facebook* e à *Cambridge Analytica*, escândalo que envolveu a coleta de dados de aproximadamente 87 milhões de usuários do *Facebook* para fins políticos entre 2014 e 2018. Tal caso ensejou em uma movimentação global que repensou normas éticas em ambientes virtuais. As reações às violações de privacidade pressionaram o *Facebook* a se adequar ao GDPR ainda em 2018 (Ashford, 2018), com a garantia de um ambiente mais seguro para os usuários.

Em suma, a sociedade da informação, conforme assegura Zygmunt Bauman (2013), encontra-se em um momento pós-pan-panóptico, em que a vigilância é constante e cada vez mais expande o seu poder. A internet tornou-se uma tecnologia apta a acumular dados pessoais de indivíduos e a atual conjuntura econômica é fundada no processamento desses dados em larga escala, o que urge novas reflexões a respeito de regulamentações de privacidade.

No âmbito da saúde, as novas tecnologias revolucionaram a forma de organizar e de processar dados de pacientes. A digitalização de dados de saúde tem passado por uma transformação intensa nos modelos clínicos, operacionais e de negócios. Todo esse cenário tem sido estimulado pelo envelhecimento da população, por mudanças no estilo de vida, pela proliferação de aplicativos de *software* e dispositivos móveis, por tratamentos inovadores, pelo maior foco na qualidade e valor do cuidado, e pela medicina baseada em evidências (Abouelmehdi; Beni-Hessane; Khaloufi, 2018). A telemedicina e outras formas de assistência remota igualmente dependem de que os dados sejam protegidos, tendo em vista a importância de se assegurar o sigilo médico-paciente, a privacidade e a confidencialidade, valores expressos no Código de Ética Médica.

As novas tecnologias têm igualmente transformado a forma de se conduzir pesquisas científicas, de exercer vigilância sobre a população, de identificar casos, de rastrear contatos e de avaliar intervenções com base em dados de mobilidade e comunicação. Na saúde, são coletados inúmeros dados para o atendimento de pacientes, dentre os quais encontram-se dados sensíveis, importantes para a sequência do tratamento. No mencionado setor, várias fontes de *big data* incluem registros hospitalares, registros médicos de pacientes, resultados de exames médicos e dispositivos que fazem parte da internet das coisas. Com uma forte integração de dados biomédicos e de saúde, as organizações de saúde modernas podem revolucionar as terapias médicas e a medicina personalizada (Dash et al., 2019), mas tudo isso depende de novos sistemas de informação e de novas abordagens, necessários para evitar violações de informações confidenciais e outros tipos de incidentes de segurança, a fim de fazer uso eficaz dos grandes dados de saúde.

Em âmbito sanitário, existem esforços para que se padronize e se formule normas elucidativas a respeito da proteção de dados em saúde. A Lei nº 12.965, de abril de 2014, também denominada Lei do Marco Civil da Internet, introduziu os princípios básicos de segurança a respeito do tema. Em 2015, a Política Nacional de Informação e Informática em Saúde (PNIIS) foi instituída. A Lei Geral de Proteção de Dados (LGPD) veio sedimentar ainda mais o tema, a fim de complementar, consequentemente, os aspectos relativos à proteção de dados e às informações em saúde. O presente trabalho, por meio de pesquisa exploratória, através de levantamento bibliográfico e documental, tem por escopo a análise das imprecisões trazidas pela LGPD no que diz respeito à realização de Relatórios de Impacto, com recorte relativo ao tratamento de dados em instituições de saúde. Deseja-se responder ao seguinte questionamento: é obrigatória a realização de Relatórios de Impacto quando forem tratados dados sensíveis de saúde? Busca-se, em um primeiro momento, abordar os aspectos gerais da Lei Geral de Proteção de Dados (LGPD), bem como as suas principais diferenças em relação ao Regulamento Geral sobre a Proteção de Dados (GDPR). Em seguida, realiza-se uma consideração a respeito do tratamento dos dados sensíveis na saúde e a inevitável associação entre o tratamento primoroso de tais dados e a confidencialidade na assistência em saúde. Por fim, o trabalho debate acerca da importância da realização da avaliação de impacto em dados sensíveis, ocasião em que se considera a experiência europeia de uma metodologia baseada nos riscos.

2. A Lei Geral de Proteção de Dados: aspectos gerais e principais diferenças em relação ao Regulamento Geral sobre a Proteção de Dados

A privacidade e a segurança de dados tornaram-se pautas recorrentes após inúmeros escândalos relativos ao vazamento de dados em âmbito nacional e internacional. Na maioria dos casos, os ciberataques expõem dados como CPF, nome, sexo, data de nascimento, dentre outros. Ao longo dos últimos anos, o Brasil registrou uma série de ataques cibernéticos que expuseram informações pessoais de milhões de indivíduos. Em um dos escândalos relativos ao vazamento de dados, ocorrido em 2021, cerca de 223,74 milhões de informações foram expostas em um fórum de internet (Ventura, 2021).

A partir dessa cultura de atenção e busca pela privacidade, surgiram legislações em todo o mundo cujas disposições tratam da proteção de dados pessoais. Na União Europeia, o Regulamento Geral sobre a Proteção de Dados (GDPR) 2016/679 revoga a Diretiva de Proteção de Dados Pessoais de 1995 (95/46/CE) e contém artigos relativos à proteção da privacidade no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Trata-se de um regulamento que inspirou inúmeras outras legislações que tratam do mesmo tema, como o *California Consumer Privacy Act of 2018 (CCPA)* nos Estados Unidos da América, a *Ley General de Protección de Datos Personales (LGPDP)* no México e a Lei Geral de Proteção de Dados (LGPD) no Brasil.

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre o:

> *tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).*

É a primeira legislação a reger o tema relativo à regulamentação da coleta, do uso e do tratamento dos dados de pessoas identificáveis no Brasil de maneira mais ampla. A referida lei entrou em vigor em 18 de setembro de 2020, após um período de muitas reformas na *vacatio legis*, o que ocasionou muitas críticas devido à insegurança legislativa causada pela imprevisibilidade e pelas suas postergações. Os arts. 52, 53 e 54, relacionados às sanções administrativas, contudo, apenas entram em vigor em 1º de agosto de 2021, conforme o art 65, incluído pela Lei nº 14.010, de 2020.

A LGPD foi bastante inspirada pela GDPR, mas as duas legislações possuem disparidades. A LGPD determina proteção especial aos dados sensíveis, cujo tratamento apenas poderá ocorrer nas hipóteses previstas em seu art. 11. Na GDPR, contudo, o tratamento de dados sensíveis é proibido pelo art. 9º, 1, e é apenas lícito em algumas situações, presentes em seu art. 9º, 2, dentre as quais duas não foram incluídas pela lei brasileira: "dados tornados públicos pelo titular" e "dados relativos a atuais ou ex-membros de fundações, associações ou organizações sem fins lucrativos, tratados para fins legítimos e com medidas de segurança apropriadas".

Outra diferença está no tratamento de dados de menores. A LGPD revela, em seu art. 14, que "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse", bem como que, segundo o §1º desse mesmo artigo, para o tratamento de dados pessoais de crianças, deve haver o consentimento de ao menos um dos pais ou responsável legal. A GDPR aceita o consentimento dado por menores, desde que eles tenham pelo menos 16 anos (art. 8º), caso contrário o consentimento do responsável legal é necessário.

Há também diferenças na relação entre o controlador e o operador, posto que, apesar de a legislação brasileira estabelecer a necessidade de o operador realizar tratamento segundo as instruções fornecidas pelo controlador (art. 39), não há nenhuma menção à necessidade da formalização desse vínculo, ao passo que a lei europeia a determina no nº 81 do preâmbulo.

A LGPD não explicita os casos em que serão necessários os Relatórios de Impacto, o que na GDPR está presente no art. 35, à medida que revela que tal avaliação será feita quando o tratamento resultar em elevado risco para o direito e para a liberdade das pessoas. Como será ressaltado ao longo do estudo, esse requisito apontado pela GDPR no art. 35 refere-se aos dados sensíveis, que necessitam de uma atenção especial em seu tratamento.

De forma geral, os principais aspectos que diferenciam ambas as legislações podem ser assim elencados:

***Tabela 1** – Principais diferenças entre a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral sobre a Proteção de Dados (GDPR)*

	Lei Geral de Proteção de Dados	**Regulamento Geral sobre a Proteção de Dados**
Escopo territorial	Aplicáveis a todas as empresas que oferecem bens ou serviços no Brasil, independentemente de onde estejam.	Aplicáveis a todas as empresas que oferecem bens ou serviços na União Europeia, independentemente de onde estejam.
Tratamento de dados sensíveis	Apenas pode ocorrer nas hipóteses elencadas no art. 11.	Essa modalidade de tratamento é proibida pelo art. 9º, 1. Apenas lícito nas situações do art. 9º, 2.
Tratamento de dados de menores	Deve ser realizado "em seu melhor interesse" (art. 14). Art 14, § único estabelece ser necessário haver o consentimento de ao menos um dos pais ou pelo responsável legal.	É permitido o consentimento de menores, desde que tenham 16 anos (art. 8º). Caso contrário, o consentimento do responsável legal é necessário.
Formalização do vínculo entre controlador e operador	Não há menção à necessidade de formalização do vínculo.	Formalização entre controlador e operador obtida por meio de um contrato (art. 81).
Relatórios de Impacto	Não explicita os casos em que são necessários.	Art. 35, 3 considera-os como obrigatórios em casos de (a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares; (b) Operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10 ; ou (c) Controle sistemático de zonas acessíveis ao público em grande escala.
Notificações de violação de dados	Não há prazos detalhados para a notificação de vazamento de dados à autoridade. Há apenas menção que a comunicação será feita em "prazo razoável" (art. 48, §1º). Há previsão de que a comunicação a esse respeito deve ser feita à autoridade nacional e ao titular dos dados.	Art. 33, 1 estabelece que os incidentes devem ser notificados à autoridade de controle em até 72 horas. Há apenas menção à necessidade de notificar a autoridade de controle a respeito da violação. No que tange ao titular dos dados, o art. 34 versa que o responsável lhe comunicará a respeito da violação "sem demora injustificada".
Sanções	O art. 52 apresenta as sanções administrativas. Dentre outras sanções como advertência e publicização da infração, o inciso II desse dispositivo estabelece a aplicação de multa simples de até 2%, limitada a R$ 50 milhões de reais por infração.	Em casos de incidentes de violação de dados, o art. 83, 4 estabelece sanções que variam de 10 milhões a 20 milhões de euros ou, no caso de uma empresa, de 2 a 4% do seu faturamento anual total, consoante o montante que for mais elevado.

Fonte: Elaborada pelos autores com base em ambas as legislações.

Não obstante o Regulamento Geral sobre a Proteção de Dados (GDPR) apresentar um texto consideravelmente mais detalhado que a Lei Geral de Proteção de Dados (LGPD), ambas as legislações possuem lacunas, requisitos vagos e conceitos jurídicos indeterminados, os quais necessitarão de tempo para que as práticas de mercado, as autoridades nacionais ou tribunais os esclareçam e desenvolvam. Ademais, em ambas há carências, que ressaltam a necessidade de se repensar aspectos como custo de conformidade e senso de confiança online.

Tabela 2 *– Principais carências presentes na Lei Geral de Proteção de Dados (LGPD) e no Regulamento Geral sobre a Proteção de Dados (GDPR)*

	Lei Geral de Proteção de Dados	**Regulamento Geral sobre a Proteção de Dados**
Principais carências	Desproporcionalidade (Legislação que apresenta alto custo de conformidade, o que beneficia grandes empresas e afasta pequenas e médias empresas); Falta de menção à necessidade de formalização de vínculo entre operador e controlador; Não são explicitados os casos em que relatórios de impacto são necessários; Não há prazos detalhados no que se refere à comunicação em casos de incidente de segurança que possa acarretar risco ou dano aos titulares dos dados; Não há menção expressa a respeito do que seria "melhor interesse" no que se refere ao tratamento dos dados de menores; Não há um prazo definido no que se refere à notificação do risco de vazamento de dados à autoridade. Não há definição do que constitui nível "razoável" de proteção para dados pessoais, o que entrega aos reguladores flexibilidade significativa na avaliação de multas por violações de dados e/ ou não conformidade.	Desproporcionalidade (Legislação que apresenta alto custo de conformidade, o que beneficia grandes empresas e afasta pequenas e médias empresas); Não há definição do que constitui nível "razoável" de proteção para dados pessoais, o que entrega aos reguladores flexibilidade significativa na avaliação de multas por violações de dados e/ ou não conformidade.

Fonte: Elaborada pelos autores com base em ambas as legislações.

Como exemplificado pela tabela acima, há consideravelmente mais deficiências na legislação brasileira, cujas lacunas foram mormente deixadas para serem preenchidas pela Autoridade Nacional de Proteção de Dados. Não obstante, assim como a GDPR tem evoluído, a LGPD deve evoluir com o tempo, a fim de suprir as carências ressaltadas acima.

3. Tratamento de dados sensíveis e confidencialidade na assistência em saúde

Os dados sensíveis são uma espécie de dados pessoais cujo conteúdo possui uma carga maior de intimidade, o que torna o titular dos dados mais vulnerável perante os terceiros que tiverem acesso a esses registros. No art. 5º, II, da LGPD, define-se dado sensível como:

> *Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (Brasil, 2018)*

No GDPR, estabelece-se que os dados pessoais que sejam sensíveis, pela sua natureza, devem ter proteção específica, uma vez que determinado contexto do tratamento de tais dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Dados pessoais sensíveis de um indivíduo relacionam-se com aspectos bastantes íntimos e, ao serem violados, podem ocasionar ofensas à honra, à privacidade e à dignidade de um indivíduo.

A quantidade e o tipo de informações de saúde que são coletadas, dentre os quais uma enorme quantidade de dados sensíveis, têm aumentado drasticamente nos últimos anos. O número crescente de tecnologias disponíveis para diagnóstico e terapia indica que detalhes que um provedor poderia armazenar devem agora ser registrados e, assim, estar disponíveis para inspeção. Informações sobre estilo de vida, histórico familiar e estado de saúde tornaram-se de maior interesse e possuem maior relevância à medida que se tem compreendido mais sobre a relação desses fatores com a saúde e o bem-estar. Ademais, os dados genéticos estão se tornando mais prontamente disponíveis, não apenas para testes pré-natais, mas também para avaliar o grau de risco de um indivíduo para uma condição hereditária (Institute of Medicine, 1994).

As imposições para o tratamento desses dados são mais rigorosas, uma vez que é exigido consentimento expresso, em documento separado e para uma finalidade específica, nos termos do art. 11 da LGPD. Segundo o inciso II do mesmo artigo, somente podem ser tratados os dados sensíveis, sem consentimento do titular, nas hipóteses em que for indispensável para:

(a) cumprimento de obrigação legal ou regulatória pelo controlador;

(b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

(c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

(d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

(e) proteção da vida ou da incolumidade física do titular ou de terceiro;

(f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

(g) 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 art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (Brasil, 2018)

O acesso descontrolado e o uso indevido dos dados de saúde, igualmente denominados dados clínicos ou informações médicas, banalizam o direito à privacidade do indivíduo, que não raramente desconhece o destino de seus registros. A autodeterminação informativa do paciente é fundamento da LGPD, conforme preconiza o art. 2º, II, e inicia-se a partir do preenchimento do termo de consentimento esclarecido e informado, documento exigido para procedimentos ou intervenções cirúrgicas, bem como para a realização de pesquisas. Tais atos necessitam de dados de saúde e os termos de consentimento que eles exigem devem conter avisos relativos ao grau de confiabilidade de exames, alertas de possíveis riscos, consequências fisiológicas e complicações, além do caráter, objetivos e benefícios da intervenção. O termo deve estar escrito em linguagem simples e decodificada do jargão médico ou científico, a fim de que o paciente tenha plena consciência do teor de sua permissão (Siqueira; Hoch, 2019, p. 10).

Segundo Mendelson e Rees (2014, p. 373), no século XXI, os conceitos de confidencialidade e privacidade são frequentemente considerados intercambiáveis. No entanto, a confidencialidade é principalmente um dever ético e profissional (muitas vezes imposto pela legislação), enquanto a privacidade é uma criação da legislação moderna. Em um ambiente médico, a confidencialidade é imposta ao médico em uma relação terapêutica médico-paciente e o dever de confidencialidade antecede em cerca de 2.200 anos a noção de privacidade. Essa engloba direitos para controlar informações sobre si mesmo e o direito de excluir outros de acessá-las.

A confidencialidade é um dever previsto em inúmeros códigos deontológicos e é um pressuposto ético imprescindível à relação médico-paciente. Prevista nos princípios fundamentais (XI e XXV) e nos arts. 54, 73-79 e 110 do Código de Ética Médica, ela se estende a todos os atores envolvidos na assistência em saúde. Quando há violação de registros médicos e ocorrem vazamentos de dados, o dever de confidencialidade é desrespeitado e deve-se haver responsabilização daqueles que deveriam garantir a segurança do armazenamento dos dados,

segundo a LGPD, os agentes de tratamento. O art. 46 da LGPD estabelece que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. Outrossim, devem ser consideradas disposições de outros códigos, como as Resoluções da ANVISA e do Ministério da Saúde, dentre outros.

O setor de saúde é um dos mais suscetíveis a violações de dados divulgados publicamente. Os invasores podem usar métodos de data mining para descobrir dados confidenciais e divulgá-los ao público (Abouelmehdi; Beni-Hessane; Khaloufi, 2018). Em novembro de 2020, uma falha na segurança no sistema do Ministério da Saúde, expôs informações de 16 milhões de pessoas que tiveram diagnóstico suspeito ou confirmado de Covid-19. Um mês depois, outra falha acarretou na exposição de dados pessoais de mais de 200 milhões de brasileiros que fazem uso do Sistema Único de Saúde ou que são clientes de planos de saúde (Bertoni, 2020).

De acordo com dados colhidos no HIPAA Journal, entre 2009 e 2020, 3.705 violações de dados de saúde de 500 ou mais registros foram relatadas ao Gabinete de Direitos Civis de Saúde e Serviços Humanos dos Estados Unidos da América. Essas violações resultaram na perda, roubo, exposição ou divulgação inadmissível de 268.189.693 registros de saúde. Isso equivale a mais de 81,72% da população dos Estados Unidos. Em 2018, violações de dados de saúde de 500 ou mais registros estavam sendo relatadas a uma taxa de cerca de 1 por dia. Em dezembro de 2020, essa taxa dobrou. O número médio de violações por dia em 2020 foi de 1,76 (Hipaa, 2021).

Em virtude do grande volume de dados e informações eletrônicas gerados e utilizados no cotidiano das instituições de saúde, é necessário que se identifiquem as melhores estratégias para a gestão, mantendo critérios de segurança da informação, como confidencialidade, integridade e disponibilidade (Anahp, 2020, p. 33). É fundamental que as organizações implementem soluções de segurança de dados de saúde que protejam ativos importantes e, ao mesmo tempo, que atendam às exigências de conformidade de saúde. Para tanto, recomenda-se que a instituição implemente um Sistema de Gestão de Segurança da Informação (SGSI), sistema organizacional que visa à proteção dos dados dentro dos critérios de confidencialidade, integridade e disponibilidade da organização (Fontes, 2012, pp. 17-22).

4. O gerenciamento de riscos no tratamento de dados nas instituições de saúde

Lourau e Lapassade (1972) preconizam que o conceito de instituição é composto de três momentos dinâmicos, baseados em universalidade, dada pelo instituído; particularidade, dada pelo movimento instituinte; e singularidade, dada pela institucionalização. A instituição de saúde

é um estabelecimento que presta serviços com as técnicas apropriadas para o desenvolvimento de cuidados em saúde relativos às atenções primária, secundária e terciária. Tais cuidados na assistência em saúde envolvem um conjunto diversificado de coleta de dados, incluindo dados sensíveis, conforme evidenciado anteriormente.

Quando as instituições utilizavam documentos físicos, o padrão de segurança era que o local de armazenamento fosse trancado. Os hospitais precisam manter os prontuários físicos por, no mínimo, vinte anos para algumas patologias e, em caso de outras situações, o prazo pode aumentar. A digitalização dos documentos facilita a gestão e o armazenamento, o que torna necessário garantir sua disponibilidade e segurança. As instituições geralmente possuem suas próprias políticas de segurança da informação, bem como processo de detecção e classificação de risco próprio (Anahp, 2019, pp. 49-50).

Há uma enorme importância em garantir que os dados coletados pelas instituições de saúde sejam protegidos contra exposições e outras ações prejudiciais que possam causar danos às liberdades civis, aos direitos fundamentais e aos demais direitos dos titulares, que, dentro de uma relação terapêutica, muitas vezes não imaginam que o destino de seus registros médicos possa ser outro. O controle e a gestão dos dados são imprescindíveis em um contexto digital, em que as informações se dispersam com extrema facilidade. Para o exercício dessa gestão, torna-se necessário a realização dos relatórios de impacto, uma atividade necessária que garante que o controlador não viole os direitos supracitados, garantindo o sigilo médico, a confidencialidade, a privacidade e a segurança do paciente.

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) é um documento fundamental para demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigar os riscos que possam afetar liberdades civis e direitos fundamentais dos titulares.

Trata-se de um documento prioritário na LGPD, o qual é definido pelo art. 5º, XVII como "a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

O RIPD deve ser elaborado antes de a instituição iniciar o tratamento de dados pessoais, de preferência, na fase inicial do programa ou projeto que tem o propósito de usar os dados (Brasil, 2020), mas com visão completa do ciclo de vida dos dados (Vainzof, 2020) apesar de tal consideração não estar explícita na Lei Geral de Proteção de Dados.

O relatório deve conter, no mínimo, de acordo com o parágrafo único art. 38 da LGPD, a descrição dos tipos de dados coletados, a metodologia que foi utilizada na coleta e na garantia da segurança das informações e a análise do controlador em relação a mecanismos de mitigação de risco. Na GDPR, contudo, os elementos mínimos obrigatórios são, de acordo com o art. 35, nº 7:

> *a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;*
>
> *b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;*
>
> *c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o nº 1; e*
>
> *d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa. (União Europeia, 2016)*

De acordo com a norma ABNT NBR ISO 31000, que trata da gestão dos riscos, risco é o "efeito da incerteza nos objetivos" (Brasil, 2009). Nesse mesmo sentido, gestão de riscos seria o "conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos"(Brasil, 2009). É ideal, portanto, antes mesmo de começar o gerenciamento dos riscos, que se tenha um planejamento estratégico atualizado, com os objetivos alinhados à missão da empresa. Há riscos estratégicos e operacionais, mas é recomendado que se comece a gestão de riscos pelos estratégicos, uma vez que são aqueles que podem comprometer a razão da existência da empresa ou instituição (Baracat, 2019). O risco é composto pelo impacto do dano e pela sua chance de ocorrência.

São nove as etapas da elaboração do Relatório, que contempla a identificação dos agentes de tratamento (controlador e operador) e do encarregado; a identificação da necessidade de elaborar o Relatório; a descrição do tratamento; a identificação das partes interessadas consultadas; a descrição da necessidade e proporcionalidade; a identificação e avaliação dos riscos; a identificação das medidas para tratar os riscos; a aprovação do Relatório; e a revisão (Brasil, 2020). A estrutura do RIPD foi resultado de pesquisa nos modelos propostos por autoridades de proteção de dados europeias e consulta na norma ABNT ISO/IEC 29134:2017. Igualmente, teve inspiração no modelo utilizado pela Inglaterra devido à abordagem completa, simples e direta para registro da Avaliação de Impacto (Secretaria De Governo Digital, 2020).

A questão relativa à obrigatoriedade dos Relatórios, contudo, não ficou explícita na LGPD. Na lei, há apenas artigos que definem o que ele é e informam que a ANPD em alguns casos poderá vir a solicitar esses Relatórios aos controladores, mas sem especificar em quais situações. Apesar disso, eles possuem um papel fundamental na transformação de processos de tratamento de dados pessoais, principalmente quando a metodologia utilizada para esses Relatórios contribui para a formação de uma cultura de governança de dados (Gomes, 2019, p. 145-146).

A GDPR trata do tema com maior clareza, principalmente tendo em vista que as primeiras Avaliações de Impacto de privacidade já estavam previstas na Diretiva 95/46/EC e estavam relacionadas à mitigação de riscos envolvendo possíveis violações aos direitos dos titulares (Gomes, 2019, p. 143). De acordo com a GDPR, em seu art. 35, os Relatórios de Impacto são obrigatórios quando o processamento de dados provavelmente resultará em alto risco, ou seja, em caso de:

> *a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;*
>
> *b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, nº 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º; ou*
>
> *c) Controle sistemático de zonas acessíveis ao público em grande escala. (União Europeia, 2016)*

De acordo com as Diretrizes sobre Avaliação de Impacto de Proteção de Dados (DPIA), presentes no WP248, Relatórios de Impacto devem ser requeridos quando, a título de exemplo, um hospital processa os dados genéticos e de saúde de seus pacientes (sistema de informações do hospital), dentre os quais encontram-se dados sensíveis ou dados de natureza altamente pessoal, dados relativos a titulares de dados vulneráveis, bem como dados processados em grande escala (Article 29 Data Protection Working Party, 2017, p. 11).

Desde que a segurança da informação passou a oficialmente ser considerada e valorizada como um investimento, não mais como um custo acessório, a realização de Relatórios de Impacto são essenciais para a gestão de uma instituição ou empresa que vise a uma regulação responsiva. O Relatório de Impacto, muito embora não esteja explícito pela lei brasileira, é necessário quando o tratamento de dados envolve dados sensíveis. No caso das instituições de saúde, tais Relatórios se apresentam como uma ferramenta fundamental para que se alcance uma maior conformidade

com a LGPD. O maior referencial do risco é o titular dos dados e tal Avaliação de Impacto deve ser realizada de forma qualitativa e valorativa, não apenas quantitativa.

De acordo com material desenvolvido pela Associação Nacional de Hospitais Privados, ainda que a LGPD não disponha sobre a obrigatoriedade do controlador possuir um Manual de Boas Práticas e de Governança, recomenda-se que os hospitais implementem tais medidas, uma vez que a Autoridade Nacional de Proteção de Dados (ANPD) poderá solicitar a efetividade de seu programa de governança em privacidade, com o intuito de comprovar o cumprimento da lei (Anahp, 2019, p. 15).

Segundo o art. 55-J, I, II, III, IX e XI da LGPD, a ANPD terá a competência de recomendar determinados padrões e metodologias de Relatórios de Impacto no Brasil. É importante evidenciar que não há apenas a metodologia de Relatório de Impacto baseada em riscos. Existe, por exemplo, a metodologia baseada em riscos e benefícios, no entanto, ao considerar a influência da GDPR na elaboração da LGPD, supõe-se que a ANPD, ao formular as metodologias das Avaliações de Impacto, levará em consideração a experiência europeia das aludidas Avaliações.

A experiência europeia demonstra que, se após a realização da Avaliação da Relação de Impacto de Proteção de Dados verificar-se que haveria elevado risco para um processo de tratamento de dados na ausência das medidas tomadas pela organização para atenuar o risco, a organização deve consultar a Autoridade Supervisora, a entidade reguladora pública, que tem o propósito de ajudar a garantir a conformidade com o regulamento, conforme artigo 36 da GDPR. Tal autoridade deve aconselhar a organização sobre como proceder, quais medidas de mitigação de risco tomar, ou indicar que o processo de tratamento de dados não deve ser realizado, nos termos do art. 58, 2, f da GDPR (Mendes, 2018, p. 3).

De acordo com o art. 42 da LGPD, o controlador ou operador que causar danos patrimoniais, morais, individuais ou coletivos é obrigado a repará-lo. No que se refere a dados pessoais, o controlador é responsável direto e objetivo pelos incidentes. Nos termos do art. 8º, §6º, cabe a ele o ônus da prova de que o consentimento foi obtido conforme a lei. As instituições de saúde, como clínicas e outras organizações possuem um ônus considerável por atuarem como controladores e como operadores dos dados em grande parte dos casos.

Conforme a Associação Nacional de Hospitais Privados, a conformidade com a lei pode ser verificada com um conjunto de formulários, em linguagem clara e objetiva, dentre os quais termos de esclarecimento contendo o consentimento do paciente. Para ser considerado informado, deve o consentimento possuir informações de identificação da empresa responsável pelo tratamento de dados (quando contratada) e as finalidades do tratamento. Ainda, a aceitação não pode ser passiva, uma vez que o silêncio do paciente não significa consentimento (Anahp, 2019, pp. 56-57).

5. Conclusões

Diferentemente da GDPR, que em seu art. 35 determina como mandatória a realização de Relatório de Impacto quando a operação de tratamento de dados for suscetível de ocasionar alto risco aos titulares dos dados – em resumo, ao tratar dados sensíveis – a LGPD não trata como obrigatória a realização de Avaliações de Impacto nem mesmo nessas ocasiões. A lei apenas estabelece que a ANPD pode, em determinados contextos, requerer ao controlador a realização de tais Relatórios. Igualmente, caberá à ANPD desenvolver os padrões e as metodologias das avaliações. No entanto, uma vez que o processamento de dados sensíveis em saúde é suscetível de ocasionar alto risco para os direitos dos titulares, considera-se essencial que sejam realizadas as citadas Avaliações de Impacto dentro dos procedimentos de governança.

Em respeito aos princípios expostos no art. 6º da LGPD, quais sejam, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, conclui-se que a lei exigirá das instituições de saúde uma regulação responsiva dos dados dos pacientes. A realização de Avaliação de Impacto pelas instituições de saúde é uma forma de garantir a adequação da instituição à LGPD e evitar as sanções, cuja entrada em vigor está prevista para agosto de 2021.

Para além de uma adequação à referida legislação, é importante ressaltar que o respeito aos dados de pacientes evoca aspectos relativos ao sigilo, à privacidade e à confidencialidade na assistência em saúde, imprescindíveis valores deontológicos que não podem ser olvidados. Afora uma conformação que vise ao compliance, as instituições de saúde têm a responsabilidade de promover segurança para os titulares de dados, que muitas vezes sequer imaginam que suas informações sensíveis possam ter um destino não cogitado.

Referências

- Abouelmehdi, K., Beni-Hessane, A.; Khaloufi, H. (2018) "Big healthcare data: preserving security and privacy". *Journal of Big Data,* El Jadida, 5, 1, 1-18. Disponível em: https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-017-0110-7.pdf. Acesso em: 10 fev. 2021.
- Anahp (2019) *Lei Geral de Proteção de Dados: Recomendações Anahp para os hospitais*. Disponível em: https://d335luupugsy2.cloudfront.net/cms/files/62776/1574277107Cartilha_LGPD-Anahp.pdf. Acesso em: 20 fev. 2021.
- _____ (2020) *Manual Melhores Práticas LGPD*. Disponível em: https://www.anahp.com.br/pdf/manual-melhores-praticas-lgpd.pdf. Acesso em: 20 fev. 2021.

- Article 29 Data Protection Working Party (2017) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248*. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Acesso em: 10 fev. 2021.
- Ashford, W. (2018) "Facebook is ready for GDPR, says Zuckerberg". *Computer Weekly*, 23 mai. 2018. Disponível em: https://www.computerweekly.com/news/252441730/Facebook-is-ready-for-GDPR-says-Zuckerberg. Acesso em: 3 fev. 2021.
- Baracat, M. K. (2019) "A gestão de riscos e a LGPD". *Estadão*, 18. nov. 2019. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/a-gestao-de-riscos-e-a-lgpd/. Acesso em: 17 mar. 2021.
- Bauman, Z. (2013) *Vigilância Líquida. Diálogos com David Lyon*. Rio de Janeiro: Zahar.
- Bertoni, E. (2020) "O novo vazamento de dados na Saúde. E suas consequências". *Nexo*, 2 dez. 2020. Disponível em: https://www.nexojornal.com.br/expresso/2020/12/02/O-novo-vazamento-de-dados-na-Saúde.-E-suas-consequências. Acesso em: 22 fev. 2021.
- Brasil (2009) *ABNT NBR ISO 31000. Gestão de riscos – princípios e diretrizes*. Disponível em: https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso em: 20 mar. 2021.
- _____ (2018) Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Poder Executivo, Brasília, DF, 28 jan. 2021. p. 3. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 20 fev. 2021.
- _____ (2020) Lei Geral de Proteção de Dados (LGPD): Guia de Boas Práticas Para Implementação na Administração Pública Federal. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em: 27 mar. 2021.
- Dash, S. et al. (2019) "Big data in healthcare: management, analysis and future prospects". *Journal of Big Data*, Guimarães, 6, 54. Disponível em: https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-019-0217-0.pdf. Acesso em: 22 fev. 2021.
- Fontes, E. (2012) *Políticas e normas para segurança da informação*. Rio de Janeiro: Brasport.
- Gomes, M. C. O. (2019) "Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados". In Lima, A. P.; Hissa, C.; Saldanha, P. M. (org.). *Direito Digital: Debates Contemporâneos*. São Paulo: Revista dos Tribunais, p. 141-153.
- Hipaa (2021) *Healthcare Data Breach Statistics*. Disponível em: https://www.hipaajournal.com/healthcare-data-breach-statistics/. Acesso em: 27 mar. 2021.
- Institute of Medicine (1994) "Confidentiality and Privacy of Personal Data". In Donaldson, M. S.; Lohr, K. N. *Health Data in the Information Age: Use, Disclosure, and Privacy*. Washington, DC: The National Academies Press, p. 136-224.
- Lourau, R.; Lapassade, G. (1972) *Chaves da sociologia*. Rio de Janeiro: Civilização Brasileira.
- Mendelson, D.; Rees, A. (2014) "Medical confidentiality and patient privacy". In White, B.; Mcdonald, F.; Willmott, L. *Health Law in Australia*. Pyrmont:Thomson Reuters, 396-433.
- Mendes, P. A. B. (2018) *Análise de Risco no GDPR*. Tese (Mestrado em Segurança Informática) - Faculdade de Ciências, Universidade de Lisboa. Lisboa, 106 p.

- Secretaria de Governo Digital (2020) *Oficina Dirigida: Relatório de Impacto à Proteção de Dados Pessoais - RIPD*. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/apresentacoes/apresentacao_ripd.pdf. Acesso em: 22 mar. 2021.
- Siqueira, L. S.; Hoch, P. A. (2019) "Os dados pessoais e a proteção de dados de saúde: análise a partir das iniciativas de e-Saúde". In *Congresso Internacional de Direito e Contemporaneidade*, 5º, 2 e 3 set. 2019, Santa Maria. Anais [...]. Santa Maria: UFSM. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.2.pdf. Acesso em: 20 mar. 2021.
- União Europeia (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Disponível em: https://gdpr-info.eu. Acesso em: 20 fev. 2021.
- Vainzof, R. (2020) "O que é o relatório de impacto à proteção de dados pessoais (RIPD)". *Opice Blum Academy*, 17 fev. 2020. Disponível em: https://opiceblumacademy.com.br/2020/02/ripd-relatorio-impacto-protecao-dados-pessoais/. Acesso em: 20 mar. 2021.
- Ventura, F. (2021) "Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensaba". *Tecnoblog*, 22 jan. de 2021. Disponível em: https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/. Acesso em: 20 fev. 2021.

Fecha de recepción: 31 de julio de 2021

Fecha de aceptación: 25 de enero de 2022