DIMENSÕES DA PRIVACIDADE DAS INFORMAÇÕES EM SAÚDE NO BRASIL

Virna de Barros Nunes Figueiredo

Mestre em Filosofia. Professora do Curso de Bacharelado em Direito. Doutoranda em Direito pelo Centro Universitário de Brasília – UNICEUB. Distrito Federal.

Marcelo Dias Varella

Doutor e Livre-docente em Direito. Pesquisador nível 1 do CNPq. Professor do Programa de Mestrado e Doutorado do Centro Universitário de Brasília – UNICEUB. Distrito Federal.

Resumo: Há uma tensão entre direito à privacidade e direito à saúde, não apenas no Brasil, como em vários países do mundo. A recente Lei Geral de Proteção de Dados Pessoais – LGPD –, surge como resposta inicial a tal anseio com a missão de proteger os direitos e liberdades fundamentais, em especial o direito à proteção de dados pessoais. Porém, o desafio se revela bem superior àquele que originalmente foi previsto pela norma, especialmente no que se refere aos dados sensíveis aplicáveis à saúde. Por meio de questões recentemente suscitadas ao Judiciário e da análise das Estratégias de Saúde Digital do Governo Federal, o presente estudo buscou ilustrar dificuldades e apontar algumas vulnerabilidades quanto à efetividade das proteções destinadas aos dados de saúde, que demandam um olhar diferenciado do Estado para efetivar o almejado direito à privacidade e assegurar a dignidade da pessoa que se utiliza dos serviços de saúde.

Palavras-chave: Privacidade. Dados pessoais. Saúde digital. Conflitos entre saúde e privacidade.

1 Introdução

Os avanços tecnológicos e as recentes crises sanitárias recolocaram em debate os limites da privacidade individual diante do bem estar coletivo, sobretudo quando o tema envolve saúde. No Brasil, o direito à privacidade dos dados pessoais foi recentemente consolidado pela Lei Geral de Proteção de Dados Pessoais, mas que já sofre vários desafios em face da necessidade de informações para políticas públicas de controle sanitário.

A cada momento, diversas classes de informações são colhidas e projetadas nas redes, onde se tecem incontáveis bancos de dados, em um movimento

que demanda uma reflexão sobre a necessidade de mecanismos que assegurem o direito à privacidade e confidencialidade para o indivíduo. Ao analisar a importância do acesso à Internet, questão que recentemente passou a pleitear a condição de direito humano com base no artigo 19 da Declaração Universal dos Direitos Humanos de 1948, por ser considerada ferramenta essencial e um dos principais meios para o exercício da liberdade de expressão, percebe-se que é preciso reavaliar conceitos essenciais como intimidade, privacidade e dignidade da pessoa. A humanidade se encontra sob os reflexos do antagonismo entre as ideias de exposição e compartilhamento de informações *versus* a necessidade de preservação e sigilo.

No ordenamento jurídico brasileiro a proteção à privacidade do indivíduo se encontra assegurada no rol dos direitos e garantias fundamentais da Constituição Federal de 1988, além de configurar um dos princípios norteadores do Marco Civil da Internet,[1] norma que contempla as relações estabelecidas em ambiente digital. Recentemente, esse direito tornou-se um dos pontos centrais da Lei Geral de Proteção de Dados (LGPD) que regulamenta o uso, a proteção e a transferência de dados pessoais no Brasil. A LGPD, como ficou popularmente conhecida, entrou em vigor com o objetivo de garantir maior controle dos cidadãos sobre suas informações pessoais, exigindo consentimento explícito para coleta e uso dos dados e obriga a oferta de opções para o usuário visualizar, corrigir e excluir esses dados. Em seu texto, a LGPD dedicou especial atenção aos dados obtidos em procedimentos associados à saúde, objeto sobre o qual se desenvolveu este estudo, atribuindo-lhes a condição de dados sensíveis em razão de seu conteúdo oferecer uma especial vulnerabilidade, e ensejar possibilidade de discriminação.[2]

Assim, a partir da caracterização do cenário intangível do mundo tecnológico e da visão do Estado brasileiro acerca do direito à saúde, ora ampliado para a esfera digital, o presente artigo tem por objetivo apresentar uma reflexão sobre os desafios do Poder Judiciário ao buscar estabelecer uma tutela de preservação para os dados sensíveis, em especial aqueles aplicáveis à saúde, a partir de ponderações realizadas mediante a análise da Estratégia de Saúde Digital para o Brasil. Na busca de uma melhor compreensão acerca da relevância e possíveis desdobramentos da matéria, o estudo apresenta ainda, a visão de bibliografias

[1] A Lei nº 12.965/14, denominada Marco Civil da Internet, tem como objetivo estabelecer princípios, garantias, direitos e deveres para o uso da *internet* no Brasil, bem como regular como se daria nesse contexto a atuação da União, dos Estados, do Distrito Federal e dos Municípios, pode ser encontrada em: BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias e deveres para o uso da internet. Brasília: Presidência da República, 2014.

[2] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais* - A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2018.

específicas e se serve de exemplos de casos recentes de questões relacionadas aos dados sensíveis de saúde que acometeram a sociedade brasileira.

2 O direito à saúde e as tecnologias na sociedade da informação

As inovações tecnológicas características da quarta revolução industrial se tornam ainda mais evidentes nas matérias científicas e na área de saúde. A Organização Mundial de Saúde (OMS) afirma que a ideia de saúde deve ser compreendida em sentido amplo, como um estado de completo bem-estar físico, mental e social e não somente enquanto ausência de afecções e enfermidades. Logo, trata-se de um processo em constante evolução.

Diante da incorporação de tecnologias no setor da saúde,[3] testemunha-se a cada dia a descoberta de novos métodos para cuidar e melhorar a qualidade de vida da população e o surgimento do que a OMS convencionou chamar de "e-health" ou "e-saúde", com a criação de sistemas de informação e comunicação, que resultam na prática de atenção facilitada e aperfeiçoada para aquele que busca cuidados. O e-saúde[4] abrange assistência ao paciente, pesquisa, educação e capacitação da força de trabalho e monitoração e avaliação em saúde.

O direito à saúde que se encontra elencado como direito fundamental, é simultaneamente um instrumento de proteção ao indivíduo e um meio de assegurar o próprio direito à vida, inviolável conforme o artigo 5º da Constituição Federal. Está ainda, diretamente relacionado ao princípio da dignidade da pessoa humana, sendo este princípio fundamental da República Federativa do Brasil, nos termos do artigo 1º, de modo que se infere que para que seja possível uma vida digna, é necessário que todos vivam bem e, por conseguinte, com saúde.[5] Ainda, nos termos do artigo 196, tem-se a saúde como direito de todos e dever do Estado, a ser garantido mediante políticas sociais e econômicas que visem a redução dos riscos de doença e de outros agravos e o acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação.

---

3 Desde a década de 1970, as inovações tecnológicas no setor de saúde desenvolvem o que se denominou de *e-health* ou Saúde Eletrônica. Ver em: BRASIL. *A experiência brasileira em sistemas de informação em saúde*. Ministério da Saúde, Organização Pan-Americana da Saúde, Fundação Oswaldo Cruz. v. 2. Brasília: Editora do Ministério da Saúde, 2009.

4 O uso do conceito "e-Saúde" espelha uma estratégia para a adoção de padrões de informática em saúde para o atendimento de diretrizes propostas pelas políticas de informação em saúde mundiais. Ver em: BRASIL. *Política Nacional de Informação e Informática em Saúde*. Ministério da Saúde, Secretaria-Executiva, Departamento de Monitoramento e Avaliação do SUS. Brasília: Ministério da Saúde, 2016.

5 Para Sandra Regina Martini (2017, p. 140), o direito humano à saúde se configura, hoje, como um dos mais importantes direitos, sem o qual é impossível pensar na efetivação de outros direitos. Por isso, este se configura como ponte para a cidadania efetiva: a saúde é um bem da própria comunidade.

Dessa forma, enquanto bem intangível de todos os seres humanos, a saúde é considerada digna da tutela protetiva estatal, apresentando-se como um dever do Estado a ser observado de forma plena, não apenas por meio de regulação legal, mas também através da efetivação de políticas públicas governamentais. Somente é possível se falar na garantia de uma vida digna mediante a promoção de medidas de bem-estar e vida saudável. A responsabilidade do Estado pela criação de políticas públicas que permitam acesso aos serviços necessários à promoção da saúde é executada por via de normas infraconstitucionais, tais como a Lei nº 8.080/90, que regulamenta o Sistema Único de Saúde, bem como estabelece princípios e diretrizes para a saúde em nosso país e ora enfrentam o desafio de abarcar os novos paradigmas oriundos da influência da tecnologia no setor.

Na sociedade da informação, os dados pessoais configuram verdadeiras extensões do indivíduo demandando proteções eficazes. No caso da saúde, tratam-se de informações que na maioria dos casos são fornecidas pelo próprio cidadão sobre sua condição física e mental e que são classificadas como sensíveis pela LGPD, dado seu potencial discriminatório na hipótese de serem reveladas em determinadas situações e sem o devido consentimento de seu titular.

Os direitos à intimidade e à vida privada foram inicialmente reconhecidos em documentos internacionais, como a Declaração Americana dos Direitos e Deveres do Homem (1948), a Declaração Universal dos Direitos Humanos (1948) e o Pacto Internacional de Direitos Civis e Políticos (1966). Somente na década de 1970 eles passaram a ser expressamente garantidos em textos constitucionais, como a Constituição de Portugal de 1976 e a Constituição da Espanha de 1978. A partir daí, esses direitos passam a integrar o rol de direitos fundamentais.[6] No Brasil, desde a Constituição de 1824, há previsão do direito à inviolabilidade do domicílio e da correspondência, matizes do direito à privacidade. A Constituição Federal de 1988, por sua vez, em seu artigo 5º, inciso X, foi pioneira ao consagrar expressamente a proteção da intimidade e da vida privada no ordenamento jurídico brasileiro.

Ressalte-se que a intimidade deve ser entendida como uma esfera da privacidade ainda mais íntima do que a vida privada. Trata-se de um espaço impenetrável e indevassável, que diz respeito apenas ao próprio indivíduo, como recordações pessoais, memórias, diários etc. A esfera da intimidade abrange, portanto, a do segredo, ou seja, os assuntos delicados a ponto de a pessoa não desejar partilhar com ninguém. Já a vida privada consiste em uma esfera um pouco mais abrangente: diz respeito a assuntos que, a princípio estão blindados contra a intromissão

[6] FARIAS, Edilson Pereira de. *Colisão de Direitos*: a honra, a intimidade, a vida privada e a imagem *versus* a liberdade de expressão e de informação. 3. ed. Porto Alegre: Sérgio Antonio Fabris, 2008, p. 117-118.

alheia, mas que podem ser partilhadas, de acordo com o desejo e a conveniência do indivíduo. Nesse sentido, Ferraz Júnior defende que a intimidade corresponde a um âmbito mais exclusivo da vida privada:

> A intimidade é o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum). Não há um conceito absoluto de intimidade, embora se possa dizer que o seu atributo básico é o estar-só, não exclui o segredo e a autonomia. [...] Já a vida privada envolve a proteção de formas exclusivas de convivência. Seu atributo máximo é o segredo, embora inclua também a autonomia e, eventualmente, o estar-só com os seus. [...] A vida privada pode envolver, pois, situações de opção pessoal, mas que, em certos momentos, podem requerer a comunicação a terceiros. Por aí ela difere da intimidade, que não experimenta esta forma de repercussão.[7]

Dessa forma, entende-se que o constituinte fez uso de ambos os termos com o objetivo de assegurar a máxima aplicabilidade da norma, na medida em que pretende afastar qualquer espécie de interferência, pública ou privada, em assuntos íntimos dos indivíduos ou inerentes à sua personalidade. Essa preocupação assume especial importância no âmbito da sociedade da informação, em que tais direitos são constantemente ameaçados, em decorrência da popularização da rede mundial de computadores, do crescimento exponencial de bancos de dados e da utilização indevida de dados pessoais, muitas vezes sem o consentimento do titular.

Diante dessa realidade, há de se admitir que o direito à privacidade não mais pode ser entendido como "direito a ser deixado só", ou seja, como mera liberdade negativa de recusar ou de proibir a utilização das informações sobre a própria pessoa. Mais que isso, a privacidade na quarta revolução industrial consiste na liberdade positiva de poder controlar os dados a ela concernentes, e deve ser lido sob o prisma do direito à autodeterminação informativa, como um direito fundamental, além de direito da personalidade.

Essa releitura do direito à privacidade na sociedade da informação se faz necessária com o intuito de evitar a perda do controle do indivíduo sobre os seus dados pessoais, sobretudo aqueles que podem ensejar qualquer forma de discriminação. Assim, defende-se uma nova forma de tutela da privacidade que não

[7] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: direito à privacidade e os limites à função fiscalizadora do Estado. *In*: *Revista da Faculdade de Direito USP*, v. 88, 1993, p. 439-459.

se limita à proibição à intromissão alheia na vida íntima, isto é, um dever geral de abstenção, mas impõe também deveres de caráter positivo. Como ensina Schreiber, ultrapassando a dimensão procedimental, vinculada ao tratamento destinado aos dados pessoais desde sua coleta até o momento de sua eliminação em caráter definitivo, a privacidade possui uma dimensão substancial, conectada à própria utilização da informação obtida. Todo indivíduo possui o direito de controlar a representação de si mesmo constituída a partir de seus dados e informações pessoais. É direito de toda pessoa exigir que tal representação reflita a realidade, impedindo que seu uso assuma caráter discriminatório.[8]

Não obstante a urgência de atuação do legislador com vistas a promover a manutenção do sigilo e a proteção de dados pessoais, somente em 2018 foi editada a Lei Geral sobre a Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018 –, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A lei brasileira dispôs acerca da proteção de dados como um dos paradigmas da dignidade humana, conforme o disposto no Regulamento Geral de Proteção de Dados da União Europeia (RGPD), no qual se considera os direitos da personalidade como projeção da dignidade humana e a proteção de dados como espécie daquele. Logo, elementos como consentimento informado e legítimo interesse, seriam utilizados como parâmetros na busca pela preservação da autonomia da vontade e controle, pelos cidadãos, do uso dos dados e informações pessoais.[9]

A LGPD veio em boa hora e assume ainda mais importância no momento em que o Brasil ainda enfrenta os efeitos da pandemia de Covid-19, que acarretou a desorganização dos setores produtivos e a sobrecarga do sistema de saúde. Não se pode admitir que a crise sanitária sirva como pretexto para a inobservância da legislação em matéria de proteção de dados pessoais, sendo assim considerados toda informação relacionada a pessoa natural identificada ou identificável, nem para o descumprimento dos deveres dos responsáveis pelo tratamento de dados pessoais, em prejuízo dos indivíduos e, notadamente, dos pacientes, no caso de dados médicos. No que tange a estes últimos, os hospitais devem dedicar especial atenção à proteção das informações de seus pacientes, sob pena de responsabilização civil por eventuais vazamentos, utilização indevida ou outras condutas que, de alguma forma, violem a privacidade, tendo em vista se tratarem de dados pessoais sensíveis, como será abordado em maior profundidade nas secções subsequentes deste trabalho.

8 SCHREIBER, Anderson. *Direitos da personalidade*. 2. ed. São Paulo: Atlas, 2013, p. 141.

9 GONÇALVES, Tânia Carolina Nunes Machado. *Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal*: desafios, modelos e principais impactos com a nova Lei. Dissertação (Mestrado em Direito). Centro Universitário de Brasília (UniCEUB): Brasília, 2019, p. 94.

3 Da proteção jurídica de dados pessoais relacionados à saúde

O desenvolvimento tecnológico das últimas décadas permitiu enorme expansão da capacidade de armazenamento e processamento de informações, com o surgimento de novas tecnologias que possibilitaram mais agilidade, rapidez e facilidade de acesso aos dados. A utilização da *internet* proporcionou ao tratamento de dados pessoais um diferencial em termos quantitativo e qualitativo. Em outros termos, passou a ser possível o processamento de mais dados em menos tempo, com a aplicação de técnicas mais sofisticadas, de forma a extrair resultados mais úteis e valiosos dos dados, coletados diretamente de seus titulares ou obtidos a partir da transferência daqueles armazenados em outros bancos de dados.[10]

A despeito dos diversos benefícios econômico-sociais de se ter todas as informações disponíveis em bancos de dados conectados a uma rede, percebe-se que a internet se tornou um espaço fragilizado justamente por conter informações de todos os níveis de conhecimento. Embora o desenvolvimento da ciência objetivamente se encontre caracterizado por um processo focado no bem-estar social, por vezes os recursos disponíveis ao público permitem certa multiusabilidade que pode dar ensejo a utilizações com finalidades prejudiciais a terceiros. Daí a necessidade de criação de ferramentas jurídicas que regulamentem e permitam a tutela de tais fatos quando necessário.[11]

No Brasil, até a primeira metade de 2018, inexistia legislação específica sobre a proteção de dados pessoais.[12] Havia apenas normas esparsas, insuficientes para regular o tema com efetividade, em sua completude. Dentre elas, merecem menção a Lei do Habeas Data (Lei nº 9.507, de 12 de novembro de 1997), o Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990), a

[10] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 172.

[11] VELASCO, Nara. Privacidade: Direito A Intimidade Na Era Digital. *Revista Ciência e Sociedade*, v. 1, n. 1, 2016.

[12] Na União Europeia, a matéria já era regulada na década de 1990, com a Diretiva 95/46/CE e, no início dos anos 2000, com a Diretiva 2002/58/CE da União Europeia, sobre o tratamento de dados pessoais e sobre a proteção da privacidade no setor das comunicações eletrônicas, respectivamente. Em abril de 2016, foi aprovado o Regulamento UE 2016/679 do Parlamento Europeu e do Conselho, para a regulação comum da matéria pelos países-membros, em substituição às normas anteriores. Ver em: PARLAMENTO EUROPEU – CONSELHO EUROPEU. Directiva 2002/58/CE, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de las Comunidades Europeas*. 2002. Disponível em: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF. Acesso em: 19 jul. 2021. Ou em: PARLAMENTO EUROPEU – CONSELHO EUROPEU. *Diretiva 95/46/CE, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Anacom, 1995. Disponível em: http://www.anacom.pt/render.jsp?categoryId=332397. Acesso em: 19 jul. 2021.

Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011), a Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011) e o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014).

Somente com a edição da Lei nº 13.709, de 14 de agosto de 2018, o Brasil finalmente passou a possuir uma Lei Geral sobre a Proteção de Dados Pessoais. Com entrada em vigor originalmente prevista para vinte e quatro meses após a data de sua publicação, a LGPD acabou por percorrer tortuosos caminhos, primeiramente com seu período de *vacatio legis* estendido até 3 de maio de 2021 pela Medida Provisória nº 959, de 29 de abril de 2020. Contudo, o artigo 4º da referida Medida Provisória que embasava a extensão do prazo foi tempos depois considerado prejudicado e, assim, o adiamento nele previsto passou a ser desconsiderado. Em 18 de agosto de 2020 entrou em vigor.

A disciplina da proteção de dados pessoais pela LGPD tem como fundamentos, expressos no seu artigo 2º, o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, dentre outros. A sua aplicabilidade diz respeito a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que exista algum elemento de conexão com o Brasil (artigo 3º). Relevante, portanto, apresentar o conceito legal de bancos de dados e tratamento, constantes do artigo 5º da LGPD:

> Art. 5º Para os fins desta Lei, considera-se:
>
> IV – banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> [...]
>
> X – tratamento: 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.[13]

Dessa forma, entende-se que a referida legislação considera tratamento de dados pessoais qualquer atividade que tenha como objeto a manipulação de dados pessoais, como o seu armazenamento em bancos de dados, que podem

[13] BRASIL. Congresso Nacional. *Lei nº 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

promover inclusive o seu cruzamento e a interconexão de bases de dados diversas, além da sua transmissão para terceiros. Quanto aos requisitos para o tratamento de dados pessoais, o artigo 7º da LGPD estabelece um rol de hipóteses em que será permitido o tratamento de dados pessoais. No que interessa ao presente trabalho, cabe destacar os casos de tratamento mediante o fornecimento de consentimento pelo titular (inciso I), para a proteção da vida ou da incolumidade física do titular ou de terceiro (inciso VII) e para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (inciso VIII).

A Recomendação Relativa à Proteção e Uso de Dados Relacionados à Saúde,[14] elaborada pela força-tarefa sobre privacidade e proteção de dados relacionados à saúde da Organização das Nações Unidas (ONU), por sua vez, lança luz sobre o que se deve entender por "dados relacionados à saúde". Segundo o relatório, são eles todos os dados pessoais referentes à saúde física ou mental de um indivíduo, incluindo a prestação de serviços de saúde, que revelem informações sobre a sua saúde passada, atual ou futura. Dados genéticos são igualmente considerados dados relacionados à saúde no entendimento desta recomendação. Ademais, os dados relacionados à saúde referentes, mas não limitados, aos resultantes de testes, como diagnóstico pré-natal, diagnóstico de pré-implantação ou identificação de características genéticas, sejam ou não considerados dados relacionados à saúde da mãe, devem ser protegidos ao mesmo nível que outros dados relacionados à saúde.

Nesse universo, estão incluídos o tratamento de dados pessoais relacionados à saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias, bem como o tratamento de dados pessoais para o fim de realização de estudos e pesquisas científicas, por exemplo. Tratam-se de informações íntimas, que necessitam de mecanismos específicos que assegurem sua proteção, segurança e confidencialidade.

No campo da saúde, o princípio da confiança ultrapassa os contornos da ética e se funda como alicerce primário da relação entre o paciente e os profissionais responsáveis por orientar e conduzir o tratamento que influenciará nas condições de vida do indivíduo. Contudo, é preciso recordar que a transmissão desses dados sensíveis perpassa uma extensa cadeia de serviços para além da relação médico-paciente, ao tempo em que abrange seguradoras, laboratórios, prestadores de serviços subcontratados, entre muitos outros.

[14] UNITED NATIONS. *Special Rapporteur on the Right to Privacy*. Draft Recommendation on the protection and use of health-related data. 2019, p. 06.

Mediante o conteúdo sensível que permeia as informações de saúde, é imperioso que as instituições e organizações que atuam neste setor, seja na esfera pública ou na esfera privada, estabeleçam uma organização que permita o armazenamento e tratamento adequado desses dados, distanciando-os o máximo possível de vazamentos ou qualquer tipo de violação. Para tanto, se faz necessária a implementação de políticas específicas, que congreguem organização, processos e tecnologias a serviço da segurança, privacidade e integridade dos cidadãos brasileiros e os primeiros avanços neste sentido têm sido apresentados por uma série de planos, projetos e documentos assinados pelo Ministério da Saúde, dentre os quais se destacam as Estratégias de Saúde Digital para o Brasil.

4 A privacidade nas estratégias de saúde digital para o Brasil

As propostas para o desenvolvimento e implantação da saúde digital foram sistematizadas e apresentadas pelo governo brasileiro nos últimos anos e embora afirmem a necessidade da proteção da privacidade dos dados de saúde, não se verifica até o presente momento, um aprofundamento adequado da questão. Em que pese a elaboração de princípios e a indicação de atividades norteadoras e práticas futuras, a realidade atual carece de respostas concretas que ainda não se encontram disponíveis por meio de uma normativa específica. Para analisar este cenário, propõe-se a seguir uma breve retrospectiva documental.

No ano de 2016, foi apresentada a Política Nacional de Informação e Informática em Saúde (PNIIS) com o objetivo de nortear ações de tecnologia da informação e comunicação (TIC) de todo o sistema de saúde brasileiro.[15] Em seu conteúdo, a questão da privacidade surge inicialmente na apresentação de seus princípios básicos que incluem a confidencialidade, sigilo e privacidade da informação de saúde pessoal como direito de todo indivíduo. Em sequência, surge associada ao recurso de certificação digital e ao final é exposta como uma das principais barreiras para a implantação de projetos de TI em saúde, denotando fragilidade e incertezas quanto a seus meios garantidores em via prática.

[15] O texto da PNIIS, de caráter orientador, apresenta princípios e diretrizes norteadores de uma organização institucional, tais como: a melhoria da qualidade e do acesso ao sistema de saúde brasileiro; a transparência e segurança da informação em saúde; o acesso à informação de saúde pessoal como um direito do cidadão; o suporte da informação para tomada de decisão por parte do gestor e profissional de saúde; e, por fim, o desenvolvimento institucional do SUS e de todo o sistema de saúde brasileiro, com ganhos de eficiência na redução do número de sistemas de informação em saúde existentes ou sua simplificação, gestão e formação de pessoas, aquisição de insumos, monitoramento e avaliação das ações, logística, pagamento e transferência de recursos e outros processos-meio, pode ser visto em: BRASIL. *Política Nacional de Informação e Informática em Saúde*. Ministério da Saúde, Secretaria-Executiva, Departamento de Monitoramento e Avaliação do SUS. Brasília: Ministério da Saúde, 2016.

No ano seguinte, uma visão mais concreta sobre a saúde digital foi oferecida por meio do documento intitulado Estratégia e-Saúde para o Brasil, aprovado pela Resolução CIT nº 19, de 22 de junho de 2017, da Comissão Intergestores Tripartite (CIT), que apresentou diretrizes e princípios para o Sistema Único de Saúde (SUS), além de dispor sobre a política brasileira de governo eletrônico, destacando a proposta de Saúde Digital apontando mecanismos contributivos para sua incorporação ao SUS. Conforme tal documento, a e-Saúde estaria incorporada ao SUS na condição de dimensão fundamental até o ano de 2020, possibilitando uma melhoria consistente dos serviços de Saúde por meio da disponibilização e uso de informação abrangente, precisa e segura. Seriam as tecnologias aplicadas um caminho para que se atinja um patamar superior de qualidade na atenção e nos processos de saúde, nas três esferas de governo, bem como no setor privado, beneficiando pacientes, cidadãos, profissionais, gestores e organizações de saúde.[16]

Como meio de concretização da visão proposta para a e-saúde brasileira foi indicado o programa do governo federal intitulado Concecte SUS,[17] composto por um sistema integrador direcionado a fomentar o apoio à informatização e ao intercâmbio de informações entre os estabelecimentos de saúde. Tendo sido materializado por meio de aplicativo aberto ao uso de operadores da saúde e cidadãos em geral, o Conecte SUS segue o mesmo padrão das políticas de privacidade dos aplicativos do Ministério da Saúde e apresenta uma série de regras com o objetivo de preservar a confidencialidade das informações que serão armazenadas em seu sistema e ainda um documento informativo ao titular dos dados de saúde, no qual se esclarecem importantes questionamentos sobre o acesso às informações e até mesmo a possibilidade da recusa do compartilhamento dos dados em saúde.

Por meio da "Nota Informativa ao Titular de Dados de Saúde"[18] o usuário é informado que seus dados de saúde estarão disponíveis por trinta minutos ao profissional, devidamente habilitado a acessar os dados da Rede Nacional de Dados em Saúde, que esteja prestando atendimento a você ou à pessoa que você seja responsável legal. Segundo informa o documento, o profissional habilitado terá acesso a informações de caráter administrativo (por exemplo: data e horários de atendimento, entrada e saída do estabelecimento), informações relativas a medicamentos distribuídos, internações hospitalares, atendimentos ambulatoriais, de vacinação e resultados de exames, considerando dados coletados a partir de janeiro de 2018. Em nenhum momento, porém, explicita por quanto tempo

[16] BRASIL. *Estratégia de Saúde Digital para o Brasil 2020-2028*. [recurso eletrônico]. Ministério da Saúde, Secretaria-Executiva, Departamento de Informática do SUS. Brasília: Ministério da Saúde, 2020.

[17] CONECT SUS. *Plataforma de saúde para o cidadão, profissionais e gestores de saúde do Sistema Único de Saúde Brasileiro*, 2021.

[18] CONECT SUS APLICATIVO. *Nota Informativa ao Titular de Dados de Saúde*, 2021.

as informações serão mantidas no sistema e quais as formas de controle para assegurar que apenas o profissional em atendimento terá aceso aos dados de saúde daquele indivíduo.

Nas disposições contidas no Termos de Uso e Políticas de Privacidade,[19] diversos tópicos são apresentados aos usuários, tais como a obrigação da observância às normas vigentes e destinação dos serviços apenas para finalidades lícitas nos termos da legislação brasileira; o esclarecimento pela responsabilidade do conteúdo e notas sobre propriedade intelectual. No tópico "Leis, regulamentos, direitos e deveres" é explicitado ao usuário a observação das normas de proteção de dados, o cumprimento de todas as leis e regulamentos aplicáveis, os quais podem ser modificados de tempos em tempos. E mais à frente, surge referência expressa à questão do respeito à privacidade e adequação à LGPD que parecem contrastar com a garantia de sigilo e anonimato ofertada em caráter parcial. Conforme se infere do texto, a garantia de sigilo e anonimato das informações produzidas pelo utilizador do sistema, será relativizada não apenas nos casos de exigência legal, ou para tratar de questões de descumprimento, mas também mediante a possibilidade de utilização interna de informações visando uma contribuição que será vinculada ao apelido do usuário, em substituição aos dados pessoais dos utilizadores. Ambos os textos silenciam sobre meios e práticas para a efetivação do sigilo e confidencialidade prometidos.

Ciente da necessidade destas e de outras análises sobre a operacionalização do sistema, o Ministério da Saúde que caracterizou o Conect Sus como um programa de evolução contínua, a ser monitorado e avaliado sistematicamente e para este fim, foi aprovado no ano de 2019 na 34ª Reunião Ordinária do Comitê Gestor da Estratégia de Saúde Digital e posteriormente pactuado por *Ad Referendum* em 30 de março de 2020, o Plano de Ação, Monitoramento e Avaliação destinado a identificar, priorizar e integrar, de forma coordenada, programas, projetos e ações de saúde de forma a implantar as iniciativas que compõem o sistema Conecte SUS. Ainda no mesmo ano, foi proposto o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), com o objetivo organizar e apresentar a estratégia de TIC e o conjunto de resultados esperados durante o período de 2019 a 2021 do DATASUS do Ministério da Saúde. Este plano trouxe como um dos princípios orientadores das atividades de governança digital, a segurança e privacidade e propôs expressamente a elaboração do marco legal de e-saúde no país. Conforme aponta o escrito, os serviços públicos digitais devem propiciar

[19] CONECT SUS APLICATIVO. *Termos de Uso de Aplicativo e Políticas de Privacidade*, 2021.

disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações, além de proteger o sigilo e a privacidade pessoais dos cidadãos na forma da legislação.[20]

Nos Estados Unidos e na Europa, onde há anos existe o prontuário eletrônico de pacientes, a discussão está em um nível bastante diferente. Cada médico consegue acessar, automaticamente, os dados completos dos pacientes, mesmo aqueles fornecidos por outros médicos, em consultas e tratamentos anteriores. Contudo, isso apenas é realizado com o consentimento do paciente. Existem políticas públicas em discussão há alguns anos. A principal se refere ao estímulo aos pacientes de publicizarem seus prontuários eletrônicos para a pesquisa científica. Com o cruzamento dos dados de saúde de milhares de pessoas, seria mais fácil prever novas doenças e mesmo identificar possíveis tratamentos mais efetivos.

O Sistema Nacional de Saúde no Reino Unido, por exemplo (NHS), desde 25 de maio de 2018, permite que os pacientes autorizem a divulgação de seus prontuários eletrônicos, de forma anonimizada, para finalidades além do seu próprio tratamento. Interessante notar que se presume a aceitação, ou seja, aqueles contrários devem se manifestar e desautorizar expressamente o compartilhamento de informações.[21]

No Brasil, em momento mais recente, foi publicada por meio da Portaria GM/MS nº 3.632, de 21 de dezembro de 2020, a versão mais recente do documento Estratégia de Saúde Digital para o Brasil 2020-2028[22] que, com base nos avanços obtidos pelos projetos que compõem o Programa Conecte SUS, ratifica a proposta original, enquanto procura sistematizar e consolidar as ações realizadas ao longo da última década, acrescentando uma visão futura, segundo a qual a Rede Nacional de Dados em Saúde (RNDS) estará estabelecida e reconhecida como a plataforma digital de informação e inovação e serviços de saúde, apresentando benefício em diversas esferas. Aqui se discute a própria criação de prontuários eletrônicos, compartilhados ou não.

Dentre as indicações contidas nesse documento, poucas linhas são dedicadas à palpitante questão da proteção de dados por operadores e usuários dos sistemas de saúde. A proposta nesta seara é desenhada em uma abordagem quase generalista, sem ainda enfatizar peculiaridades verificadas no contexto nacional.

[20] BRASIL. *Plano Diretor de Tecnologia da Informação e Comunicação* – 2019/2021 (1ª Revisão de 2020). Brasília – DF: Ministério da Saúde. 2020.

[21] NHS. *Sharing your health records*. About the NHS, 2018.

[22] Documento que apresenta a Estratégia de Saúde Digital para o Brasil com uma visão de oito anos, isto é, até o final de 2028. Ver em: BRASIL. *Estratégia de Saúde Digital para o Brasil 2020-2028* [recurso eletrônico]. Ministério da Saúde, Secretaria-Executiva, Departamento de Informática do SUS. Brasília : Ministério da Saúde, 2020.

Em fato, as consequências e limites do uso de tecnologias aplicadas à saúde ainda mantêm uma série de incógnitas, tanto no que se refere aos inúmeros benefícios e avanços que se projetam para o futuro quanto aos perigos decorrentes do vazamento de informações. Nas disposições sobre a legislação e a regulação para a saúde digital apresentada, merece destaque positivo a indicação expressa da necessidade de uma norma apta a prover segurança jurídica a todos os envolvidos, garantindo direitos essenciais como os de confidencialidade e privacidade de dados, corroborando a orientação do PDTIC de 2019 e a previsão de definição e adoção de normas e padrões para a representação, armazenamento, troca e utilização de dados de saúde, incluindo as terminologias clínicas e os aspectos legais referentes ao uso da informação, como a LGPD.

Conforme o texto, as iniciativas de saúde digital devem se pautar pela Lei Geral de Proteção de Dados e como caminho para essa adequação são indicadas as seguintes atividades: identificação dos pontos críticos de alinhamento à LGPD para a expansão da Rede Nacional de Dados em Saúde (RNDS); identificação de modelos de compartilhamento de dados de saúde alinhados à LGPD; proposição de modelos robustos de consentimento esclarecido e informado de fácil compreensão, implementação e adesão pelo paciente; proposição de modelos de autenticação, segurança, sigilo e privacidade. Por meio dessas atividades apontadas como prioritárias pretende-se gerar segurança jurídica, enquanto consequência da privacidade e confidencialidade dos dados, o que sem dúvidas beneficia não apenas usuários, profissionais, gestores e organizações, mas também promove o fortalecimento da credibilidade da Saúde Digital, permitindo maior aceitação e alcance do sistema, destacando seus benefícios e minorando seus riscos.

No que se refere à regulação de ambientes de inovação e interconectividade, foi pontuado que além do cumprimento dos ditames da LGPD, as regras de participação, troca de informações, financiamento e utilização dos resultados da colaboração sejam claramente estabelecidas e alinhadas. A implementação de uma normativa específica viabilizaria que as colaborações envolvendo dados de saúde se realizem de maneira segura e transparente para cidadãos, órgãos de controle e sociedade civil em geral. Destaca ainda, a pertinência da definição de critérios éticos, de propósito de utilização e de responsabilidade legal quanto aos dados coletados. Para esta proposta, o plano governamental recomenda como primeiro passo identificar e atrair os atores relevantes; estabelecer o arcabouço legal e organizacional para a regulação da colaboração; implementar, avaliar e aprimorar continuamente os processos de regulação.

Por este panorama, tornam-se claros os esforços do governo brasileiro para a implantação da saúde digital com a integração das informações de todos os setores, sejam originárias da esfera pública ou privada, mediante a construção de

um arcabouço organizacional, legal, regulatório e de governança, que possibilite o desenvolvimento adequado de serviços e procedimentos da área. Contudo, o aprofundamento das questões sobre privacidade parece ter ficado em um segundo plano, possivelmente em aguardo ao que poderá emergir a partir da aplicação prática dos mecanismos recentemente implementados, enquanto as situações imediatas permanecem sendo discutidas à luz da visão geral apresentada pela LGPD.

5 Desafios da saúde digital no contexto brasileiro

A questão da privacidade no contexto da saúde digital demanda reflexão. Em uma análise mais concreta de questões envolvendo a proteção de dados do sistema de saúde digital já aplicado em território nacional torna-se perceptível a multiplicação das ameaças à privacidade no contexto da assistência médico-hospitalar, em decorrência de falhas na segurança da atividade de tratamento de dados pessoais dos pacientes. Dentre os processos do e-Saúde incluem-se hoje, o Cartão Nacional de Saúde adotado no Sistema Único de Saúde (SUS), teleconsultorias, telediagnóstico, segunda opinião clínica, telecirurgia, telemonitoramento, televigilância, educação permanente, teleducação e prontuário eletrônico. Contudo, esses novos recursos nem sempre oferecem a segurança necessária para seus usuários, conforme pode ser constatado com o exemplo do prontuário eletrônico.

Ao fornecer as informações solicitadas para o preenchimento do prontuário, documento de extrema relevância que norteia o tratamento médico, o paciente declara uma série de informações pessoais que, divulgadas de forma indevida, poderiam trazer prejuízos que vão desde constrangimento até formas de discriminação. Enquanto em sua versão eletrônica, os prontuários asseguram atualização, legibilidade e exatidão das informações, por outro lado exigem cuidados quanto a seu sigilo e proteção, visto que o uso secundário dos dados colhidos por terceiros de má-fé poderia acarretar diversos prejuízos seja do ponto de vista físico, econômico ou até mesmo psíquicos.

O Superior Tribunal de Justiça (STJ) teve a oportunidade de examinar um caso que ilustra os riscos da utilização de dados pessoais relativos à saúde para a realização de golpes e fraudes, em prejuízo do titular dos dados e de seus familiares. No caso concreto, uma quadrilha de estelionatários supostamente teve acesso a informações sigilosas armazenadas no servidor de um hospital, como o cadastro interno e o prontuário médico da paciente, à época internada na Unidade de Terapia Intensiva.

O cônjuge da paciente, então, recebeu ligação telefônica de uma pessoa que se identificou como médico plantonista, informando a necessidade de realização

de um exame urgente, motivo pelo qual deveria depositar uma quantia em dinheiro, via transferência bancária, que seria ressarcida pelo plano de saúde. Não percebendo se tratar de fraude, tendo em vista que o suposto profissional detinha informações confidenciais a respeito do estado de saúde de sua esposa, bem como dados pessoais que o levaram a acreditar que de fato se tratava de pessoa ligada ao hospital em que estava internada, o homem realizou os pagamentos, somente constatando mais tarde que fora vítima de um golpe. Então, pleiteou indenização por danos materiais e morais contra o hospital, alegando falha na prestação do serviço, com base no Código de Defesa do Consumidor, decorrente da falha na guarda de dados pessoais. O pedido foi indeferido em primeira e segunda instâncias, sendo assim ementado o acórdão do julgamento de Recurso de Apelação pelo Tribunal de Justiça do Distrito Federal e Territórios (TJDFT):[23]

> CIVIL, PROCESSUAL CIVIL E CONSUMIDOR. REPARAÇÃO POR DANOS MORAIS E MATERIAIS. FALHA NA PRESTAÇÃO DE SERVIÇO HOSPITALAR. AUSÊNCIA DE NEXO DE CAUSALIDADE. INDENIZAÇÃO INDEVIDA. 1. A responsabilidade civil do estabelecimento hospitalar é objetiva, não se questionando da ocorrência ou não de culpa, bastando que se comprove a ocorrência do dano e o nexo de causalidade com a prestação defeituosa do serviço, conforme preceitua o *caput* do artigo 14 do Código do Consumidor. 2. Não se desincumbindo a parte autora da tarefa de comprovar o liame causal existente entre a suposta falha na guarda de informações do paciente e o prejuízo financeiro por ela suportado, inviável se apresenta o pedido compensatório por danos morais e materiais. 3. Inexistindo elemento evidenciando que o hospital repassou dados pessoais de paciente internado em suas dependências, a facilitar a realização de estelionato, afasta-se o dever indenizatório. 4. Recurso desprovido.

Dessa forma, o tribunal de piso julgou improcedente o pedido indenizatório, ao argumento de que não teria ficado comprovado que os danos experimentados pelo autor foram ocasionados por falhas na prestação do serviço pelo hospital, haja vista que a prova do liame causal existente entre os eventos e os danos constituiria ônus da parte autora, tarefa da qual não se desincumbiu. Na oportunidade, o TJDFT ponderou que, embora não descartada a possibilidade abstrata de que tenha havido falha na guarda de dados do prontuário médico da paciente, seria

[23] BRASIL. Acórdão nº 1133378, 07014199820178070017. Relator: Mario-Zam Belmiro. 8ª Turma Cível, Data de julgamento: 25/10/2018, publicado no *DJE*: 6/11/2018. Tribunal de Justiça do Distrito Federal e Territórios, 2018.

preciso que viessem aos autos provas robustas para provar o nexo de causalidade a gerar o dever indenizatório. Irresignado, o autor recorreu para o Superior Tribunal de Justiça.

O STJ, em decisão datada de 20 de setembro de 2019, em sede de Agravo em Recurso Especial – AREsp 1.558.260/DF, conheceu do Agravo, mas não do Recurso Especial, em virtude do óbice da Súmula nº 7 do STJ ("A pretensão de simples reexame de prova não enseja recurso especial"), entendendo que a pretensão recursal demandaria o reexame do acervo fático-probatório juntado aos autos.[24]

À luz da LGPD, no entanto, entende-se que o deslinde da controvérsia poderia ser outro. Isso porque o seu artigo 43 prevê que os agentes de tratamento só não serão responsabilizados quando provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído, que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído não houve violação à legislação de proteção de dados, ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. Logo, o ônus da prova, nesse caso, seria atribuído ao hospital. Ademais, o artigo 44 da referida Lei dispõe que o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, dentre as quais: o modo pelo qual é realizado, o resultado e os riscos que razoavelmente dele se esperam e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Ainda segundo a lei, caberia ao hospital zelar pela segurança e do sigilo de dados de seus pacientes. Isso porque, nos termos do artigo 46, os agentes de tratamento devem adotar 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. Vale ressaltar ainda o disposto no artigo 4º da Lei nº 13.787, de 27 de dezembro de 2018, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente,[25] no sentido de que os meios de armazenamento

[24] BRASIL. *Agravo em Recurso Especial nº 1558260/DF*. Min. João Otávio de Noronha (Presidente), Superior Tribunal de Justiça, 2019.

[25] O Conselho Federal de Medicina define prontuário médico como "o documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo" (Resolução CFM 1.638/2002, artigo 1º). Ver em: BRASIL. *Resolução CFM nº 1.638/2002* (Publicada no D.O.U. de 9 de agosto de 2002, Seção I, p.184-5). Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde, 2002.

de documentos digitais deverão protegê-los do acesso, do uso, da alteração, da reprodução e da destruição não autorizados. No caso específico dos documentos hospitalares, solicita-se a utilização do nível mais alto de assinatura eletrônica, de modo a possibilitar rastrear quem teve acesso ao documento. No nível intra-hospitalar, tal exigência inexiste, para dar agilidade ao acesso a dados por médicos e enfermeiros, mas é de esperar que os hospitais tenham instrumentos de rastreabilidade de acesso a dados para evitar violações à privacidade e eventual responsabilização em caso de abusos.

No contexto da pandemia de Covid-19 que assola o Brasil, a discussão acerca dos riscos da utilização indevida de dados pessoais relativos à saúde assume especial importância, sobretudo pelas graves implicações que pode provocar para o indivíduo que teve sua privacidade violada, e em alguns casos, também para toda a sociedade. Um exemplo disso ocorreu antes mesmo do registro oficial do primeiro caso da doença no Brasil, em fevereiro de 2020, na cidade de Foz do Iguaçu, Paraná, quando um paciente deu entrada em uma Unidade de Pronto Atendimento com suspeita de gripe. Na ocasião, o médico responsável pelo atendimento confundiu os sintomas com os do coronavírus, tendo solicitado exames e registrado a suspeita de Covid-19 no prontuário do paciente. Logo em seguida, uma cópia do documento começou a se espalhar pela *internet*. A suspeita do vírus foi descartada em seguida, após a chegada do resultado dos exames, mas o boato já havia se disseminado, gerando pânico na população.[26]

A Covid-19 também tem realçado o elevado potencial discriminatório dos dados pessoais relativos à saúde. Diversos casos de discriminação têm sido noticiados, inclusive contra profissionais de saúde, como o caso de um médico que contraiu o coronavírus no trabalho e passou a receber ligações intimidatórias e ameaças dos vizinhos pelo interfone, no período em que precisou ficar em isolamento domiciliar. Ele narrou ao Portal de Notícias G1 que, quando soube que estava acometido com a doença, procurou o síndico do prédio para avisar sobre o seu quadro de saúde e pedir apoio para que os porteiros recebessem as suas compras e deixassem na porta, para que ele não precisasse usar o elevador e as áreas comuns do edifício. O síndico, então, colocou um comunicado no elevador alertando os demais sobre um morador que tinha sido positivado e, dois ou três dias depois, as ligações anônimas pelo interfone começaram. Segundo o médico, os vizinhos não ligavam para prestar solidariedade, mas para fazer críticas contra ele e pedir que se mudasse do edifício para não contaminar os demais moradores.[27]

[26] CLICKFOZ. *Secretaria de Saúde desmente caso de Coronavírus em Foz do Iguaçu*. ClickFoz. 2021.

[27] RODRIGUES, Rodrigo. Médico se recupera do coronavírus em SP, mas relata hostilidade dos vizinhos durante isolamento. *GLOBO – G1*. 2020.

Logo, deve-se reafirmar que se trata de dados com elevado potencial discriminatório, cuja utilização pode ensejar consequências especialmente lesivas, oferecendo riscos potenciais mais elevados do que a média para o seu titular e até mesmo para uma coletividade. Nesta categoria se pode citar aqueles relativos a raça ou etnia, preferências políticas, religiosas e sexuais, além dos dados referentes à saúde, como o histórico médico e os dados genéticos ou biométricos de um indivíduo.[28]

Neste contexto, nota-se uma diferença importante de políticas públicas aceitáveis entre diferentes países em relação aos dados pessoais. Em vários países orientais, o direito coletivo prepondera sobre o individual. A dignidade é coletiva, mais do que individual.[29]As medidas adotadas na China para o combate da pandemia do coronavírus demonstram essa visão. Não apenas houve o rastreamento de pessoas infectadas, como houve testagem massiva obrigatória, reconhecimento facial de pessoas infectadas e informações a todos que tiveram contatos com os infectados.

Nos países europeus e nos Estados Unidos, muito se utilizou uma ferramenta desenvolvida pelo Google e pela Apple para rastreamento de pessoas infectadas e comunicação aos contatos, de forma a garantir o sigilo sobre a identificação da pessoa contaminada. No Brasil, um instrumento similar foi tentado, mas não alcançou escala.

A LGPD, ao disciplinar o tratamento de dados pessoais sensíveis, prevê que ele somente poderá ocorrer em determinados casos, a saber: com o consentimento do titular ou seu responsável legal, de forma específica e destacada, para finalidades exclusivas ou, sem fornecimento de consentimento do titular, dentre outras hipóteses, quando for indispensável para cumprimento de obrigação legal ou regulatória pelo controlador; realização de estudos por órgão de pesquisa; proteção da vida ou da incolumidade física do titular ou de terceiro; ou tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

A legislação brasileira, portanto, reconheceu o caráter sensível dos dados pessoais relativos à saúde, bem como a necessidade de exigir um nível maior de proteção no seu tratamento. Nesse sentido, salutar a vedação expressa à comunicação ou uso compartilhado entre controladores de dados pessoais sensíveis

[28] Lei nº 13.709/2018. Art. 5º 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).

[29] VARELLA, Marcelo; MONEBHURRUN, Nitish; GONTIJO, André Pires. *Proteção internacional dos direitos humanos*. Rio de Janeiro: Processo, 2019, p. 204.

referentes à saúde com objetivo de obter vantagem econômica.[30] Entretanto, a própria legislação em um movimento perigoso permite excepcionalmente a utilização ou compartilhamento de dados relativos à saúde nas hipóteses relacionadas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir a portabilidade de dados, quando solicitada pelo titular, ou as transações financeiras e administrativas resultantes do uso e da prestação dos referidos serviços de saúde.[31] Também é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.[32]

Por fim, importa ressaltar que, na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. Na hipótese de divulgação dos resultados ou de qualquer excerto desses estudos ou pesquisas, em nenhuma hipótese poderão ser revelados dados pessoais. Além disso, o órgão de pesquisa será o responsável pela segurança dessas informações, não permitida, em circunstância alguma, a transferência dos dados a terceiro.[33]

A princípio, o Ministério da Saúde se responsabiliza pela manutenção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, bem como qualquer forma de tratamento inadequado ou ilícito por meio de seus aplicativos. Em conformidade ao art. 48 da LGPD, o Ministério da Saúde deverá comunicar ao usuário e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao Titular. Porém, há muitos desdobramentos nesta intrincada rede que se amplia vertiginosamente. Tem-se incontáveis possibilidades para além dos aplicativos governamentais envolvendo o uso das tecnologias na esfera da saúde, de modo que a necessidade de uma normativa específica, conforme já apontado por meio dos documentos que

[30] BRASIL, 2018, cit. Lei nº 13.709/2018. Art. 11, parágrafo 4º.
[31] BRASIL, 2018, cit. *Lei nº 13.709/2018*.
[32] BRASIL, 2018, cit. *Lei nº 13.709/2018*. Art. 11, parágrafo 5º.
[33] BRASIL, 2018, cit. *Lei nº 13.709/2018*. Art. 13.

compõem as estratégias de saúde digital para o Brasil deve ser alçada ao patamar de prioridade.

Contudo, os esforços do direito brasileiro encontram seus limites na própria característica de transnacionalidade tanto do direito sanitário como das novas tecnologias. Tanto as doenças, como as soluções eletrônicas para sua solução não respeitam fronteiras. Yuval Harari bem coloca que a tendência de globalização eletrônica das soluções de saúde, com monitoramento digital contínuo e tratamento imediato, de acordo com padrões globais, para toda a humanidade, o que deve revolucionar a medicina, deve se acentuar daqui a alguns anos.[34] Neste caso, torna-se possível que os cidadãos do mundo sejam tratados por sistemas eletrônicos transnacionais, talvez de forma muito mais efetiva.

A dúvida é se o direito nacional, com regras próprias, será suficiente para se sobrepor à força dos fatos, com os avanços tecnológicos ou se o direito brasileiro vai continuar a convergir com o direito internacional. O mais provável, nesse caso é que não apenas as regras, mas as soluções possíveis para garantir a privacidade caminhem cada vez mais para instrumentos tecnológicos próprios de preservação da dignidade e para regras de conduta globais do que para instrumentos legislativos nacionais. Nessa tensão entre dignidade e saúde, restará decidir qual a lógica de proteção da dignidade que prevalecerá: a defesa do individual ou a defesa do coletivo.

6 Considerações finais

Para além dos processos eletrônicos e da utilização de *softwares* e meios de inteligência artificial, testemunham-se mudanças nas formas de interpretar e aplicar o Direito. Neste breve estudo foi possível constatar a evolução do direito à privacidade, enquanto um dos pilares do Estado Democrático de Direito, atualmente interpretado de forma ampla e associado ao direito de controle de imagem e informações do indivíduo. A proteção de dados pessoais emerge como um direito autônomo que se fixa no rol dos direitos fundamentais através dos fundamentos do parágrafo 2º do artigo 5º da Constituição Federal de 1988 e desperta uma série de inquietações para a sociedade da informação.

O direito à saúde originalmente atrelado à noção de vida digna e bem-estar passa a despertar preocupações associadas a confidencialidade e intimidade privada de seus destinatários, atraindo os olhos do Estado para a necessidade diferenciada de meios que assegurem a proteção de dados. Pelo presente estudo,

[34] HARARI, Y. N. *21 lições para o século 21*. São Paulo: Companhia das Letras, 2009.

evidenciou-se que na seara da saúde, os processos ganham eficiência e os resultados são otimizados por meio das vias tecnológicas, sendo interesse do Estado implementar a saúde digital. Contudo, a partir das novas práticas são gerados dados pessoais sensíveis que carecem de meios específicos de proteção em virtude das graves consequências ocasionadas a partir de sua divulgação indevida. Ainda que inverídica, a informação disseminada possui por si só potencial de agredir e discriminar o indivíduo e terceiros que com este se relacionem.

É notório que a exposição de dados de qualquer natureza sem a devida autorização pode gerar prejuízos ao seu titular, mas quando se fala em dados oriundos de matérias relativas à saúde a questão se agrava e demanda respostas do Poder Judiciário. Informações coletadas em ambiente em face da saúde pública, especialmente em procedimentos realizados por empresas privadas, necessitam de termos e condições bem definidos que esclareçam sobre sua utilização, acesso, compartilhamento, armazenamento e descarte, bem como possíveis responsabilizações. Neste aspecto, a LGPD configura um importante avanço ao dispor sobre procedimentos de organização, tratamento e sistemas de dados, que deverão ser implementados por profissionais e organizações de saúde, porém não oferta uma regulamentação específica para abarcar os inúmeros casos associados à área que se apresentam diariamente em solo brasileiro.

A insuficiência da norma legal aqui relatada era de certo modo esperada, visto a infinidade de possibilidades de má utilização dos dados sensíveis de saúde, somada ao fato de que os progressos tecnológicos velozmente alteram processos e sistemas, apresentando constantes mutações na esfera da segurança digital. Em que pese todos os esforços realizados no tratamento de informações, tem-se acompanhado com certa frequência episódios de vazamento de dados pessoais relativos à saúde, que acabaram por alimentar a realização de golpes e fraudes. Ao se pensar sobre a condução e manuseio de informações pessoais em saúde é preciso ir além de prontuários e exames, atingindo a consciência de que a matéria é bem mais ampla do que se apresenta nas breves linhas da LGPD, a exemplo das inesperadas problemáticas que eclodiram com a pandemia da Covid-19.

Outro ponto de atenção se fixa no alto custo regulatório para a aplicação e fiscalização dos procedimentos a serem adotados conforme a norma. Diante do rigor das políticas propostas para o controle dos dados pessoais, de sua coleta ao descarte, as organizações de saúde assumem uma imensa responsabilidade, vez que seu acervo ultrapassa exames, prontuários e informações biométricas, atingindo ainda registros financeiros, informações de seguros de saúde e inúmeros fornecedores. Deste modo, a adequação exigida demandará não apenas recursos financeiros, mas especialmente tempo para que se preparem profissionais e para

que se altere toda a perspectiva de cibersegurança, conforme previsto nas estratégias de Saúde de Digital.

Há necessidade, portanto, de uma revisão profunda tanto na via documental quanto na via operacional para cumprir as exigências da LGPD e efetivar as atividades prioritárias indicadas na Estratégia de Saúde Digital para o Brasil, iniciando-se pelos avisos legais de tratamento de dados pessoais com informações para cumprir com os princípios do artigo 6º sobre finalidade, adequação e necessidade, que determinam que o tratamento de dados pessoais ocorra com propósitos legítimos, específicos, explícitos e informados, compatíveis com a finalidade informada e limitados ao mínimo necessário.

Logo, o desafio enfrentado pelo Estado nesse caso, perpassa o reconhecimento dos impactos das tecnologias na promoção do direito à saúde e de seus possíveis desdobramentos e abraça a difícil meta de efetivar políticas e instrumentos capazes de viabilizar as proteções pretendidas na Carta Magna de 1988, na LGPD e em seu planejamento técnico, ao tempo em que equilibra as noções de sigilo, dignidade e segurança com a promoção do progresso por meio das tecnologias e do amplo acesso à informação, reduzindo a sensação de vulnerabilidade do indivíduo, em especial daquele que em busca da conservação de sua saúde, fornece seus próprios dados com a confiança da proteção de sua privacidade.

Abstract: There is a tension between the right to privacy and the right to health, not only in Brazil, but in many countries around the world. The recent General Law for the Protection of Personal Data – LGPD, emerges as a initial response to this desire with the mission of protecting fundamental rights and freedoms, especially the right to the protection of personal data. However, the challenge proves to be far superior to that originally envisaged by the standard, especially with regard to sensitive data applicable to health. Through questions recently raised to the Judiciary and the analysis of the Federal Government's Digital Health Strategies, the present study sought to illustrate difficulties and point out some vulnerabilities regarding the effectiveness of the protections aimed at health data, which demand a different view from the State to effect the desired right to privacy and to ensure the dignity of the person using health services.

Keywords: Privacy. Personal data. Digital Health. Conflicts between health and privacy.

Referências

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

BRASIL. *Agravo em Recurso Especial nº 1558260/DF*. Min. João Otávio de Noronha (Presidente), Superior Tribunal de Justiça. 2019. Disponível em: https://ww2.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=100856741&num_registro=201902296573&data=20190927&tipo=0%20Acesso%20em:%2017%20mai.%202020. Acesso em: 22 ago. 2021.

BRASIL. *Estratégia de Saúde Digital para o Brasil 2020-2028* [recurso eletrônico]. Ministério da Saúde, Secretaria-Executiva, Departamento de Informática do SUS. Brasília: Ministério da Saúde, 2020. Disponível em: https://saudedigital.saude.gov.br/a-estrategia-brasileira/. Acesso em: 15 maio 2021.

BRASIL. *Estratégia de Saúde Digital para o Brasil 2020-2028* [recurso eletrônico]. Ministério da Saúde, Secretaria-Executiva, Departamento de Informática do SUS. Brasília: Ministério da Saúde, 2020. Disponível em: http://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 29 abr. 2021.

BRASIL. *Política Nacional de Informação e Informática em Saúde*. Ministério da Saúde, Secretaria-Executiva, Departamento de Monitoramento e Avaliação do SUS. Brasília: Ministério da Saúde, 2016. 56 p.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias e deveres para o uso da internet. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 jul. 2021.

BRASIL. *Lei nº 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: 17 abril. 2021.

BRASIL. Plano Diretor de Tecnologia da Informação e Comunicação – 2019/2021 (1ª Revisão de 2020). Brasília – DF: Ministério da Saúde. 2020. Disponível em: https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/PlanoDiretordeTecnologiadaInformaoeComunicao.pdf. Acesso em: 17 maio 2021.

BRASIL. *A experiência brasileira em sistemas de informação em saúde*. Ministério da Saúde, Organização Pan-Americana da Saúde, Fundação Oswaldo Cruz. v. 2. Brasília: Editora do Ministério da Saúde, 2009.

BRASIL. *Política Nacional de Informação e Informática em Saúde*. Ministério da Saúde, Secretaria-Executiva, Departamento de Monitoramento e Avaliação do SUS. Brasília: Ministério da Saúde, 2016. Disponível em: https://www.conasems.org.br/wp-content/uploads/2019/02/politica_nacional_infor_informatica_saude_2016.pdf. Acesso em: 23 mar. 2021.

BRASIL. *Resolução CFM nº 1.638/2002* (Publicada no D.O.U. de 9 de agosto de 2002, Seção I, p.184-5). Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. 2002. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm. Acesso em: 17 abr. 2021.

BRASIL. Acórdão nº 1133378, 07014199820178070017. Relator: Mario-Zam Belmiro, 8ª Turma Cível, Data de julgamento: 25/10/2018, publicado no *DJE*: 6/11/2018. Tribunal de Justiça do Distrito Federal e Territórios. 2018. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/busca?q=RELATOR+MARIO-ZAM+BELMIRO. Acesso em: 20 mar. 2021.

CLICKFOZ. *Secretaria de Saúde desmente caso de Coronavírus em Foz do Iguaçu*. ClickFoz. 2021. Disponível em: https://www.clickfozdoiguacu.com.br/secretaria-de-saude-desmente-caso-de-coronavirus-em-foz-do-iguacu/. Acesso em: 19 maio 2021.

CONECT SUS APLICATIVO. *Nota informativa ao titular de dados de saúde*. 2021. Disponível em: https://conectesus-paciente.saude.gov.br/menu/termo-uso. Acesso em: 17 maio 2021.

CONECT SUS APLICATIVO. *Termos de Uso de Aplicativo e Políticas de Privacidade*. 2021. Disponível em: https://conectesus-paciente.saude.gov.br/menu/termo-uso. Acesso em: 17 maio 2021.

CONECT SUS. *Plataforma de saúde para o cidadão, profissionais e gestores de saúde do Sistema Único de Saúde Brasileiro*. 2021. Disponível em: https://conectesus.saude.gov.br/home. Acesso em: 17 jun. 2021.

DIARIO OFICIAL DE LAS COMUNIDADES EUROPEAS. *Directiva 2002/58/CE*, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). 2002. Disponível em: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF. Acesso em: 19 jul. 2021.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

FARIAS, Edilson Pereira de. *Colisão de Direitos*: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e de informação. 3. ed. Porto Alegre: Sérgio Antonio Fabris, 2008.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: direito à privacidade e os limites à função fiscalizadora do Estado. *In*: *Revista da Faculdade de Direito USP*, v. 88, 1993, p. 439-459.

GONÇALVES, Tânia Carolina Nunes Machado. *Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal*: desafios, modelos e principais impactos com a nova Lei. Dissertação (Mestrado em Direito). Centro Universitário de Brasília (UniCEUB): Brasília, 2019, p. 94.

HARARI, Y. N. *21 lições para o século 21*. São Paulo: Companhia das Letras, 2009.

MARTINI, Sandra Regina. Direito e fraternidade: a saúde do "outro" esquecido no trabalho humanitário. *In*: MARTINI, Sandra Regina; CAVACLANTI, Ana Elizabeth Lapa Wanderley (Org). *O movimento entre os saberes*: os desafios dos direitos humanos na sociedade da informação. Porto Alegre: Evangraf, 2017.

JORNAL OFICIAL DAS COMUNIDADES EUROPEIAS. *Directiva 95/46/CE do Parlamento Europeu e do Conselho*, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 19 jul. 2021.

NHS. *Sharing your health records*. About the NHS. 2018. Disponível em: https://www.nhs.uk/using-the-nhs/about-the-nhs/sharing-your-health-records/. Acesso em: 10 jun. 2021.

RODRIGUES, Rodrigo. Médico se recupera do coronavírus em SP, mas relata hostilidade dos vizinhos durante isolamento. *GLOBO – G1*. 2020. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/05/01/medico-se-recupera-do-coronavirus-em-sp-mas-relata-hostilidade-dos-vizinhos-durante-isolamento.ghtml. Acesso em: 19 abr. 2021.

SCHREIBER, Anderson. *Direitos da personalidade*. 2. ed. São Paulo: Atlas, 2013.

UNITED NATIONS. *Special Rapporteur on the Right to Privacy*. Draft Recommendation on the Protection and Use of Health-Related Data. 2019. Disponível em: https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf. Acesso em: 19 maio 2021.

VARELLA, Marcelo; MONEBHURRUN, Nitish; GONTIJO, André Pires. *Proteção internacional dos direitos humanos*. Rio de Janeiro: Processo, 2019.

VELASCO, Nara. Privacidade: Direito a Intimidade na Era Digital. *In*: *Revista Ciência e Sociedade*, Macapá, n. 1, v. 1. 2016. Disponível em: http://periodicos.estacio.br/index.php/cienciaesociedade/article/view/2104/1232. Acesso em: 18 maio 2021.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

FIGUEIREDO, Virna de Barros Nunes; VARELLA, Marcelo Dias. Dimensões da privacidade das informações em saúde no Brasil. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 16, n. 47, p. 319-343, jul./dez. 2022.

Recebido em: 20.07.2021
Pareceres: 10.09.2021, 01.10.2021
Aprovado em: 13.10.2021