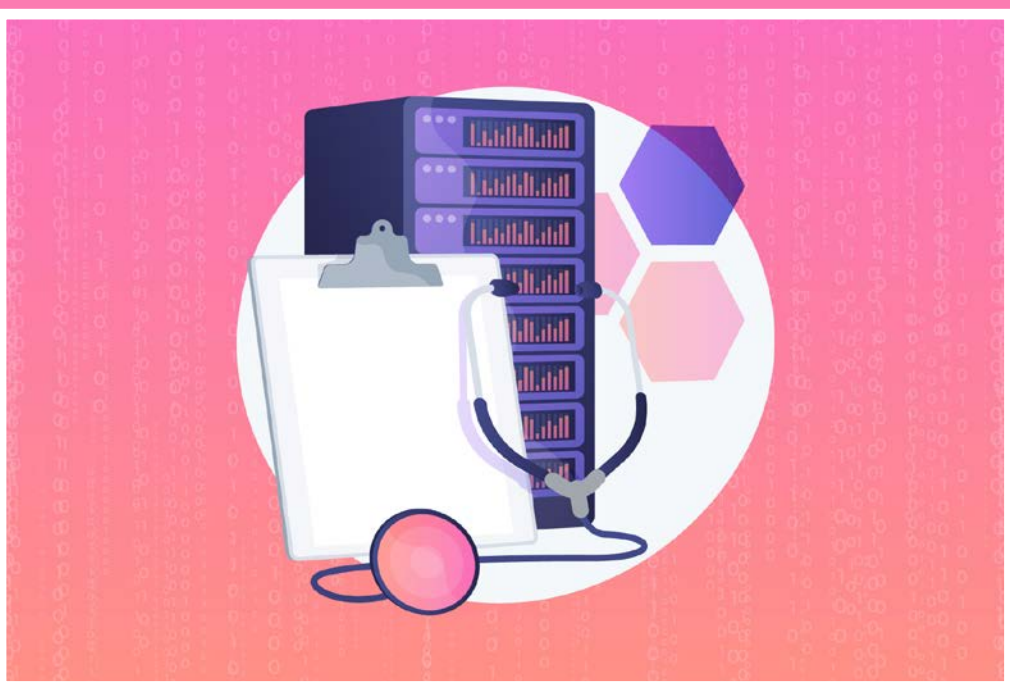
REVISTA CEJ

ISSN 1414-008X
Ano XXVI
n. 83, jan./jun. 2022

Centro de Estudos Judiciários
Conselho da Justiça Federal

83

JUSTIÇA FEDERAL
Conselho da Justiça Federal
Centro de Estudos Judiciários



DESAFIOS À PROTEÇÃO DE DADOS PESSOAIS NO SETOR DA SAÚDE: enfrentando o risco de vazamentos

CHALLENGES TO PROTECT PERSONAL DATA IN THE HEALTH SECTOR: facing the risk of leaks

Camila Rosa da Mata

RESUMO

O estudo examina os limites impostos ao tratamento de dados no setor da saúde, bem como os riscos e implicações do seu vazamento, advertindo, conclusivamente, que o adequado implemento da saúde eletrônica é condição indispensável à realização da eficácia do direito de proteção de dados de saúde.

PALAVRAS-CHAVE

Direito Civil; dados de saúde; dados pessoais sensíveis; vazamento de dados; setor de saúde.

ABSTRACT

The study examines the limits to data processing in the health sector, as well as the risks and implications of its breach, warning, conclusively, that the appropriate implement of e-health, is indispensable condition of the effectiveness of the right to health personal data protection.

KEYWORDS

Civil Law; health data; sensible personal data; data breaches; healthcare sector.

1 INTRODUÇÃO

O uso das tecnologias das grandes redes e dos sistemas de informação, sobretudo o da internet, cresce ininterruptamente, permeando as mais diversas atividades humanas e transformando o modo de sua realização (RODOTÀ, 2008, p. 41). Esse crescimento é resultado direto de uma nova realidade social, que, sob o desígnio de "sociedade de informação" ou "sociedade em rede", é marcada pelo intenso fluxo de informações e pelo constante tratamento e compartilhamento de dados.

Esse intercâmbio agudo de dados também penetrou o setor da saúde, transformando-o drasticamente. Desde contribuições à melhoria da habilidade e experiência de estudantes de Medicina, a partir de treinamentos de realidade virtual, até a prestação de serviços, a inserção da Tecnologia de Informação e de Comunicação (TIC), o e-Saúde (*e-Health*) (ARAGÃO; SCHIOCCHET, 2020, p. 698-699)[1], na relação do paciente com os profissionais de saúde reformulou toda a contextura dos tratamentos, encetando um novo panorama sociocultural, que permite a comunicação ubíqua a partir da interconexão dos bancos de dados e das ferramentas de inteligência artificial (SARLET; FERNANDES; RUARO, 2020), viabilizando a comparação de dados de saúde de indivíduos nas mais diversas localidades e a otimização do processo de revisão do tratamento assistencial proposto, bem como possibilitando a quebra das "piscinas estagnadas" de dados e anos de pesquisa médica em jornais e livros didáticos, remendando inconsistências e melhorando as abordagens de atendimento, produtividade e bem-estar.

O regulamento europeu reconhece as fragilidades associadas aos diversos aspectos relacionados ao uso dos dados de saúde, categorizando este como hipótese de dado sensível e impondo regras que se ocupem em garantir a segurança e a proteção da privacidade [...]

O contemporâneo robustecimento das inovações tecnológicas nos intermeios das atividades humanas, além de sedimentar o perfil dinâmico da tecnologia como medidora do progresso social (DONEDA, 2006, p. 42), detém um significado utilitarista e instrumental (LIMA, 2017, p.4-5) que, no anseio de alcançar determinado fim, opera energicamente para a melhoria dos resultados e eficiência. Paralela a esses contornos funcionais vantajosos, a ascensão da sociedade de informação também intensificou a produção de riscos que acompanha o progresso tecnológico, a qual, em andadura cada vez mais acelerada, ameaça valores e flexibiliza direitos fundamentais (FERRY, 2015, p. 61; RODOTÀ, 2008, p. 41).

Note-se, a despeito dos benefícios trazidos pela inserção das novas tecnologias na prestação dos serviços de saúde, inclusive para a própria promoção do direito à saúde, estas também expuseram fragilidades latentes, que, diante do fluxo massivo e armazenamento de dados pessoais, potencializam a sua utilização abusiva ou indevida (ARAGÃO; SCHIOCCHET, 2020, p. 694-695), aumentando sobremodo o risco de vazamentos e reidentificação, mesmo após a anonimização ou a desidentificação das bases de dados de saúde (ARAGÃO; SCHIOCCHET, 2020, p. 698-699), tornando os direitos à privacidade e à intimidade mais vulneráveis (LIMA, 2017, p. 8).

Em um contexto em que as relações intersubjetivas tornam-se progressivamente mais publicizadas (RUARO; RODRIGUEZ, 2010), *permeado por princípios panópticos a partir de uma discursividade de vigilância* (SARLET; FERNANDES; RUARO, 2020), exsurge uma nova delimitação aos contornos do direito à privacidade (RODOTÀ, 2008, p. 17), o qual abrange não apenas a proteção à vida íntima do indivíduo, mas também a proteção de seus dados pessoais, reconhecendo-se que estes *exprimem uma importante projeção da personalidade humana* (SCHREIBER, 2020), sendo seu resguardo inafastável à concretização dos ideários de liberdade e autonomia (CAPURRO; ELDRED; NAGEL, 2013, p. 65-67).

Transposta a discussão ao universo dos dados em saúde, a carência por tutela é ainda mais ululante. Se, por um lado, a dinâmica de ressignificação do direito à privacidade e à informação na saúde atende ao interesse coletivo, intrínseco à compreensão de bem comum e determinante ao uso e a disponibilização das informações para garantir a satisfação de necessidades grupais, esta também requer uma regulamentação e governança que articule virtuosamente a proteção da privacidade individual (VENTURA; COELI, 2018). Caracterizado, tanto pelo Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679, como pela Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, Lei n. 13.709/2018), como um dado pessoal sensível, o dado de saúde impõe peculiaridades a sua coleta e tratamento, limitando as hipóteses de uso e elevando as exigências de modulações dos riscos de vazamentos. Assim, a fruição das novas vantagens facultadas pela saúde eletrônica (LIMA, 2017, p. 2) deve operar sob a vigilância de estratégias normativas dotadas de uma proteção especial dos direitos fundamentais do titular (DONEDA, 2009, p. 87), com o resguardo da dignidade humana (ARAGÃO; SCHIOCCHET, 2020, p. 695) e a neutralização do potencial discriminatório que possa ser atribuído ao uso dos seus dados (SARLET; KEINERT, 2015, p.113-145).

A despeito dos instrumentos normativos protetivos vigentes, a possibilidade de violação ou vazamentos de dados pessoais é uma mazela irremovível da sociedade de redes, sendo particularmente severo no setor de saúde, que, mais suscetível, se tornou a principal vítima de violações de dados nos últimos anos (SEH, A. H., *et al.*, 2020, p. 4-5).

Atentando-se às premissas expostas, este estudo tem por finalidade examinar os limites impostos ao tratamento de dados no setor da saúde, perpassando pelas peculiaridades da proteção especial dos dados sensíveis, bem como analisar os riscos e implicações do seu vazamento, ponderando acerca dos deveres que nascem da sua ocorrência e refletindo sobre a necessidade de se adotar mecanismos de segurança aptos a garantir a proteção ou, ao menos, reduzir substancialmente os riscos de tais vazamentos.

2 A PROTEÇÃO DE DADOS PESSOAIS NA ÁREA DA SAÚDE

A adoção dos sistemas de e-Saúde a partir da utilização de registros eletrônicos, compartilhamento de dados, *big data* e

uso secundário de dados vem revolucionando a prática médica nas últimas três décadas no setor público e privado (VIEIRA, 2015, p. 33), oferecendo oportunidades de otimização e melhoria na prestação do serviço e no cuidado com a saúde (KAPLAN, 2016, p. 312-313), operando no controle de epidemias, na cura de doenças e na produção de diagnósticos mais eficientes (DONEDA; MONTEIRO, 2015, p. 148).

Se, por um lado, esse entrelaçamento das relações sociais com o ciberespaço (MOLINARO; RUARO, 2013, p. 19) viabilizou maior eficiência na proteção e promoção do direito fundamental à saúde, por outro, também contribuiu para o surgimento de novas preocupações sobre privacidade, confidencialidade e proteção de dados (KAPLAN, 2016, p. 312-313). Esse ambiente de fluidez, incerteza e fugacidade, no qual habitam os sistemas automatizados de informações de saúde, possui um risco em potencial (LIMA, 2017, p.11-12), podendo *fragilizar os controles quanto às garantias à privacidade, à não discriminação, ao controle das informações pessoais, ao respeito, à autodeterminação e, especialmente, ao compartilhamento dos dados pessoais* (SARLET; FERNANDES; RUARO, 2020).

Dessa permanente situação de risco, mister a elaboração de modelos regulatórios aptos a promover a proteção de dados, preservando os direitos fundamentais de indivíduos e de grupo de indivíduos, em particular direitos da personalidade (SARLET; FERNANDES; RUARO, 2020). Essa proteção regulatória traduz-se na elaboração dos arcabouços normativos nacionais e internacionais de proteção de dados, bem como na redefinição de padrões éticos e jurídicos que permeiam e orientam a atividade.

Embora a metodologia seja distinta, há um consenso dos Estados acerca da necessidade de se prestar atenção especial às informações de saúde (KAPLAN, 2016, p. 314) e a sua proteção. Os Estados Unidos abordam a privacidade dos dados de forma setorial. O *Health Insurance Portability and Accountability Act* (HIPAA), de 1996, estabelece regras e diretrizes para modernizar o fluxo de informações na área da saúde, determinando a forma pela qual dados pessoais deveriam ser mantidos pelos serviços de saúde e seguradoras para fiscalizar atos fraudulentos, fixando padrões para o uso, a transmissão e o compartilhamento de dados e informações de assistência à saúde com a finalidade de protegê-las (SARLET; FERNANDES; RUARO, 2020). A União Europeia, por sua vez, uniformizou o regime de tratamento de dados mediante a instituição do Regimento Geral de Proteção de Dados (RGPD) em 2018, instrumento jurídico assentado na ideia de responsabilidade, informação e transparência, posicionando a pessoa e a defesa dos direitos humanos e fundamentais no centro dos regimes de tratamento de dados.

O regulamento europeu reconhece as fragilidades associadas aos diversos aspectos relacionados ao uso dos dados de saúde, categorizando este como hipótese de dado sensível e impondo regras que se ocupem em garantir a segurança e a proteção da privacidade, determinando a adequação ética para sua utilização, gerenciamento, armazenamento e descarte. Essa dinâmica também se verifica no ordenamento jurídico brasileiro, notadamente na Lei Geral de Proteção de Dados (LGPD), que, como se demonstrará neste primeiro segmento do estudo, também posiciona os dados de saúde na categoria específica dos dados sensíveis (SARLET, 2016, p. 446), impondo limites ao seu tratamento e elevando o rigor das exigências de segurança a fim de evitar incidentes.

2.1 A EVOLUÇÃO DA PROTEÇÃO DE DADOS DE SAÚDE

A coleta, documentação e disseminação de informações pessoais de pacientes não são inovações para o setor da saúde. Historicamente, a experiência brasileira no tratamento de dados em saúde constitui-se de sistemas de informação instituídos para fins epidemiológicos, demográficos e de produção de serviços (ARAGÃO; SCHIOCCHET, 2020, p. 698-699). Essa prática, contudo, intensificou-se massivamente após a incorporação das tecnologias de informação e comunicação no setor, especialmente a partir da década de 1970, conduzindo ao desenvolvimento da já mencionada "Saúde Eletrônica", ou e-Saúde (ARAÚJO, 2016, p. 3), assim denominada pela Organização Mundial da Saúde (OMS) (VIEIRA, 2015, p. 34).

Atualmente, no Brasil, os processos de e-Saúde são múltiplos, encontrando-se no Cartão Nacional de Saúde do SUS[2], nas práticas de teleconsultorias, telemonitoramento, prontuário eletrônico, dentre numerosos outros sistemas de produção e gestão da informação em saúde, os quais desafiam cotidianamente as limitações de tempo e espaço, potencializando o volume e a variedade de informações coletadas, processadas e compartilhadas.

Conquanto essa nova configuração preste-se à promoção da disseminação e publicização de dados, auxiliando as atividades dos profissionais e gestores, bem como atendendo às necessidades de controle social e de intercâmbio das instituições, ela não acompanhou as práticas de privacidade que permeia os dados de saúde e que insere, dentre os deveres fiduciários, o dever de confidencialidade (KAPLAN, 2016, p. 313-315). Não se pode olvidar que as informações fornecidas pelos pacientes para seu tratamento dizem respeito a áreas muito pessoais e sensíveis de suas vidas, guardando relação com aspectos de sua existência, tanto física quanto simbolicamente. Descabe, portanto, diante de sua natureza, a presunção de que sejam informações que possam ser divulgadas ou utilizadas livremente (KAPLAN, 2016, p. 316); seu resguardo integra, para além das expectativas sobre privacidade em geral, as normas de prática profissional, privilégio, autonomia e sigilo, estabelecendo requisitos específicos para sua coleta, disseminação e retenção.

Esse dever de resguardo da confidencialidade, memorável desde o Juramento de Hipócrates, reitera-se em todos os instrumentos de deontologia médica, como no Código Internacional de Ética[3] e na Declaração dos Princípios Éticos de Helsinque para Pesquisa Médica Envolvendo Seres Humanos[4] da Associação Médica Mundial (WMA), ou, ainda, na Res. CNS 196/96 (MINISTÉRIO DA SAÚDE, 1996); todos os quais impõem deveres de responsabilidade sobre os dados pessoais coletados e armazenados para fins de clínica ou pesquisa médica (MINISTÉRIO DA SAÚDE, 2002, p. 37), isto é, deveres de proteção ao direito à autodeterminação e privacidade das informações pessoais dos pacientes independentemente do seu consentimento (KAPLAN, 2016, p. 315).

Note-se, mesmo antes da entrada em vigor da LGPD, que sanou a ausência de uma legislação geral sobre proteção de dados, os órgãos já regulavam a matéria de maneira setorizada,

instituindo critérios técnicos para o tratamento e compartilhamento de dados nos sistemas de saúde vigentes no País, quais sejam, o Sistema Único de Saúde (SUS), a Saúde Suplementar e a Saúde Privada.

Não obstante seja a saúde um dever do Estado, realizável pelos órgãos e instituições da Administração Pública, preceitua a Lei n. 8.080/1990 que a assistência à saúde é livre à iniciativa privada, que poderá participar do SUS em caráter complementar, mediante contrato ou convênio, observadas as normas de Direito Público[5]. Para padronizar a troca de informações tanto pela Administração Pública, quanto pelas entidades privadas, o Ministério da Saúde (MS) instituiu regras para os sistemas de Informação. A Portaria de Consolidação n. 1, de 28 de setembro de 2017, dedica um capítulo específico à regulamentação do uso de padrões, informações em saúde e de interoperabilidade entre os sistemas de informação do SUS, nos níveis municipal, distrital, estadual e federal, abarcando também os sistemas privados e de saúde suplementar[6], responsabilizando-os pela guarda, segurança e confidencialidade dos dados gerados e tratados e determinando identificação obrigatória do profissional, trabalhador ou agente que acessa os dados dos usuários a fim de garantir a responsabilização por disponibilização incorreta ou possíveis vazamentos de dados[7]. Essa interoperabilidade entre os sistemas se dá sob vigilância do Departamento de Informática do SUS (DATASUS), mediante um padrão de criptografia e assinatura digital, para garantir a segurança e a integridade no compartilhamento dos dados (Portaria de Consolidação n. 1, de 28 de setembro de 2017).

A Agência Nacional de Saúde Suplementar (ANS), agência reguladora responsável pela regulação da saúde suplementar instituída pela Lei n. 9.961/2000, também estabelece responsabilidades e normas de procedimento para a garantia dos direitos dos beneficiários, inclusive no tocante ao armazenamento de dados e ao compartilhamento de informações[8]. De forma semelhante, o Conselho Federal de Medicina (CFM), a despeito dos limites da sua atuação normativa, editou muitas normas que tratam de questões operacionais, inclusive sobre níveis de segurança que devem ser observados para o armazenamento e a transmissão de informações, em especial dos prontuários médicos, de modo a preservar a privacidade do paciente e o sigilo profissional (Resolução CFM n. 1.821/2007).

Todo esse arcabouço normativo demonstra a evidente preocupação em assegurar a proteção dos dados pessoais no setor saúde, orientando-se pelos princípios constitucionais de privacidade e intimidade e tratando de níveis de segurança da informação e regulamentação de ferramentas de tecnologia da informação mesmo antes da edição da LGPD. Essas normativas subsistem no novo contexto de proteção de dados pessoais instituído no Brasil, ao qual passa a integrar, ao lado da Lei de Acesso à Informação (Lei n. 12.527/2011), do marco civil da internet (Lei n. 12.965/2014) e do Código de Defesa do Consumidor (Lei n. 8.078/1990), a recentemente sancionada Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei n. 13.709/2018) (ARAGÃO; SCHIOCCHET, 2020, p. 695).

Com a entrada em vigor da LGPD, controladores e operadores, que atuam tanto no âmbito interno quanto em nível setorial, precisarão realizar relevantes alterações em suas próprias práticas, elevando a cautela com a segurança das informações, sempre orientando suas práticas com atenção aos princípios da finalidade, adequação, livre acesso, transparência, responsabilização e prestação de contas, sobretudo tratando-se de dado relacionado à saúde do titular, os quais, como se demonstrará no próximo subitem, receberam proteção especial no arcabouço regulatório brasileiro da informação.

2.2 O REGIME ESPECIAL DE TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS DE SAÚDE NA LGPD

A LGPD, assim como o fez o RGPD europeu, inclui, dentro da categoria de dados sensíveis, os dados de saúde[9], os quais se constituem não apenas dados resultantes de diagnóstico médico, mas todos aqueles relacionados ao paciente (LIMA, 2017, p.11), isto é, que revelam informações sobre a saúde física e psíquica, no passado, presente ou futuro do titular (SARLET; FERNANDES; RUARO, 2020) concedendo-lhe uma proteção especial (KAPLAN, 2016, p. 313-314) a partir da imposição de restrições mais rigorosas para o seu tratamento. Essa proteção especial decorre da natureza intrinsecamente personalíssima desses dados que, conforme alerta Doneda, se *conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva* (DONEDA, 2009, p. 160-161), bem como do uso e da finalidade que lhe são outorgados a eles por meio do seu tratamento (LEME; BLANK, 2020, p. 212). Também nesse sentido, descreve Bioni que os dados sensíveis seriam "*uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação*" (BIONI, 2019).

Escolhas de estilo de vida, habilidades reprodutivas e condições estigmatizantes são consideradas altamente sensíveis (KAPLAN, 2016, p. 313-314). A sensibilidade dos dados de saúde é explicada em razão da viabilidade da exposição desses dados gerar uma discriminação do paciente, como, por exemplo, no caso de doenças que ainda são estigmatizadas, como patologias vinculadas à genética humana, doenças mentais, AIDS, entre outros. Note-se, dados sensíveis são nucleares para a composição dos perfis ou das identidades dos seus titulares, possuindo valor político e econômico, podendo servir de instrumentos de controle social, sobretudo no atual contexto digitalizado, marcado pelo uso de algoritmos, de inteligência artificial e de *Big Data* (RUARO; SARLET, 2020) que cada vez mais integra o setor da saúde.

Diante dessa conjuntura, em que o manejo dos dados pode expressar uma afetação direta à pessoa humana, o direito à proteção de dados em matéria de saúde faz-se primordial (SARLET; KEINERT, 2015, p. 127-131). Com fundamento constitucional (art. 5º, inciso XII, CRFB/1988), este deve orientar-se pelo resguardo da dignidade da pessoa humana, da privacidade e da identidade do indivíduo, isto é, do livre desenvolvimento da personalidade, da honra, da reputação, da imagem, entre outras, e da proteção em face das atuais técnicas de delineamento da identidade advindas do tratamento dos dados pessoais (RUARO; SARLET, 2020).

A LGPD, conforme elucidado, reconhece essa proteção. Adotando conceituação ampla de tratamento de dados pessoais[10], a LGPD estabelece princípios (art. 6º, LGPD) e requisitos (art. 7º, LGPD) para sua realização. Referidos limites intensificam-se em se tratando de dados pessoais sensíveis, cujas

hipóteses de tratamento podem se dar: (I) com o consentimento do titular; ou (II) sem o fornecimento do consentimento do titular, nas hipóteses exaustivamente estabelecidas em lei[11].

Veja-se, a estrutura da norma privilegia, em primeiro lugar, a participação ativa do titular do dado sensível por meio do consentimento (ARAGÃO; SCHIOCCHET, 2020, p. 700-701), que deve ser sempre livre, informado e com finalidade determinada (art. 5º, inciso XII) (BRASIL, Lei n. 13.709/2018), isto é, há, necessariamente, a obrigatoriedade de se descrever todas finalidades, de forma específica e destacada (art. 11, inciso I, LGPD) (BRASIL, Lei n. 13.709/2018), que embasarão o uso dos dados, sendo dever do controlador comprovar que o consentimento do titular foi obtido de forma regular, respeitando os preceitos dispostos na referida Lei[12]. Importante observar que havendo alteração de emprego dos dados, seja em virtude da coleta, do tratamento ou da finalidade, exsurge a obrigatoriedade de novo consentimento (art. 9º, § 2º) (BRASIL, Lei n. 13.709/2018), regra esta que se aplica de modo irrefutável ao âmbito da saúde (SARLET; FERNANDES; RUARO, 2020). Também em valorização da autonomia informativa do titular, a Lei reconhece, entre outros, os direitos de acesso, de retificação, de cancelamento, de exclusão, de oposição e de revogação do consentimento a qualquer tempo.

Consoante salientado, a LGPD (art. 11, inciso II) (BRASIL, Lei n. 13.709/2018) também previu hipóteses em que os dados sensíveis poderão ser tratados sem o fornecimento de consentimento do titular, quais sejam a) cumprimento de obrigação legal ou regulatória pelo controlador, b) necessidade para formulação de políticas públicas, c) realização de estudos por órgão de pesquisa, d) exercício regular de direitos em contratos e em processos, e) proteção da vida ou da incolumidade física, f) tutela da saúde por profissionais ou serviços de saúde, g) garantia de prevenção à fraude e à segurança do titular (em processos de identificação e autenticação de cadastro em sistemas eletrônicos).

Conquanto constitua rol taxativo, a experiência demonstra que muitas das hipóteses legais permitem uma atuação ampla, sobretudo tratando-se do setor da saúde. Note-se, como previamente indicado, existem numerosos dispositivos legais que obrigam os atores da cadeia da saúde a coletarem dados e remeterem a terceiros. Exemplo de disponibilização de informações em cumprimento de obrigação legal ou regulatória no setor da saúde, pode-se mencionar o caso das notificações compulsórias. Dependendo do evento de saúde registrado, é dever do serviço de saúde notificar à vigilância sanitária para fins de controle epidemiológico (MINISTÉRIO DA SAÚDE, Portaria de Consolidação n. 4, de 28 de setembro de 2017). Outro exemplo é o do ressarcimento ao SUS, nos casos em que o serviço de saúde, público ou privado, presta atendimento em regime de complementaridade ao SUS e colhe os dados do paciente. O SUS e a ANS compartilham dados, a fim de verificar se, dentre os pacientes, há beneficiários de planos privados de assistência à saúde[13]. Essa troca de informações permite que a operadora tenha acesso ao prontuário do paciente para impugnar tecnicamente o pedido de ressarcimento formulado pela ANS, independentemente de qualquer consentimento.

Outra hipótese que os dados pessoais sensíveis poderão ser tratados sem o consentimento do titular é o de execução de políticas públicas pela Administração Pública. Exemplo prático encontra-se no Conjunto Mínimo de Dados da Atenção à Saúde (Resolução n. 6, de 25 de agosto de 2016), instituído pela Comissão Intergestores Tripartite com o objetivo de subsidiar a formulação, o monitoramento e a avaliação das políticas de saúde, viabilizando as informações do SUS e da Saúde Suplementar à Administração Pública no âmbito da assistência prestada no SUS.

A LGPD também traz exceção ao consentimento do titular dos dados para a realização de estudos por órgãos de pesquisa, garantindo, sempre que possível, a anonimização dos dados pessoais sensíveis. Referida exceção à obtenção do consentimento não deve, contudo, modificar os conceitos preceituados pela Resolução n. 466, de 12 de dezembro de 2012, expedida pelo Conselho Nacional de Saúde, a qual determina, à semelhança do consentimento qualificado dos dados sensíveis estabelecido na LGPD, a obrigatoriedade de as pesquisas envolvendo seres humanos serem precedidas de consentimento livre e esclarecido do participante da pesquisa e/ou representante legal, por meio do detalhamento dos métodos que serão utilizados e os riscos decorrentes da participação na pesquisa. Ademais, vale destacar, a autorização para o tratamento dos dados para estudo em saúde pública observa as restrições do art. 13 (BRASIL, Lei n. 13.709/2018), devendo, portanto, observar o princípio da finalidade, restrito à finalidade do estudo e da segurança dos dados, só podendo ocorrer o tratamento dentro do órgão, sob responsabilidade do órgão de pesquisa, vedando-se a transferência dos dados a terceiro (MARTINS; SOARES, 2020).

Com a entrada em vigor da LGPD, controladores e operadores, que atuam tanto no âmbito interno quanto em nível setorial, precisarão realizar relevantes alterações em suas próprias práticas, elevando a cautela com a segurança das informações [...]

Também não há a necessidade de consentimento do titular dos dados pessoais sensíveis, caso o tratamento de dados se torne indispensável para o exercício regular de direitos em contrato e em processo judicial, administrativo e arbitral. Um exemplo seria a hipótese de um exame em um laboratório de análise clínicas, em que não haveria, necessariamente, a obrigatoriedade de o titular dos dados consentir de forma expressa que seus dados sejam transferidos a uma empresa de transporte terceirizada que realiza o deslocamento do material coletado. Essa abertura, cumpre recordar, não exime quaisquer dos prestadores de serviços envolvidos na cadeia no sentido de respeitar os princípios da LGPD, em especial o princípio da finalidade e da necessidade, devendo sempre agir com boa-fé e adotar medidas para prevenir a ocorrência de danos em virtude do tratamento.

Há, ainda, dispensa do consentimento para a proteção da vida ou da incolumidade física. Tendo em vista a ausência de maiores esclarecimentos conceituais na legislação nacional, oportuno mencionar os conceitos previstos na RGPD, o qual faz remissão à segurança pública. Exemplo encontra-se diante de uma situação que demanda a atuação imediata da Administração Pública para salvar vidas como em catástrofes naturais ou para a preven-

ção, a investigação e a repressão de infrações penais pelos agentes públicos responsáveis. O RGPD também acresce à hipótese as violações da deontologia de profissões regulamentadas, como no caso de médicos que estão submetidos aos preceitos éticos dispostos no Código de Ética Médica.

Por fim, merece menção a hipótese de dispensa para a tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, abarcando desde casos de urgência ou emergência médica, até atividades dos serviços de saúde de modo amplo, contemplando o citado compartilhamento de dados inerente à assistência à saúde pública ou suplementar.

Ainda no tocante ao compartilhamento, o art. 11, § 4º (BRASIL, Lei n. 13.709/2018) da lei veda a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica. Para evitar distorções interpretativas, a Lei n. 13.853/2019 incluiu uma exceção à redação do dispositivo, permitindo o compartilhamento de dados quando houver a necessidade de comunicação para a adequada prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º do referido dispositivo legal, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados (SARLET; FERNANDES; RUARO, 2020).

Todo esse arcabouço normativo integra o regime especial de proteção dos dados sensíveis em saúde. Sua eficácia reafirma a imprescindibilidade do princípio da responsabilidade e prestação de contas, a partir da orientação dos princípios da precaução e da prevenção, pilares de uma constelação jurídica cujo vetor primordial é a proteção da dignidade da pessoa humana, dentro e fora do ambiente digital (RUARO; SARLET, 2020). A LGPD prevê a necessidade de cuidado com os dados sensíveis, mediante o emprego de medidas de segurança necessárias e suficientes à sua proteção, determinando, conforme debruçar-se-á com mais detalhes na segunda parte do estudo, a obrigação imediata de informar na presença de indícios de vazamento ou qualquer dano à estrutura de proteção.

3 ENFRENTANDO O VAZAMENTO DE DADOS PESSOAIS NO SETOR DA SAÚDE: CONFLUÊNCIAS DE DIREITOS E MODULAÇÕES DE RISCOS

A coleta e o processamento de dados pessoais integram, conforme elucidado na primeira parte do estudo, o exercício regular da prática médica na contemporaneidade. Com a fruição das novas tecnologias, essa prática acelerou-se, permitindo, em rapidez sem precedentes, que se efetue a comparação e o compartilhamento desses dados, atribuindo maior precisão à prestação do serviço. Veja-se, após a captura de imagens em um exame de raio-x ou de ressonância magnética, por exemplo, estas são enviadas em segundos para uma central de telerradiologia, permitindo que profissionais habilitados elaborem laudos, os quais são imediatamente disponibilizados para os consultórios, as clínicas e os hospitais (LEME; BLANK, 2020, p. 215-216). Igualmente revolucionários para a prática médica são as coletas massivas na medicina de precisão e o uso de *big data* (CHIAVEGATTO FILHO, 2015), cujo volume e o detalhamento dos dados gerados permitem identificar as causas e as concausas das doenças, auxiliando a ação preventiva, a mitigação de riscos e a precisão das condutas e tratamentos (LEME; BLANK, 2020, p. 215-216).

Apesar dos benefícios advindos dessa ampliação e difusão das bases de dados, ela indubitavelmente põe em risco a manutenção do caráter sigiloso que permeia as informações de saúde, tornando cada vez mais vulnerável o titular. Seja pela negligência na coleta, uso, compartilhamento, armazenamento ou descarte dos dados, seja pela comercialização indevida ou vazamento das informações (LEME; BLANK, 2020, p. 215-216), os dados pessoais correm risco iminente de violação, fragilizando a tutela de direitos fundamentais prioritários.

Em 2017 viu-se exemplo dessa fragilidade ocasionada no episódio de vazamento de dados do Cartão Nacional de Saúde do SUS. Na ocasião, houve a divulgação na rede mundial de computadores de nome, endereço completo, número do Cadastro de Pessoa Física (CPF) e nome dos genitores de milhares de usuários (ARAGÃO; SCHIOCCHET, 2020, p. 699-700). Em 2020, novamente, a *Open Knowledge* Brasil, organização que promove transparência e dados abertos, identificou brecha no sistema e-SUS Notifica do Ministério da Saúde, que teria permitido o acesso às credenciais para acessar base de dados com informações pessoais dos pacientes, dentre as quais, informações confidenciais tais como doenças preexistentes (G1, 2020).

O alto valor dos dados de saúde os transforma em isca para a apropriação indébita e furto de dados de saúde. Conforme se demonstrará no próximo subitem, o setor de saúde tornou-se a principal vítima de ataques externos e internos, sendo o impacto da violação, independentemente da modalidade, sempre alarmante, trazendo consequências não apenas para os pacientes afetados, mas também às próprias instituições (SEH, A. H., *et al*. 2020, p. 1).

Diante dessa nova realidade, marcada pelo desafio de equilibrar a segurança dos dados do paciente e a produtividade, a ordem jurídica impõe uma série de deveres a serem observados pelos agentes de tratamento, a fim de prevenir incidentes ou, ao menos, mitigar os danos no caso de sua ocorrência. Sob essas prerrogativas, debruçar-se-á esta segunda parte do estudo acerca do fenômeno do vazamento de dados no setor da saúde, orientando-se pelo prisma de que o desenvolvimento do planejamento e gerenciamento de riscos é indispensável para salvaguardar a confidencialidade, a integridade e a segurança das informações (LEME; BLANK, 2020, p. 215-216), sobretudo diante deste novo cenário, em que o setor de saúde depende cada vez mais do ambiente digital, não é mais possível assegurar a segurança dos pacientes sem também assegurar a segurança de seus dados sensíveis relacionados à sua saúde.

3.1 O PERIGO DOS VAZAMENTOS DE DADOS PESSOAIS DE SAÚDE

A revolução tecnológica no setor da saúde vem transformando seus dados, tornando-os cada vez mais digitalizados, distribuídos e móveis. Nada obstante essa nova conformação tenha trazido benefícios de operabilidade, ela também gerou uma fonte importante de violações de privacidade. Vulnerabilidades de software, falhas de segurança, erro humano: múltiplas são as variáveis que podem conduzir à exposição ilícita de dados confidenciais, podendo causar danos severos ou até mesmo irrepa-

ráveis (SEH, A. H., *et al*. 2020, p. 1-2).

A violação de dados de saúde representa verdadeiro rompimento dos deveres de segurança e de proteção da privacidade. O Departamento de Saúde e Serviços Humanos dos Estados Unidos (HHS) a define como *o uso ilegal ou divulgação de informações confidenciais de saúde*, produzindo riscos de finanças, reputação ou outro tipo de dano à pessoa afetada (WIKINA, 2014). Semelhantemente, o HIPAA Journal aponta a violação de dados como *a aquisição, acesso, uso ou exposição de informações confidenciais de saúde de forma ilegítima, comprometendo a privacidade ou segurança dessas informações confidenciais de saúde* (tradução livre) (COLLINS, J. D. *et al*., 2011). De forma mais abrangente, o RGPD (art. 4º, 12) define violação de dados pessoais como *uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento*.

Infere-se dessa conjuntura conceitual que as violações de dados podem ser de ordem interna e externa, abrangendo desde vulnerabilidades do sistema e abusos de privilégios, até incidentes de *hacking*/TI por fontes externas (SEH, A. H., *et al*. 2020, p. 3-4). Esta última modalidade tem-se tornado cada vez mais comum no setor da saúde. Apenas em 2018, hackers roubaram 1,5 milhão de dados pessoais, incluindo registros médicos de 160.000 pacientes do sistema de saúde on-line de Singapura, inclusive do primeiro-ministro (BRITISH BROADCASTING CORPORATION, 2018). Nos Estados Unidos, o número de registros de pacientes roubados do provedor de planos de saúde Anthem Blue Cross foi de 78,8 milhões, um dos maiores vazamentos de dados no setor da saúde (POOL; AK; FATEHI, 2018).

Referidos números demonstram uma nova tendência de cibercrimes que têm particularmente ameaçado o setor da saúde, gerando severas consequências aos indivíduos afetados e altos custos financeiros e organizacionais, que variam de penalidades regulatórias a danos à marca, os quais são devastadores para as organizações de saúde (POOL; AK; FATEHI, 2018). Atualmente, o histórico médico de uma pessoa tem muito mais valor para um hacker do que seu cartão de crédito (HUMER; FINKLE, 2014), podendo o preço de um arquivo de registro completo de um único paciente chegar a centenas de dólares na *dark web* (CHERNYSHEV, Maxim *et al*., 2018). De acordo com um relatório *da International Business Machines Corporation* (IBM), o custo médio de uma violação de dados, em 2019, foi de US$ 3,92 milhões, enquanto, no setor de saúde, foi de US$ 6,45 milhões. Nos Estados Unidos, esse valor foi ainda mais alto, chegando a US$ 15 milhões (SEH, A. H., *et al*. 2020, p. 2).

Além da atratividade dos valores, destaca-se que esses registros geralmente contêm grandes quantidades de dados confidenciais, como nome completo, detalhes de contato, detalhes de seguro, diagnósticos, prescrições e tratamentos. Por conta disso, permanecem válidos por muito tempo ou mesmo permanentemente, não podendo ser descartados como os números de cartão de crédito, por exemplo. Assim, se violados, dados de saúde podem ser usados para uma ampla variedade de fins fraudulentos, incluindo roubo de identidade, fraude de seguro e receitas falsas (POOL; AK; FATEHI, 2018); eles também podem influir no próprio tratamento, que, se incorreto, produzirá perdas fatais e irreversíveis para os pacientes (SEH, A. H., *et al*. 2020, p. 2).

Uma análise comparativa dos episódios de violação ocorridos nos últimos anos revela claramente que o setor de saúde é o mais suscetível ao furto de dados (LIU, Vincent *et al*., 2015, p. 1471-1473). Entre 2005 e 2019, foram relatados 6.355 incidentes de violação; destes, 3.912 (61,55%) foram registrados apenas no setor de saúde, sendo que 40,56% dessas violações se deram entre 2015 e 2019, indicando um rápido aumento no número de violações no setor (SEH, A. H., *et al*. 2020, p. 4-5). A situação agravou-se ainda mais no ano de 2020. Conforme a HHS, houve um aumento de 25% nas violações de dados de saúde em 2020, sendo mais de 29 milhões os registros de saúde violados apenas nos Estados Unidos[14]. Em 2021, pelo menos 712 violações de dados de saúde foram relatadas entre 1º de janeiro e 31 de dezembro, estabelecendo um novo recorde para violações de dados de saúde, superando o total do ano anterior, com um aumento de 10,9%. a partir de 2020 (DECEMBER 2021 Healthcare DATA Breach Report).

Outro aspecto a ser observado são os tipos de ameaças que integram as violações de dados. O Departamento de Saúde e Serviços Humanos dos EUA, a partir dos relatórios de violação de dados HIPAA, identifica cinco principais causas de violações, quais sejam, acesso não autorizado, divulgação, hacking, incidente de TI, descarte impróprio e perda ou roubo (POOL; AK; FATEHI, 2018).

Incidentes de hackers (*Hacking/IT Incident*) abrangem todos os ataques cibernéticos usados para obter acesso não autorizado a dados confidenciais. *Ransomware* e *malware* são as principais abordagens usadas para expor informações de saúde protegidas (SEH, A. H., *et al*. 2020, p. 7-8).

O acesso não autorizado (*Unauthorized Access/Disclosure*) inclui situações de exposição de dados confidenciais de saúde com a ajuda de qualquer fonte interna de uma organização, geralmente vinculado a abuso de privilégios, acesso ou divulgação não autenticada etc. (SEH, A. H., *et al*. 2020, p. 7-8). Conforme POOL *et al*. (2020), a maioria dos estudos aponta o acesso ou divulgação não autorizado como o principal motivo de violações de dados. Exemplo dessa categoria encontra-se na violação interna de dados relatada pelo *Memorial Hermann Health System*, sistema de saúde do sudeste do Texas constituído por 17 hospitais, no qual um funcionário obteve acesso não autorizado aos registros médicos eletrônicos de 10.604 pacientes, visualizando seus nomes, endereços, números de prontuários médicos, datas de nascimento, informações de seguro de saúde e, em alguns casos, números do seguro social (OUELLETTE, 2014). Outro exemplo bastante comum de ameaça interna reside no fato de muitos residentes, bolsistas e estudantes usarem seus telefones celulares pessoais para salvar e transferir imagens clínicas, apesar da segurança precária desse modo de comunicação (POOL; AK; FATEHI, 2018).

Também bastante comum é perda de dados (*loss*) armazenados em mídia digital e dispositivos eletrônicos, seja devido ao mau funcionamento da tecnologia da informação em saúde, seja por erros humanos (POOL; AK; FATEHI, 2018). Há, ainda, os incidentes de roubo (*theft*), que se constituem do furto de servidores de rede, discos rígidos, laptops ou qualquer outro

dispositivo portátil que contenha dados de saúde protegidos (SEH, A. H., *et al*., 2020, p. 7-8).

A última causa direta é o descarte impróprio de dados desnecessários (*improper disposal*). Note-se, dados desnecessários, mas sensíveis e confidenciais, devem ser descartados de forma adequada para que não possam ser recuperados posteriormente. O descarte inadequado desses dados pode levar à divulgação de informações protegidas de saúde (Idem, p. 7-8).

Também merecem destaque as causas indiretas desses vazamentos, as quais, embora não resultem prontamente em uma violação de dados, podem facilitar indiretamente um incidente de violação de dados (POOL; AK; FATEHI, 2018). Dentre esses fatores que contribuem para a violação da privacidade e divulgação de dados de saúde estão: a falta de conformidade (*non-compliance*); o uso ineficaz (*ineffective use*) ou inexperiente de sistemas; aplicativos de terceiros (*third-party applications*), tais como Apple iMessage e WhatsApp, os quais são cada vez mais populares nas instituições de saúde, apresentando vulnerabilidades do software que, muitas vezes, arquiva textos automaticamente por cinco anos ou mais (FIRDOUSE, 2018); e características organizacionais (*organizational characteristics*) de tamanho, orçamento e tipo, uma vez que organizações de saúde de maior tamanho, orçamentos inadequados (com limitações na alocação de recursos financeiros para investimentos em segurança de TI) têm risco maior de violação (POOL; AK; FATEHI, 2018) do mesmo modo que hospitais pediátricos e de ensino são empiricamente mais suscetíveis do que outros tipos de hospitais (GABRIEL, M. H., et al., 2018).

Além do aspecto ilícito desses incidentes de segurança, não se pode olvidar acerca da severidade dos impactos que podem dar causa, sobretudo se as ações corretivas adequadas em resposta à violação não forem tomadas de forma adequada na primeira oportunidade. Referidos impactos podem ser divididos em comportamentais (*behavioral impacts*) e operacionais (*operational impacts*) (POOL; AK; FATEHI, 2018).

A resiliência é particularmente importante cuidando-se de vazamentos de dados, pois determina que haja adaptação, para que, diante de erros ou incidentes, os sistemas e processos possam ser recompostos em suas funções essenciais.

Os impactos comportamentais compreendem atitudes e comportamentos dos pacientes. Veja-se, violações de dados comprometem a segurança dos sistemas de saúde gerando uma percepção negativa nos pacientes sobre a proteção do sistema contra invasão de privacidade. Essas preocupações com a privacidade (*privacy concerns*), influem na confiança (*trust*), no compartilhamento de informações de saúde (*health information sharing*), no uso do sistema (*system use*), pois, diante do medo de que seus dados de saúde não sejam preservados pelos provedores, pacientes evitam divulgar informações pertinentes ao serviço ou até mesmo de usá-los. Disso decorrem impactos operacionais, pois a excelência dos serviços (*care quality*) de saúde pode ser afetada quando ocorrem incidentes de violação de dados ou quando são expressas preocupações com privacidade e segurança (POOL; AK; FATEHI, 2018).

Toda essa conjuntura, marcada pelos elevados números de incidentes no setor, pluralidade de causas e severidade de impactos, é certamente motivo de grande alarme, exigindo ação corretiva imediata, ou seja, que se identifiquem as medidas preventivas que devem ser tomadas para evitar violações de dados de saúde (SEH, A. H., *et al*., 2020, p. 16-17). Note-se, é preciso proteger os atributos dos sistemas e dos dados, sua confidencialidade, sua integridade, isto é, garantir que a informação não foi alterada no seu ciclo de vida, e sua disponibilidade, de forma que a informação esteja disponível quando for acessada. Recentemente, incluiu-se um quarto atributo: a resiliência. A resiliência é particularmente importante cuidando-se de vazamentos de dados, pois determina que haja adaptação, para que, diante de erros ou incidentes, os sistemas e processos possam ser recompostos em suas funções essenciais. Para proteger esses atributos, contudo, é preciso conhecer as vulnerabilidades, ameaças e possíveis incidentes, ponderando e estruturando medidas de controle, técnicas e administrativas, para impedir que um incidente ocorra ou para diminuir a probabilidade de sua ocorrência (MENKE; GOULART, 2021).

A LGPD regulou a matéria dando atenção especial à segurança dos dados, sobretudo sensíveis. Elencada entre os princípios da LGPD (art. 6.º, inciso VII) (BRASIL, Lei n. 13.709/2018), a segurança impõe um dever geral traduzido na tomada de medidas preventivas de proteção. Embora a mencionada lei não ofereça definição conceitual de vazamento, incidente ou violação de dados pessoais, como fizera o regulamento europeu, muito se assemelha àquele ao determinar que os agentes de tratamento adotem *medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito* (art. 46, caput) (BRASIL, Lei n. 13.709/2018). Referido conceito completa-se a partir da Seção III do Capítulo VI, o qual disciplina a responsabilidade do controlador e do operador pelo tratamento irregular, assim considerado aquele que deixa de observar a legislação ou que não fornece a segurança que o titular dele pode esperar (art. 44) (BRASIL, Lei n. 13.709/2018). Há, portanto, forte incidência do princípio da boa-fé objetiva e do princípio da confiança, atribuindo deveres contínuos de vigilância aos agentes e impondo-lhes a obrigação de ressarcir os danos decorrentes da violação da segurança (parágrafo único do art. 44) (MENKE; GOULART, 2021).

Conquanto a LGPD não enumere o conteúdo dessas medidas técnicas e administrativas, subordinando seu preenchimento ao estabelecimento de guias e parâmetros propostos pela autoridade nacional (§ 1º do art. 46) (BRASIL, Lei n. 13.709/2018), estabelece critérios para o cumprimento do dever de segurança pelos agentes de tratamento. O § 1º do art. 50, ao referir-se às "boas práticas e governança", indica que deverão ser consideradas "a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos"; em complemento, o § 2º do referido artigo determina que se observe a estrutura, escala e o volume das operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade de danos para os seus titulares.

Esse controle do risco é fundamental para a segurança da informação e o cumprimento do princípio da prevenção que se encontra subscrito no dever de segurança (MENKE; GOULART, 2021). Somente a partir do conhecimento e da compreensão das vulnerabilidades que habitam o ambiente será possível projetar medidas eficazes de prevenção, monitoramento e mitigação de riscos.

A complacência dos órgãos de saúde às regras de proteção e às medidas de segurança que garantam o sigilo e o "bom uso" dos dados coletados e armazenados em suas bases serão essenciais para garantir a segurança dos dados na atual contextura informatizada, em que o setor da saúde se tornou o principal alvo de violações. Será preciso alinhar adequadamente as camadas do sistema e a Tecnologia da Informação harmonizando os novos benefícios de desempenho, capacidade e eficiência dos sistemas de saúde e a garantia dos direitos fundamentais de privacidade e dignidade humana (ARAGÃO; SCHIOCCHET, 2020, p. 702-703).

3.2 RESPOSTAS REGULATÓRIAS À VIOLAÇÃO E VAZAMENTO DE DADOS PESSOAIS NO SETOR DA SAÚDE: NOTIFICAÇÃO, MODULAÇÃO E RESPONSABILIDADE

A despeito das previsões, de caráter preventivo, dos instrumentos normativos vigentes e a tomada de medidas técnicas e administrativas de segurança, a fim de evitar tratamentos inadequados, incidentes, vazamentos ou *data breaches*, cuja possibilidade de ocorrência é uma mazela irremovível da sociedade de redes (SCHREIBER, 2020), sendo o setor de saúde particularmente afetado por estas ameaças. Reconhecendo a inafastabilidade desse risco, a LGPD determina, ratificando o espírito preventivo elucidado no item anterior, uma série de ações a serem tomadas pelo responsável pelo tratamento, para modular danos decorrentes do incidente. Imprescindível, portanto, que controladores tenham um plano de resposta a incidentes, isto é, processos internos em vigor capazes de detectar e resolver uma violação no caso de sua ocorrência (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 12).

Dentre essas ações, destaca-se a notificação à autoridade nacional e ao titular dos dados da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos seus titulares, conforme alude a redação do art. 48 da lei (BRASIL, Lei n. 13.709/2018). O intento da norma é permitir que a autoridade possa tomar medidas administrativas de controle posterior, bem como permitir que o próprio titular adote medidas particulares de proteção (MENKE; GOULART, 2021). Observe-se, contudo, que não será todo incidente de segurança que deverá ser comunicado, mas apenas aquele que possa acarretar risco ou dano relevante aos titulares. O § 3º do art. 48 da LGPD oferece um indicativo de definição da seriedade do incidente a partir do juízo de gravidade, em que *será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los* (BRASIL, Lei n. 13.709/2018). Nessa linha, dados criptografados, cuja leitura esteja impossibilitada, representam menor potencial danoso no caso de vazamentos (GRUPO DE TRABALHO DO ARTIGO 29, 2018, p. 12). Por outro lado, incidentes que comprometam ou afetem direitos dos titulares, mediante a divulgação dos dados, comprometendo a confidencialidade, ou, por meio da sua alteração, afetando sua integridade, devem ser comunicados (MENKE; GOULART, 2021).

Essa comunicação deverá ser feita em prazo razoável que, diferentemente do almejado prazo de 72 horas estabelecido pelo legislador europeu no art. 33 do RGPD, será definido, conforme determina a LGPD, pela autoridade nacional; no caso de haver demora para a notificação, como na hipótese de realização de uma investigação técnica em situações de complexidade considerável (MENKE; GOULART, 2021), por exemplo, a qual deverá ser justificada pelo responsável. A referida lei também determina que a notificação deverá conter a descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados (observados os segredos comercial e industrial), os riscos relacionados ao incidente, bem como as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo[15].

Referidas exigências podem ser ampliadas a pedido da autoridade nacional, conforme estabelece o inciso I do § 2º do art. 48 (BRASIL, Lei n. 13.709/2018), podendo esta determinar a "ampla divulgação do fato em meios de comunicação" ou impor a adoção de "medidas para reverter ou mitigar os efeitos do incidente"[16].

Essa notificação, revestida por um dever de vigilância (MARQUES, 2019), decorre dos desdobramentos da boa-fé objetiva, cuja observância deve estar presente em todas as fases obrigacionais. Resulta disso que, mesmo nos casos em que o titular não tenha mais vínculo ativo com responsável, o dever de notificação persiste nas situações em que seus dados sofram vazamento (MENKE; GOULART, 2021).

O devido cumprimento dos deveres de informação, bem como de adoção de medidas para reduzir os impactos decorrentes do incidente de segurança, além dos aspectos protetivos que carregam, também desempenham notório protagonismo na averiguação e atribuição de responsabilidade dos agentes de tratamento.

Não obstante muito se possa discutir quanto à natureza da responsabilidade do controlador e do operador prevista na LGPD[17], não há discordâncias sobre a extrema relevância de um regime suficientemente preciso de responsabilidade civil para "assegurar tutela efetiva à proteção de dados pessoais" (SCHREIBER, 2020).

O caput do art. 42 estabelece que: *O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo* (BRASIL, Lei n. 13.709/2018). Note-se que o dispositivo, apanhando uma pluralidade de espécies de danos, evita dúvidas quanto à amplitude da proteção, a qual é reservada não apenas aos titulares de dados pessoais, mas também a terceiros que possam ser atingidos pelo tratamento eivado de ilicitude. Para Anderson Schreiber (2020), *a esfera de incidência do regime de responsabilidade civil da LGPD não é demarcada pelo interesse lesado,* [...] *(e.g., titular dos dados pessoais), mas sim pela atividade*

de lesiva, incidindo a Lei sobre qualquer dano decorrente do exercício da atividade de tratamento de dados pessoais.

A proteção ampla é particularmente importante no caso de vazamentos de dados de saúde, uma vez que a variedade de danos que podem dar causa, como demonstrado no subitem anterior, é substancialmente numerosa, abarcando desde danos extrapatrimoniais, decorrentes da violação da privacidade e intimidade dos titulares, expondo-os a situações de discriminação, até danos patrimoniais, sentidos especialmente pelas instituições prestadoras de serviços de saúde.

A gravidade do incidente (art. 48, § 3º), além de indicar a obrigatoriedade da notificação, também influi na responsabilidade e no valor das sanções administrativas pelo vazamento. O art. 52 (BRASIL, Lei n. 13.709/2018) identifica as espécies de sanções administrativas as quais os agentes de tratamento de dados ficam sujeitos no caso de infrações. Apesar de distinguir as modalidades de sanções, prevendo desde advertência até a publicização da infração, o artigo trata de infrações sem, contudo, especificá-las, de forma que, no caso de vazamento de dados pessoais, a depender da severidade do incidente, poderá resultar na aplicação desde uma advertência até a determinação de multa diária, respeitado o limite de R$ 50 milhões por infração da Lei (MENKE; GOULART, 2021).

Os parâmetros e critérios das sanções são estabelecidos nos incisos do § 1º do art. 52. Tratando-se de vazamento de dados, sobretudo dados pessoais sensíveis, que importam mais danos aos seus titulares quando violados, o cumprimento de padrões, normas e adoção de medidas técnicas e organizacionais de segurança é de especial importância para avaliar a conduta do responsável pelo tratamento (art. 52, inciso VIII). Essa previsão, advertem Menke e Goulart, assemelha-se à regra geral do parágrafo único do art. 944 do Código Civil (BRASIL, Lei n. 10.406/2002), que prenuncia a redução equitativa da indenização quando diante de desproporção excessiva entre a gravidade da culpa e o dano, excetuando o princípio da reparação integral que, conforme os autores, poderia ser aplicada, por analogia, às sanções da LGPD "para justificar a redução de altas multas em situações de cumprimento adequado das normas e padrões de segurança" (MENKE; GOULART, 2021).

Dessa conjuntura, resta claro que a prevenção é o "fio condutor" da nova Lei de Proteção de Dados Pessoais no tocante à segurança. Seja para evitar vazamentos, seja para reduzir danos e modular responsabilidades, a diligência dos agentes de tratamento é pressuposto para a eficácia do direito fundamental de proteção de dados.

4 CONSIDERAÇÕES FINAIS

O aumento do uso das tecnologias transformou o setor de saúde, oportunizando novas formas de aprendizado e de prestação de serviço, redefinindo os métodos de operabilidade das instituições e elevando os níveis de eficiência dos tratamentos propostos e dos resultados obtidos. Teleconsultorias, cirurgias robóticas, televigilância, prontuário eletrônico, todos integram esse novo modelo denominado de e-Saúde que utiliza as tecnologias de informação e comunicação nos serviços de assistência ao paciente, pesquisa, capacitação dos profissionais e avaliações epidemiológicas e demográficas em saúde.

Dentro desse contexto de elevada dependência por parte do setor da saúde dos recursos de comunicação e das técnicas de compartilhamento de dados, surgem novos desafios à manutenção da segurança dessas informações, as quais ficam cada vez mais sujeitas a violações, conforme demonstrado neste estudo. Esses vazamentos, contudo, além de onerar as instituições, violam direitos fundamentais dos titulares, esvaziando de proteção aspectos de sua vida privada.

Atento ao caráter particular desses dados, os quais, interligados a aspectos mais íntimos da vida do indivíduo, podem conduzir, caso expostos, a uma discriminação do titular, o legislador nacional, à semelhança do europeu, inseriu os dados pessoais de saúde entre o rol de dados sensíveis da LGPD, atrelando ao seu tratamento uma série de rigorosas limitações.

Tais restrições somam-se, em verdadeiro espírito de prevenção que integra o arcabouço normativo, à imposição do dever de implemento de medidas de segurança técnicas e administrativas por todas as hierarquias dos agentes de tratamento de dados, evitando acessos não autorizados, perdas, alteração ou qualquer tratamento inadequado ou ilícito. É preciso, também, a elaboração de um plano de resposta a incidentes por uma equipe especializada em segurança da informação, de forma a antecipar a reação de enfrentamento no caso de vazamentos dos dados.

Se, apesar dos esforços preventivos, não for possível evitar o incidente de segurança ou ilicitude, imprescindível observar as determinações da lei, que exigem que o agente de tratamento de dados comunique, em prazo razoável, à autoridade nacional e ao titular sobre a ocorrência do incidente, permitindo a adoção de medidas que mitiguem os prejuízos, bem como aplicam sanções diante da falta de demonstração que foram efetivamente adotados os *mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados* (art. 52, § 1º, inciso VIII, da Lei n. 13.709/2018).

O adequado cumprimento das regras atinentes à segurança da informação e, portanto, a eficácia do direito de proteção de dados de saúde ultrapassa a robustez normativa, demandando o implemento adequado da saúde eletrônica, a partir da fixação de mecanismos de segurança dos bancos de dados, da priorização da autonomia informativa do titular ao longo de todas as fases do tratamento, bem como da capacitação das equipes de tratamento. Está no equilíbrio, na razoabilidade, na harmonização dos esforços, ora para prevenir riscos, ora para modular os prejuízos advindos do eventual vazamento.

NOTAS

1 O uso de tecnologias de informação e comunicação pelo setor de saúde recebeu a denominação de "e-Saúde" (e-Health), pela Organização Mundial da Saúde (OMS). Constitui-se da assistência ao paciente, pesquisa, educação/capacitação da força de trabalho e monitoração e avaliação em saúde (ARAGÃO; SCHIOCCHET, 2020, p. 698-699).

2 Veja-se o teor dos arts. 255 e 256 da Portaria de Consolidação n. 1, de 28 de setembro de 2017, in verbis: Art. 255. Esta Seção regulamenta o Sistema Cartão Nacional de Saúde (Sistema Cartão), no âmbito das ações e serviços de saúde no território nacional. Art. 256. O Sistema Cartão é um sistema de informação de base nacional que permite a identificação unívoca dos usuários das ações e serviços de saúde, com atribuição de um número único válido em todo o território nacional. (MINISTRO DE ESTADO DA SAÚDE, 2017).

3 O MÉDICO DEVE respeitar o direito do paciente à confidencialidade. É ético divulgar informações confidenciais informações quando o paciente consente ou quando há uma ameaça real e iminente de dano a paciente ou a terceiros e esta ameaça só pode ser removida por uma quebra de sigilo. (tradução livre). (WORLD MEDICAL ASSOCIATION, 2006)

4 A declaração arrola entre os princípios o dever de *proteger a vida, saúde, dignidade, integridade, direito à autodeterminação, privacidade e confidencialidade das informações pessoais de sujeitos de pesquisa* [...], *ainda que tenham dado consentimento* (tradução livre) (WORLD MEDICAL ASSOCIATION, 2013).

5 Art. 21. A assistência à saúde é livre à iniciativa privada. [...] Art. 24. Quando as suas disponibilidades forem insuficientes para garantir a cobertura assistencial à população de uma determinada área, o Sistema Único de Saúde (SUS) poderá recorrer aos serviços ofertados pela iniciativa privada. Parágrafo único. A participação complementar dos serviços privados será formalizada mediante contrato ou convênio, observadas, a respeito, as normas de Direito Público. (BRASIL, 1990).

6 Art. 230. Este Capítulo regulamenta o uso de padrões de informação em saúde e de interoperabilidade entre os sistemas de informação do SUS, nos níveis municipal, distrital, estadual e federal, e para os sistemas privados e de saúde suplementar. Parágrafo único. Os padrões de interoperabilidade e de informação em saúde são o conjunto mínimo de premissas, políticas e especificações técnicas que disciplinam o intercâmbio de informações entre os sistemas de saúde municipais, distrital, estaduais e federal, estabelecendo condições de interação com os entes federativos e a sociedade (MINISTRO DE ESTADO DA SAÚDE, 2017).

7 Art. 287. O acesso aos dados individualizados dos usuários do SUS deverá ser controlado mediante o atendimento de todos os seguintes requisitos: *I – identificação obrigatória do profissional, trabalhador ou agente de saúde que o acessar; e II – local, data e horário do acesso realizado, ou de sua tentativa, mesmo que sem sucesso* (MINISTRO DE ESTADO DA SAÚDE, 2017).

8 Ver Resolução Normativa n. 305/2012, que estabelece parâmetros para a Troca de Informações na Saúde Suplementar (AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR, 2012).

9 Assim estabelece o Art. 5º da Lei n. 13.709, de 14 de agosto de 2018 (LGPD): Para os fins desta Lei, considera-se: [...] *II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;* (BRASIL, 2018).

10 Nos termos do art. 5º, inciso X, da Lei Federal n. 13.709, de 14 agosto de 2018, conceitua-se tratamento como *toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração* (BRASIL, 2018).

11 O legislador enumerou as hipóteses em que o tratamento de dados sensíveis são admitidos sem o consentimento do titular, restringindo-as, nos termos do art. 11, inciso II, da LGPD, aos casos 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 n. 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).

12 *Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.* (BRASIL, 2018).

13 Assim determina a Resolução Normativa n. 358, de 27 de novembro de 2014 da ANS: *Art. 3º A identificação é procedimento administrativo, de competência da ANS, que verifica a ocorrência da obrigação legal de ressarcir ao SUS por meio da constatação de atendimento no SUS a beneficiário de plano privado de saúde, do cálculo do montante devido e da determinação da OPS devedora. Art. 4º A identificação será realizada mediante cruzamento de bancos de dados relativos aos atendimentos realizados nas unidades prestadoras de serviços vinculadas ao SUS com as informações cadastrais das OPS constantes do banco de dados da ANS, nos termos do art. 20 da Lei n. 9.656, de 3 de junho de 1998, e da regulamentação da ANS. § 1° O serviço de atendimento à saúde cuja continuidade tiver demandado a emissão de mais de um documento de autorização ou registro emitido.* (AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR, 2014).

14 A maior violação de dados de saúde em 2020 foi um ataque de *ransomware* ao provedor de serviços de nuvem Blackbaud Inc. Antes de implantar o ransomware, os hackers roubaram os bancos de dados de arrecadação de fundos e de doadores de muitos clientes (*Trinity Health* (3,3 milhões de registros), *Inova Health System* (1 milhão de registros) e *Northern Light Health Foundation* (657.392 registros). Dentre as informações roubadas constavam nomes, contato, datas de nascimento, bem como algumas informações clínicas. (HIPAA Journal, 2021).

15 *Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*
§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I – a descrição da natureza dos dados pessoais afetados; II – as informações sobre os titulares envolvidos; III – a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV – os riscos relacionados ao incidente; V – os motivos da demora, no caso de a comunicação não ter sido imediata; e VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. [...] (BRASIL, 2018).

16 *Art. 48.* [...] *§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I – ampla divulgação do fato em meios de comunicação; e II – medidas para reverter ou mitigar os efeitos do incidente.* (BRASIL, 2018).

17 Na esteira da longa discussão doutrinária acerca da natureza da responsabilidade civil prevista na LGPD, afirma Anderson Schreiber *que não há uma resposta unívoca à indagação sobre a espécie de responsabilidade civil que vigora no âmbito da LGPD. Tal como ocorre no Código Civil e no Código de Defesa do Consumidor, ambos os regimes de responsabilidade civil – subjetivo e objetivo – convivem na legislação de proteção de dados pessoais. Dentre as hipóteses de responsabilidade subjetiva, o legislador destacou, por meio do parágrafo único do art. 44, a hipótese de ausência de adoção das medidas protetivas indicadas no art. 46, mas isso não afasta outros casos de responsabilidade civil subjetiva (por inobservância de deveres legalmente previstos para o agente que realiza o tratamento de dados pessoais alheios) e muito menos os casos de responsabilidade civil objetiva decorrentes do tratamento de dados pessoais que não forneça a segurança que pode esperar o titular dos referidos dados, à luz das circunstâncias indicadas nos incisos do art. 44 da LGPD.* Cf. SCHREIBER, Anderson. Op. cit.

REFERÊNCIAS

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (Brasil). *Resolução Normativa n. 305, de 9 de outubro de 2012.* Brasília, DF: ANS, 2012. Disponível em: www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=MjI2OA==. Acesso em: 2 mar. 2021.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (Brasil). *Resolução Normativa n. 358, de 27 de novembro de 2014.* Brasília, DF: ANS, 2014. Disponível em: https://bit.ly/2PN0woI. Acesso em: 08 mar. 2021.

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. *Reciis*: Revista Eletrônica de Comunicação, Informação e Inovação em Saúde, Rio de Janeiro, v. 14, n. 3, p. 692-708, jul./set. 2020. Disponível em: https://docs.bvsalud.org/biblioref/2020/10/1121860/2012-8932-1-pb.pdf. Acesso em: 19 jan. 2021.

ARAÚJO, Alexandra Rodrigues et al. Saúde Móvel: desafios globais à proteção de dados pessoais sob a perspectiva do direito da União Europeia. *Reciis*: Revista Eletrônica de Comunicação, Informação e Inovação em Saúde, Rio de Janeiro, v. 10, n. 4, out./dez. 2016. Disponível em: http://www.arca.fiocruz.br/handle/icict/17000. Acesso em: 20 fev. 2021.

BRASIL. *Constituição da República Federativa do Brasil de 1988.* Brasília, DF: Presidência da República, [2016]. Disponível em: www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 3 mar. 2021.

BRASIL. *Lei n. 8.080, de 19 de setembro de 1990.* Brasília, DF: Presidência da

República, [1990]. Disponível em: www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 18 fev. 2021.
BRASIL. *Lei n. 10.406, de 10 de janeiro de 2002.* Código civil. Brasília, DF: Presidência da República, [2002]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 19 fev. 2021.
BRASIL. *Lei n. 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 jan. 2021.
BRASIL. Ministério da Saúde. *Política Nacional de Informação e Informática em Saúde*. Brasília, DF: Ministério da Saúde, 2016. Disponível em: http://bvsms.saude.gov.br/bvs/publicacoes/politica_nacional_infor_informatica_saude_2016.pdf. Acesso em: 17 fev. 2021.
BRASIL. Ministério da Saúde. *Resolução n. 196, de 10 de outubro de 1996.* Brasília, DF: Ministério da Saúde, 1996. Disponível em: bvsms.saude.gov.br/bvs/saudelegis/cns/1996/res0196_10_10_1996.html. Acesso em: 2 mar. 2021.
BRASIL. Ministério da Saúde. *Manual operacional para comitês de ética em pesquisa*. Brasília, DF: Ministério da Saúde, Conselho Nacional de Saúde, 2002. Disponível em: https://conselho.saude.gov.br/biblioteca/livros/Manual_ceps.pdf. Acesso em: 2 mar. 2021.
BRASIL. Ministério da Saúde. *Portaria de Consolidação n. 1, de 28 de setembro de 2017.* Brasília, DF: Ministério da Saúde, 2017. Disponível em: bvsms.saude.gov.br/bvs/saudelegis/gm/2017/prc0001_03_10_2017.html. Acesso em: 2 mar. 2021.
BRASIL. Ministério da Saúde. *Portaria de Consolidação n. 4, de 28 de setembro de 2017.* Brasília, DF: Ministério da Saúde, 2017. Disponível em: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2017/prc0004_03_10_2017.html. Acesso em: 2 mar. 2021.
BRITISH BROADCASTING CORPORATION. *Singapore personal data hack hits 1.5m, health authority says. BBC*, London, 20th July 2018. Disponível em: https://bbc.in/3kWREbr. Acesso em: 8 mar. 2021.
CAPURRO, Rafael; ELDRED, Michael; NAGEL, Daniel. *Digital whoness*: identity, privacy and freedom in the cyberworld. Ontosverlag: Heusenstamm, 2013. Disponível em: https://www.arte-fact.org/dgtlwhns.pdf. Acesso em: 28 fev. 2021.
CHERNYSHEV, Maxim; ZEADALLY, Sherali; BAIG, Zubair. Healthcare data breaches: Implications for digital forensic readiness. *Journal of Medical Systems*, [Wisconsin, USA], v. 43, n. 1, p. 1-12, 2019. Disponível em: 10.1007/s10916-018-1123-2. Acesso em: 28 fev. 2021.
CHIAVEGATTO FILHO, Alexandre Dias Porto. The use of big data in healthcare in Brazil: perspectives for the near future. *Revista Epidemiologia e Serviços de Saúde,* Brasília, DF, v. 24, n. 2, p. 325-332, abr./jun. 2015.
COLLINS, J. D. et al. Organizational data breaches 2005-2010: applying SCP to the healthcare and education sectors. *International Journal of Cyber Criminology,* Gujarat, India, v. 5, n. 1, p. 794-810, Jan./July 2011.
COMISSÃO EUROPEIA. Article 29 Data Protectiona Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679,* Brussels, Belgium, Fev. 2018. WP250rev.01. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 12 fev 2021.
CONSELHO FEDERAL DE MEDICINA (Brasil). *Resolução CFM n. 1.821/2007.* Brasília, DF: CFM, 2007. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2007/1821. Acesso em: 2 mar. 2021.
CONSELHO NACIONAL DE SECRETÁRIOS DE SAÚDE (Brasil). Comissão Intergestores Tripartite. *Resolução n. 6, de 25 de agosto de 2016.* Conjunto mínimo de dados da atenção à saúde. Brasília, DF: CONASS, 2016. Disponível em: https://www.conass.org.br/wp-content/uploads/2016/12/RESOLUCAO-N_6_16.pdf. Acesso em: 4 mar. 2021.
DECEMBER 2021 Healthcare Data Breach Report. *HIPAA Journal*, Liverpool, UK, Jan 18, 2022. Disponível em: https://www.hipaajournal.com/december-2021-healthcare-data-breach-report/. Acesso em: 6 abr. 2022.
DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.
DONEDA, Danilo. Considerações sobre a tutela da privacidade e a proteção de dados pessoais no ordenamento brasileiro. *In*: CONRADO, M; PINHEIRO, R.F. (coord.). *Direito privado e Constituição*: ensaios para uma recomposição valorativa da pessoa e do patrimônio. Curitiba: Juruá, 2009.
FERRY, Luc. *A inovação destruidora*: ensaio sobre a lógica das sociedades modernas. Rio de Janeiro: Objetiva, 2015.
FIRDOUSE, Mohammed *et al*. Using texting for clinical communication in surgery: a survey of academic staff surgeons. *Surgical Innovation,* Leeds, LS, v. 25, n. 3, p. 274 – 279, Jun. 2018. Disponível em: doi:10.1177/1553350618761980. Acesso em: 7 mar. 2021.
GABRIEL, M. H. *et al.* Data breach locations, types, and associated characteristics among us hospitals. *AJMC*: American Journal of Managed Care, Cranbury, NJ, v. 24, n. 2, p. 78-84, Febr. 2018.
HUMER, Caroline; FINKLE, Jim. Your medical record is worth more to hackers than your credit card. *The Philadelphia Inquirer*, Philadelphia, PA, 24 set. 2014. Disponível em: https://bit.ly/2MXeUto. Acesso em: 8 mar. 2021.
KAPLAN, Bonnie. "How should health data be used? privacy, secondary use, and big data sales". *CQ*: Cambridge Quarterly of Healthcare Ethics, Berkeley, CA, v. 25, n. 2, p. 312-329, Apr. 2016. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/cqhe25&i=333. Acesso em: 18 jan. 2021.
LEME, RS; BLANK, M. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. *Cadernos Ibero-Americanos de Direito Sanitário*, Brasília, DF, v. 9, n. 3, p. 210-224, jul./set. 2020. Disponível em: http://dx.doi.org/10.17566/ciads.v9i3.690. Acesso em: 19 fev. 2021.
LIMA, Manuela Ithamar. Do direito à proteção de dados em matéria de saúde na sociedade de informação. *Arquivo Jurídico*: Revista Jurídica Eletrônica da UFPI, Teresina, v. 4, n. 1, p. 1-24, jan./jul. de 2017.
LIU, Vincent et al. "Data breaches of protected health information in the United States". *JAMA*, Chicago, IL, v. 313, n. 14, p. 1471-1473, 2015.
MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor*: o novo regime das relações contratuais. 9. ed., rev. e ampl. São Paulo: Revista dos Tribunais, 2019. *E-book*.
MARTINS, Guilherme Magalhães; SOARES, Flaviana Rampazzo. Proteção de dados pessoais em e-saúde: seu confronto com a utilidade do fornecimento e uso de dados em aplicativos para dispositivos móveis. *Revista de Direito do Consumidor*, São Paulo, v. 130, p. 397-429, jul./ago. 2020.
MENKE, Fabiano; GOULART, Guilherme. Segurança da informação e vazamento de dados. *In*: MENDES, Laura Schertel Ferreira; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz Rodrigues; BIONI, Bruno Ricardo (coord.). *Tratado de proteção de dados pessoais.* Rio de Janeiro: Forense, 2021. p. 339-360. *E-book.*
MOLINARO, Carlos Alberto; RUARO, Regina Liden. Internet y estado de vigilancia: el desafío de la protección de datos (=Internet and the surveillance state: the challenge of data protection). *SSRN Electronic Journal,* Rochester, NY, v. 1, p. 1-30, 2013. Disponível em: https://ssrn.com/abstract=2310267. Acesso em: 18 jan. 2021.
NOVA falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, *G1*, Economia. Tecnologia. Brasília, DF, 12 dez. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 18 jan. 2021.
OUELLETTE, Patrick. Memorial Hermann Health System suffers internal data breach. *Health It Security*, Danvers, MA, 2 set. 2014. Disponível em: https://bit.ly/3v58l9i. Acesso em: 7 mar. 2021.
POOL, Javad K.; AKHLAGHPOUR, Saeed; FATEHI, Farhad: BURTON-JONES, Andrew. Causes and impacts of Personal Health Information (PHI) breaches: a scoping review and thematic analysis completed research paper. causes and impacts of personal health information breaches. PACIFIC ASIA CONFERENCE ON INFORMATION SYSTEMS, 33., 2019, X'ian, China. *Proceedings* [...]. Atlanta, GA: PACIS, 2019.
RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.
RUARO, Regina; RODRIGUEZ, Daniel. O direito à proteção dos dados pessoais. *Revista Brasileira de Direitos Fundamentais & Justiça,* Belo Horizonte, v. 4, n. 11, p. 163-180, 30 jun. 2010.
RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD): Lei 13.709/2018. *In*: MENDES, Laura Schertel Ferreira; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz Rodrigues; BIONI, Bruno Ricardo (coord.). *Tratado de proteção de dados pessoais.* Rio de Janeiro: Forense, 2021. p. 177-198. *E-book.*
SARLET, Gabrielle Bezerra Sales; FERNANDES, Márcia Santana; RUARO, Regina Linden. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. *In*: MENDES, Laura Schertel Ferreira; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz Rodrigues; BIONI, Bruno Ricardo (coord.). *Tratado de proteção de dados pessoais.* Rio de Janeiro: Forense, 2021. p. 485-506. *E-book.*
SARLET, Ingo Wolfgang; KEINERT, Tania Margarete Mezzomo. O direito fundamental à privacidade e as informações em saúde: alguns desafios. *In:* KEINERT, Tania Margarete Mezzomo *et al* (org.). *Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética*. São Paulo: Instituto de Saúde, 2015.
SARLET, Ingo Wolfgang. Direitos Fundamentais em espécie. *In*: SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 5. ed. rev. e atual. São Paulo: Saraiva, 2016. p. 400-735.
SCHREIBER, Anderson. Responsabilidade civil na lei geral de proteção de dados pessoais. *In*: MENDES, Laura Schertel Ferreira; DONEDA, Danilo; SARLET, Ingo

Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz Rodrigues; BIONI, Bruno Ricardo (coord.). *Tratado de proteção de dados pessoais.* Rio de Janeiro: Forense, 2021. p. 319-338. *E-book.*

SEH, A. H., et al. Healthcare Data breaches: insights and implications. *Healthcare,* Basel, CH, v. 8, n. 2, 2020. Disponível em: https://doi.org/10.3390/healthcare8020133. Acesso em: 10 fev. 2021. 2020 Healthcare Data Breach Report*:* 25% increase in breaches in 2020. *HIPAA Journal*, Liverpool, UK, Jan 19, 2021. Disponível em: https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/. Acesso em: 24 fev. 2021.

VENTURA, Miriam; COELI, Claudia Medina. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança. *Cadernos de Saúde Pública*: CPS, Rio de Janeiro, v. 34, n. 7, Maio 2018. Disponível em: http://cadernos.ensp.fiocruz.br/csp/artigo/486/para-alem-da-privacidade-direito-a-informacao-na-saude-protecao-de-dados-pessoais-e-governanca. Acesso em: 19 Fev:. 2021. http://dx.doi.org/10.1590/0102-311X00106818.

VIEIRA, Augusto Cesar Gadelha. O projeto cartão nacional de saúde e a construção de e-saúde para o Brasil. *In*: BARBOSA, Alexandre F. (org.). *TIC SAÚDE 2013*: pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros. 2. ed. rev. São Paulo: Comitê Gestor da Internet no Brasil, 2015. p. 33-46.

WIKINA, Suanu Bliss. What caused the breach?: an examination of use of information technology and health data breaches. *Perspectives in Health Information Management*, Columbus, OH, v. 11, Fall, 2014.

WORLD MEDICAL ASSOCIATION. The WMA International Code of Medical Ethics: 2006. *WMA*, Ferney-Voltaire, 2006. Disponível em: https://www.wma.net/wp-content/uploads/2006/09/International-Code-of-Medical-Ethics-2006.pdf. Acesso em: 2 mar. 2021.

WORLD MEDICAL ASSOCIATION. Declaration of Helsinki Ethical Principles for Medical Research Involving Human Subjects. 2013. *WMA*, Ferney-Voltaire, 2013. Disponível em: https://www.wma.net/wp-content/uploads/2016/11/DoH-Oct2013-JAMA.pdf. Acesso em: 2 mar. 2021.

Artigo recebido em 6/4/2022.
Artigo aprovado em 1/7/2022.

Camila Rosa da Mata é Advogada e Mestranda em Direito pela Universidade Federal do Rio Grande do Sul.