https://doi.org/10.29397/reciis.v14i3.2012

ARTIGOS ORIGINAIS

Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde

General Data Protection Law: Unified Health System challenge

Ley General de Protección de Datos: desafío del Sistema Único de Salud

Suéllyn Mattos de Aragão[1,2,a]
suellyn@ufpr.br | https://orcid.org/0000-0002-4497-1621

Taysa Schiocchet[3,b]
taysa_sc@hotmail.com | https://orcid.org/0000-0002-6703-9036

[1] Ministério Público Estadual do Paraná. Centro de Apoio Operacional das Promotorias de Proteção à Saúde Pública. Curitiba, PR, Brasil.
[2] Universidade Federal do Paraná. Unidade de Saúde Ocupacional. Curitiba, PR, Brasil.
[3] Universidade Federal do Paraná. Programa de Pós-graduação em Direito. Curitiba, PR, Brasil.

[a] Mestrado em Saúde Coletiva pela Universidade Federal do Paraná
[b] Doutorado em Direito pela Universidade Federal do Paraná.

RESUMO

A Lei Geral de Proteção de Dados (LGPD) promulgada no Brasil em 2018 é reflexo do movimento internacional de busca pela preservação de direitos fundamentais como privacidade, intimidade, honra, direito de imagem e dignidade humana. O objetivo do estudo foi o de apontar em que medida a estrutura do sistema público de saúde brasileiro será impactada pela publicação da Lei e indicar eventuais caminhos a serem trilhados nesse sentido. Trata-se de pesquisa de abordagem qualitativa, descritiva e exploratória, com utilização do método dedutivo a partir de pesquisa bibliográfica/artigos e documental/ordenamento jurídico. Os resultados alcançados apontam para a estreita relação entre o SUS e a necessidade de proteção de dados sensíveis e de boas práticas em segurança da informação, com impacto direto na privacidade de pacientes. A partir dos resultados, concluiu-se que o SUS será eminentemente impactado pela LGPD e, dada a imponência de sua estrutura de tecnologia da informação, deverá adotar medidas diligentes e céleres para seu amoldamento à Lei.

Palavras-chave: Sistemas de informação; Segurança computacional; Confidencialidade; Privacidade; Sistema Único de Saúde.

ABSTRACT

The General Data Protection Law enacted in Brazil in 2018 reflects the international movement for the preservation of fundamental rights such as privacy, intimacy, honor, image rights and human dignity. The objective of the study was to point out to what extent the structure of the Brazilian public health system will be impacted by the publication of the Law and to indicate possible paths to be taken in this direction. This is a qualitative, descriptive and exploratory research using the deductive method from the analysis of articles and legal order. The results achieved point to the relationship between SUS and the need to protect sensitive data and good practices in information security, with direct impact on patient privacy. From the results, it was concluded that the SUS will be eminently impacted by GDPL and, given the importance of its information technology structure, it should take diligent and fast measures to comply with the Law.

Keywords: Information systems; Computer security; Confidentiality; Privacy; Unified Health System.

RESUMEN

La Ley General de Protección de Datos, promulgada en Brasil en 2018, reflexionó sobre el movimiento internacional para la preservación de principios fundamentales como la privacidad, la intimidad, el honor, la dirección de la imagen y la dignidad humana. El propósito de este estudio es determinar en qué medida el sistema público del sistema público brasileño se verá afectado por la publicación de la Ley e indicar eventuales caminos a seguir en esta dirección. Esta es una investigación cualitativa, descriptiva y exploratoria que utiliza el método deductivo con análisis de artículos y orden legal. Los resultados obtenidos apuntan a la estrecha relación entre el SUS y la necesidad de proteger los datos confidenciales y las buenas prácticas en seguridad de la información, con impacto directo en la privacidad del paciente. Con base en los resultados, se concluye que el SUS se verá afectado de manera eminente por la LGPD y, dada la imposición de su estructura de tecnología de la información, será necesario adoptar medidas diligentes y rápidas para su enmienda a la Ley.

Palabras clave: Sistemas de información; Seguridad computacional; Confidencialidad; Privacidad; Sistema Único de Salud.

INFORMAÇÕES DO ARTIGO

Contribuição dos autores:
Concepção e desenho do estudo: Suéllyn Mattos de Aragão, Taysa Schiocchet.
Aquisição, análise ou interpretação dos dados: Taysa Schiocchet.
Redação do manuscrito: Suéllyn Mattos de Aragão, Taysa Schiocchet.
Revisão crítica do conteúdo intelectual: Taysa Schiocchet.

Declaração de conflito de interesses: Não há.

Fontes de financiamento: Não há.

Considerações éticas: Não há.

Agradecimentos/Contribuições adicionais: Agradecemos à valorosa contribuição técnica por parte dos revisores da Revista Eletrônica de Comunicação, Informação e Inovação em Saúde, cujo olhar foi fundamental para a qualificação e o refinamento do artigo.

Histórico do artigo: submetido: 12 ago. 2019 | aceito: 01 jul. 2020 | publicado: 30 set. 2020.

Apresentação anterior: Não houve.

INTRODUÇÃO

Nas últimas décadas as organizações têm empenhado esforços no sentido de se adaptarem e de acompanharem as transformações e as necessidades sociais, desenvolvendo novos meios de resposta para os cidadãos e novas vias de comunicação e de transmissão da informação, sustentados por sistemas tecnológicos estruturados. Estas mudanças conduziram-nos para uma 'sociedade da informação', em que a ordenação e a organização dos dados adquirem papel preponderante e basilar em todos os setores e atividades, em instituições públicas e privadas. Trata-se de uma época histórica de desenvolvimento tecnológico sem precedentes, reconhecida como a do conhecimento e da tecnologia[1]. Em vista disso, a preocupação com o binômio segurança dos dados e privacidade individual tomou corpo e vem ganhando os holofotes em todo o mundo.

Como consequência da recente promulgação da Lei Geral de Proteção de Dados (LGPD), n° 13.709/2018, no Brasil, inúmeras instituições, especialmente aquelas que coletam e tratam dados pessoais sensíveis, deverão adotar medidas para adequar-se à nova legislação, inclusive as pertencentes ao Sistema Único de Saúde (SUS). Justamente aqui reside o objeto de estudo do presente artigo, traduzido no seguinte problema de pesquisa: como a aplicação da LGPD pode ajudar a coibir danos pela discricionariedade do Estado brasileiro quanto às informações de saúde das pessoas? A lacuna que o presente escrito pretende preencher diz respeito às persistentes dúvidas técnicas e jurídicas quanto à forma de aplicação e de impacto da LGPD no sistema público de saúde brasileiro.

Nesse sentido, o objetivo do manuscrito é o de apontar em que medida a estrutura do sistema público de saúde brasileiro será, de fato, impactada pela publicação da LGPD e indicar, como contribuição, eventuais caminhos a serem trilhados na necessária adequação do sistema. Para tanto, será adotada uma abordagem qualitativa, descritiva e exploratória, com utilização do método dedutivo, pois parte das premissas da LGPD (normas e princípios) e sua aplicação ao SUS para propor ações e estratégias pontuais em relação a determinados aspectos. A metodologia se utiliza ainda das técnicas de pesquisa de revisão de artigos [bibliográfica] e de análise do ordenamento jurídico [documental]. O referencial teórico se situa no campo jurídico da proteção de dados e da estrutura de tecnologia da informação do SUS. O artigo será estruturado em três tópicos: LGPD, Proteção de Dados no Sistema Único de Saúde e Caminhos para harmonização do SUS à LGPD.

Vale dizer que a LGPD é realidade próxima, pendente apenas de exíguo lapso até sua integral implantação no país, e a relativa escassez de debates acadêmicos e teóricos pertinentes à sua relação com o sistema público de saúde brasileiro é aspecto social que também impulsionaram essa pesquisa.

LEI GERAL DE PROTEÇÃO DE DADOS

O crescimento exponencial da valoração de informações, o cenário de desenvolvimento tecnológico e o tráfego digital on-line transformaram a comunicação nas últimas décadas e expuseram fragilidades até então latentes quanto à privacidade individual e ao acesso às informações pessoais. O dado passou a ser bem dos mais valiosos. A quarta revolução industrial impactou diretamente o desenvolvimento da economia e a estabilidade social, oferecendo oportunidades e ameaças. Novos termos passaram a compor a realidade e a demandar regulamentação jurídica: computação em nuvem, big data, inteligência artificial, mineração de dados, internet das coisas, aprendizado de máquinas, ataques cibernéticos e proteção de dados pessoais[2]. O massivo desenvolvimento tecnológico aumentou o potencial de utilização abusiva ou indevida dos dados pessoais ao mesmo tempo em que acentuou a vulnerabilidade do direito à intimidade.

O direito à privacidade passou a ser construído teoricamente a partir das mudanças ocorridas na sociedade com a ascensão da burguesia no século XVIII[3]. A atual valorização da ideia de privacidade,

ligada à ética informacional, é caracteristicamente um valor moral que predomina nas culturas ocidentais, correlacionada aos ideais democráticos e aos princípios de autonomia e liberdade[4].

Ter sua privacidade protegida significa, no mundo moderno, possuir autonomia. Capurro[5] entende o conceito fundamentalmente sob a denominação de "autonomia informacional", que consiste no poder de escolha do indivíduo acerca do uso da informação em um ambiente eletrônico. A partir do momento em que a autonomia dos indivíduos é infringida, tem-se a violação de sua própria liberdade. Isto porque, segundo Beate Rössler (*apud* Capurro)[5], "a autonomia de proteção da privacidade é a base da liberdade, e não o contrário". De acordo com a autora, uma vida que não seja determinada pelo próprio indivíduo resulta na infração da sua "privacidade decisional". Para Luciano Floridi (*apud* Capurro)[5], a privacidade da informação está atrelada ao próprio direito à vida e à liberdade e assim se torna um direito fundamental e inalienável.

Exatamente sob esse enfoque, surgiram debates a respeito das formas de enfrentar a problemática da exposição descomedida de dados pessoais, tutelando o direito à privacidade e, ao mesmo tempo, não obstando os benefícios advindos do avanço tecnológico. Diante desse movimento e das novas necessidades postas pelas transformações digitais, despontaram estratégias normativas de proteção da vida privada com a finalidade de assegurar que a fruição das novas vantagens facultadas pela tecnologia possa ocorrer de forma proporcional à manutenção das expectativas de privacidade[6]. Surgem, então, instrumentos de regulação com o propósito de proteger direitos fundamentais como privacidade, intimidade, honra, direito de imagem e dignidade humana[7]. Esses instrumentos se tornaram essenciais e indispensáveis uma vez que proteger juridicamente a privacidade significa garanti-la como direito fundamental baseado no princípio constitucional da dignidade humana, sobretudo quando se está a tratar de questões de saúde. Em uma perspectiva humanística, evitar o vazamento total ou parcial de informações sobre a saúde das pessoas significa neutralizar seu potencial discriminatório[8]. Assim, a criação de normas e leis de proteção de dados possui estrita relação com a necessidade de atualização nacional frente aos impactos sociais, econômicos e políticos oriundos dos avanços tecnológicos. De forma geral, pode-se afirmar que o surgimento de regramentos dessa espécie é resultado da associação entre a expansão dos direitos humanos e a atualização e adaptação de documentos internacionais de proteção aos direitos[9].

Nesse contexto, a Lei 13.709/2018[10], chamada de LGDP, sancionada no dia 14 de agosto de 2018, marca nova fase quanto à proteção de informações no Brasil. Ela é voltada à tutela de uma particular vulnerabilidade do mundo contemporâneo: o compartilhamento de dados. Seus objetivos, em essência, consistem na proteção dos direitos fundamentais de liberdade e de privacidade, no livre desenvolvimento da personalidade da pessoa natural, na promoção da intimidade do cidadão, na garantia dos direitos de personalidade dos indivíduos e no fomento à inovação. Em suma, o legislador visou à regulamentação e à governança em relação ao uso e ao tratamento dos dados pessoais com vistas a preservar alguns dos mais caros direitos fundamentais. Os principais dispositivos da LGPD entrarão em vigor em agosto de 2020 e estabelecem regras sobre coleta, tratamento, armazenamento e compartilhamento de dados pessoais. Seus efeitos são amplos e ainda não perfeitamente dimensionáveis, atingem o campo econômico, social e político. A Lei passa a integrar um conjunto normativo mais amplo no país, formado pela Lei de Acesso à Informação (Lei 12.527/2011[11]), o Marco Civil da Internet (Lei 12.965/2014[12]) e o Código de Defesa do Consumidor (Lei 8.078/1990[13]), formando o arcabouço regulatório brasileiro da informação.

Em breve alusão ao histórico normativo quanto às garantias da vida privada, deve-se mencionar a Declaração Universal dos Direitos do Homem[14], que assegura o direito de todos de terem sua vida privada resguardada sem interferências ou ataques. Além disso, o Pacto Internacional dos Direitos Civis e Políticos, ratificado pelo Brasil mediante o Decreto n. 592, de 06 de julho de 1992[15], também garante o direito à privacidade. No âmbito nacional, o direito à privacidade é espécie do gênero dos direitos da personalidade [regulados pelo art. 21 do Código Civil Brasileiro[16]] e resguardado pela Constituição da República Federativa do Brasil de 1988[17], que garante a manutenção da vida privada como direito fundamental.

Foi apenas na década de 1970 que surgiram as primeiras normas específicas que correlacionaram a proteção de dados pessoais ao efetivo direito à privacidade. Alguns dos principais instrumentos foram: lei *hessen* alemã (1970), lei de dados sueca (1973), estatuto alemão de proteção de dados de *Rheinland-Pfalz* (1974), lei federal de proteção de dados alemã (1977) e lei francesa de proteção de dados pessoais (1978). Nos Estados Unidos foi editado o *Fair Credit Reporting Act* (1970) e o *Privacy Act* (1974). Em 1976, Portugal foi o primeiro país a estabelecer, no artigo 35 de sua Constituição, o direito fundamental à autodeterminação informativa. Posteriormente, a Convenção nº108 do Conselho da Europa (1981) e a Diretiva 95/46 da União Europeia (1995) foram fundamentais para consolidar a tutela dos dados pessoais. No ano 2000, a Carta dos Direitos Fundamentais da União Europeia avançou e definiu, com precisão, que todos têm direito à proteção de dados pessoais que lhes digam respeito, os quais devem ser objeto de um tratamento leal, para fins específicos e com consentimento do interessado, possibilitando-se, inclusive, a respectiva retificação quando e se necessária[18,19]. O Regulamento Geral de Proteção de Dados europeu (RGPD) manteve as exigências feitas pela Diretiva 95/46 quanto à qualidade dos dados, isto é, previu os princípios da necessidade, lealdade, finalidade e proporcionalidade, bem como exatidão e atualidade. Todavia, de característica mais abrangente, a RGPD passou a incluir três novos princípios: a transparência, a minimização dos dados e a responsabilidade[20].

O tratamento autônomo da proteção de dados tem se desenvolvido doutrinaria e juridicamente desde então. Ao longo dos anos, diferentes gerações de normas foram adaptadas de um enfoque mais restrito para um mais geral, com técnicas específicas aplicáveis às tecnologias adotadas para o tratamento de dados. As leis foram se desenvolvendo em decorrência da necessidade dos países em delinear qual o limite entre as informações pessoais que poderiam ser públicas e as que deveriam permanecer confidenciais[2].

No Brasil, apenas no ano de 1999 surgiu a primeira intenção legislativa própria sobre a estrutura e o uso de banco de dados, sob forma do Projeto de Lei n. 268/1999[21], arquivado em 2007. Na sequência, outras iniciativas despontaram com o intuito de tratar da questão do uso e da privacidade de dados, conforme anotado no quadro 01, a seguir. Como se nota no extenso rol, anteriormente à LGPD as intenções legislativas eram fragmentadas e pouco avançaram.

Quadro 01 - iniciativas legislativas nacionais relativas à privacidade de dados – anteriores à LGPD

(continua)

Projeto de Lei[1]	Ano	Ementa	Status
3.360	2000	Dispõe sobre privacidade de dados e a relação entre usuários, provedores e portais em redes eletrônicas.	Arquivado
6.541	2002	Altera o Código Penal para inclusão da criminalização da divulgação de informações sigilosas.	Aprovado
123	2003	Veda a transmissão a terceiros de dados relativos a pessoas naturais e jurídicas.	Arquivado
2.423	2003	Dispõe sobre procedimentos de invasão de computadores.	Arquivado
836	2003	Disciplina o funcionamento de banco de dados e serviços de proteção ao crédito.	Arquivado
87	2004	Dispõe sobre as garantias de privacidade aos usuários de programas de computador.	Arquivado
281	2012	Altera a Lei 8.079/90 para incluir como direito básico a autodeterminação, a privacidade e a segurança das informações e dados pessoais.	Aprovado substitutivo
330	2013	Regula a proteção, o tratamento e o uso dos dados das pessoas naturais ou jurídicas.	Prejudicado em razão da promulgação da LGPD

(conclusão)

Projeto de Lei[1]	Ano	Ementa	Status
5.276	2016	Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.	Prejudicado em razão da promulgação da LGPD

Fonte: elaborado pelas autoras (2020).

A LGPD surge, então, como forma de conjugação de normatização de diferentes segmentos e espaços que envolvem os dados pessoais e que careciam, até então, de regulamentação uníssona. A Lei brasileira é expressão da convergência internacional em torno de princípios básicos de proteção de dados. Sua formulação sofreu influência e inspiração direta da *General Data Protection Regulation*[22], do Regimento Geral de Proteção de Dados Europeu (RGPD) e de princípios de *Fair Information Practice Principles* (FIPPs). Ainda que seja inegável a influência do RGPD sobre a LGPD, há diferenças substanciais entre tais regimes jurídicos, principalmente com relação à técnica legislativa utilizada para talhar ambas as leis. O RGPD é o ponto de chegada de uma longa jornada europeia no campo da proteção de dados pessoais, por essa razão, em termos quantitativos, ele é um corpo normativo mais extenso em comparação à LGPD. Assim, o RGPD seria um código de proteção de dados que conta com uma quantidade maior de dispositivos e com uma espécie de exposição de motivos, ao passo que a LGPD seria uma lei mais enxuta e sem pistas interpretativas deixadas por parte do legislador[20]. Importante mencionar, nesse contexto, que o plenário do Supremo Tribunal Federal em um reconhecimento manifesto do direito fundamental à proteção de dados, suspendeu, recentemente, a eficácia da MP nº 954/2020, que prevê o compartilhamento de dados de usuários de operadoras de telefonia com o IBGE para a produção de estatística oficial durante a pandemia da Covid-19[23]. Trata-se de sinalização importante sobretudo no contexto de sucessivas prorrogações da vacatio legis da LGPD, cujo início da vigência está atualmente marcado para 3 de maio de 2021, por força da Medida Provisória n. 959, de 29 de abril de 2020[24].

Conceitualmente, a LGPD está amparada na ideia central de que as pessoas tenham conhecimento e controle sobre a coleta e o processamento de suas informações, principalmente daquelas que as identificam, possibilitando a limitação desse processo[25]. Sob o aspecto social e jurídico, seu objetivo é a proteção de alguns dos principais direitos fundamentais dos indivíduos: privacidade [intimidade, vida privada, honra e imagem], cidadania e dignidade. A cidadania eletrônica, termo frequentemente utilizado para referir-se ao assunto, diz respeito ao direito à autodeterminação informativa, uma vez que os dados pertencem à pessoa e não às instituições que os coletam[26,27].

É possível identificar cinco eixos principais da LGPD em torno dos quais a proteção do indivíduo, titular de dados, se articula: i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados [hipóteses autorizativas]; iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento; v) responsabilização dos agentes[28].

Acerca da abrangência, a LGPD aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica, de direito público ou privado, independentemente do meio, desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento se refira a dados de indivíduos localizados no território nacional; os dados pessoais objetos do tratamento tenham sido coletados no território nacional. Consideram-se coletados no território nacional os dados cujo titular nele se encontre no momento da coleta[29].

A LGPD divide os dados em dois grandes grupos: dado pessoal e pessoal sensível. Pessoal seria aquele em que o objeto da informação é a própria pessoa. Sensível seria o dado pessoal sobre origem racial ou

étnica; convicção religiosa; opinião política; filiação a sindicato ou a organização de caráter religioso, filosófico ou político; referente à saúde ou à vida sexual; genético ou biométrico (art. 5º, II). Os dados de saúde, portanto, se encontram nessa última categoria. Se revelados, possuem potencial de discriminar e lesar o indivíduo e a própria sociedade[26,27].

Em virtude de ser essencialmente principiológica, a LGPD carece de limites e contornos para sua aplicação, daí a fundamental importância de órgãos autônomos e independentes para a implementação efetiva da lei, alguns a serem implementados pela Autoridade Nacional de Dados (ANPD) e pelo Conselho Nacional de Proteção de Dados, definidos no corpo da Lei. Seu alcance, entretanto, parece certo às instituições que tratam de dados em saúde, entre elas, o sistema público de saúde brasileiro. Assim, pois, o Sistema Único de Saúde (SUS) coleta, classifica, armazena, acessa, utiliza, processa, avalia, arquiva e tramita diversos tipos de informações referentes à higidez e/ou adoecimento de seus usuários, à vida sexual, aos aspectos genéticos e biométricos. Inconteste o impacto que o SUS sofrerá a partir da efetiva aplicação da LGPD. Inelutável sua necessidade de adequação às regras estabelecidas. Mencione-se, a título de exemplo, as informações sensíveis contidas nos prontuários médicos: patologias, resultados de exames e procedimentos, questões sexuais e genéticas, além de eventuais informações sobre familiares/terceiros. Isso para cada um dos três entes federados. Serão atingidos pela LGDP praticamente todos os serviços e intuições integrantes do SUS: unidades básicas de saúde, pronto atendimentos e pronto socorros, hospitais, clínicas, serviços diagnósticos [exames de imagem, laboratórios], serviços de reabilitação, serviços de pesquisa e órgãos gestores [secretarias de saúde]. Além dos prestadores contratados da iniciativa privada. Oportuno ressaltar que o sistema público de saúde brasileiro e, por conseguinte, sua estrutura de tecnologia da informação e comunicação apresentam dimensões continentais. Ante esse cenário, algumas reflexões inerentes ao encadeamento SUS – LGPD merecem ser ponderadas.

PROTEÇÃO DE DADOS NO SISTEMA ÚNICO DE SAÚDE

O uso de tecnologias de informação e comunicação (TIC) para mediar a atenção à saúde é denominado e-Saúde (*e-Health*). A terminologia, adotada pela Organização Mundial da Saúde (OMS), inclui assistência ao paciente, pesquisa, educação/capacitação da força de trabalho e monitoração e avaliação em saúde. De modo exemplificativo, processos de e-Saúde no Brasil incluem o Cartão Nacional de Saúde do SUS, teleconsultorias, telediagnóstico, telecirurgia, telemonitoramento, televigilância, educação permanente, teleducação e prontuário eletrônico[30].

Se o mote geral do discurso relacionado à proteção de dados reserva atenção especial à privacidade e à intimidade do indivíduo, quando a discussão volta-se ao universo dos dados em saúde, mormente dos sistemas sanitários, a análise extrapola, em muito, a mera tutela individual de direitos. Um dos aspectos a ser debatido nesses casos é a dicotomia entre a legítima busca de proteção das informações sensíveis e as necessidades e dificuldades práticas de gestão, contradição aparentemente inalienável. Se do ponto vista teórico esse limite parece bastante claro à vista do contido na Lei 13.709/2018, sob a ótica da *práxis* das rotinas dos serviços de saúde, a tarefa vislumbra-se mais complexa. A evolução rápida das TIC, especialmente com o uso intensivo da internet, ilimitado no tempo e no espaço, levou ao crescimento do volume e da variedade de informações que podem ser combinadas, aumentando o risco de vazamentos e re-identificação, mesmo após a anonimização ou a desidentificação de bases de dados de saúde.

No caso do SUS, esse panorama toma proporções gigantescas, bem como é a sua dimensão. Vale ponderar que as normas gerais contidas na LGPD são de interesse nacional, devem ser observadas pelos Órgãos Gestores em Saúde da União, dos Estados, do Distrito Federal e dos Municípios. Registre-se que os

milhares de estabelecimentos de saúde do SUS estão distribuídos entre os 26 Estados e os 5.570 Municípios[i] da nação, muitos dos quais não utilizam, ainda, sequer sistemas informatizados.

Historicamente, a experiência de tratamento de dados em saúde no Brasil tem sido acompanhada da implementação de múltiplos sistemas de informação, voltados para diferentes fins: epidemiológico, demográfico e de produção de serviços. Podemos citar como exemplos aqueles vinculados ao DATASUS, o Departamento de Informática do SUS: Sistema de Informação sobre Nascidos Vivos (Sinasc), Sistema de Informações sobre Agravos de Notificação (Sinan), Sistema de Informações Hospitalares (SIH), Sistema de Informação de Mortalidade (SIM), Sistema de Informação de Atenção Básica (SIAB), Sistema de Cadastramento de Usuários (CADSUS), Cadastro Nacional de Estabelecimentos de Saúde (CNES), Sistema de Informações do Programa Nacional de Imunizações (SI-PNI), Sistema de Informação do Câncer do Colo do Útero e Sistema de Informação do Câncer e Mama (SISCOLO e SISMAMA), Sistema de Cadastramento e Acompanhamento de Hipertensos e Diabéticos (HIPERDIA), Sistema de Acompanhamento da Gestante (SISPRENATAL), Sistema de Informações Ambulatoriais do SUS (SIA), Sistema para captura de dados do SAMU (e-SUS-SAMU), Relação de Doadores Não Aparentados de Medula Óssea (REDOMENet), Sistema de gerenciamento da lista de transplantes no Brasil (SNT – Órgãos), Sistema do Programa Nacional de Avaliação de Serviços de Saúde (SIPNASS), Central Nacional de Regulação de Alta Complexidade (CNRAC), Sistema de Centrais de Regulação (SISREG), Sistema do Programa Volta para Casa (PVC), Sistema do Bolsa Família, Sistema de Informações sobre Orçamento Público em Saúde (SIOPS), Sistema de Gestão de Informações Financeiras do SUS (SGIF), Sistema de Gerenciamento Financeiro (SISGERF), Sistema de Apoio à Construção do Relatório de Gestão (SARGSUS), Sistema de Gestão de Projetos do DATASUS (Redmine), Sistema de gestão hospitalar (e-SUS Hospitalar), Sistema de Gerenciamento em Serviços de Hemoterapia (HEMOVIDA), Sistema de Informações Hospitalares Descentralizado (SIHD), Sistema de Gerenciamento e Produção de Bancos de Leite Humano (BLHWeb), Sistema de Comunicação de Informação Hospitalar e Ambulatorial (CIHA), Sistema de Controle de Envio de Lotes (SISNET)[ii]. Isso para citar apenas alguns exemplos de abrangência nacional. Há ainda outros que podem ser desenvolvidos e implantados localmente por Estados e Municípios.

Ante essa infinidade de sistemas compostos por centenas de variáveis, as noções mescladas de interesse público, necessidades coletivas, privacidade, inviolabilidade da intimidade, dignidade da pessoa humana, autodeterminação informativa, livre desenvolvimento de personalidade, desenvolvimento tecnológico, direitos humanos, sigilo de dados, proteção do consumidor, saúde pública, vigilância e cidadania podem se embaraçar e tornar difícil o juízo valorativo. No austero cotidiano do sistema público de saúde brasileiro, a LGPD, provavelmente, terá de ser guiada pela proporcionalidade e razoabilidade, não se estabelecendo prevalência teórica e antecipada de uns direitos fundamentais sobre outros, especialmente em razão da profunda sobreposição entre interesses da coletividade e individuais[31].

Os dados pessoais na saúde cumprem, sem dúvida, outra função que vai além da proteção da privacidade. O interesse coletivo é intrínseco à compreensão de bem comum e determina os valores e parâmetros que devem orientar o uso e a disponibilização das informações enquanto bem jurídico tutelado, de forma a garantir, preponderantemente, a satisfação de necessidades grupais. Essa dinâmica de ressignificação do direito à privacidade e à informação na saúde requer uma regulamentação e governança que articule virtuosamente proteção da privacidade e promoção do acesso à informação em compasso com as necessidades comuns e as possibilidades tecnológicas disponíveis[32]. A dificuldade parece estar, justamente, em alcançar um espaço de equilíbrio entre esses universos. Um dos recentes cases brasileiros, exemplo da fragilidade ocasionada pela então ausência de regulamentação, é o episódio de vazamento de dados do

i Dados IBGE: https://www.ibge.gov.br/cidades-e-estados.

ii Relação disponível no sítio eletrônico do DATASUS: http://datasus.saude.gov.br/wp-content/uploads/2019/08/Catalogo-de-Produtos-DATASUS.pdf..

Cartão Nacional de Saúde do SUS, ocorrido em 2017. O escândalo envolveu a divulgação na rede mundial de computadores de nome e endereço completo, número do Cadastro de Pessoa Física (CPF) e nome dos genitores de milhares de usuários.

Apresentados esses aspectos mais gerais, nos próximos tópicos passamos a abordar de forma individuada os pontos que podem ser considerados mais críticos na relação entre a LGPD e o SUS, a saber: tratamento de dados pessoais sensíveis (art. 11º-13º), consentimento (art. 7º, II), anonimização de dados sensíveis (art. 11º, II, c), hipóteses de compartilhamento, segurança e sigilo dos dados (art. 46º-49º) e boas práticas e governança (art. 50º-51º).

Tratamento de dados sensíveis e consentimento

No que se refere aos requisitos para tratamento de dados sensíveis, a LGPD traz as seguintes exigências: consentimento do titular ou a) obrigação legal, b) necessidade para formulação de políticas públicas, c) realização de estudos por órgão de pesquisa, d) exercício regular de direitos 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 [processos de identificação e autenticação de cadastro em sistemas eletrônicos]. Assim, a estrutura da norma privilegia, em primeiro lugar, a participação ativa do titular do dado sensível por meio do consentimento. As demais hipóteses previstas, a depender da interpretação do que se enquadra em uma ou outra categoria, podem ser mais ou menos extensivas. Além disso, um exercício de bom senso e ponderação entre o custo [econômico, social] dispendido para se obter o consentimento e o benefício real que o tratamento de dados trará, seja para o titular, controlador ou coletividade, deve ser imperioso.

Dessa forma, as hipóteses para tratamento de dados sensíveis, mesmo que restringidas pela norma, permanecem relativamente amplas. Especialmente nos casos da necessidade de execução de políticas públicas[10] e da tutela da saúde por profissionais ou serviços de saúde[10] as possibilidades de enquadramento parecem vastas. Afinal, muitas ações podem se configurar como justificativas para fins de planejamento e formulação de políticas em saúde ou para a tutela da saúde. Quem definirá os limites dessas prerrogativas e quais profissionais disporão dessa imunidade?

Particularmente com relação ao consentimento, a LGPD define que ele deve ser livre, informado e com finalidade determinada (art. 5º, XII). O termo livre alude a um ato do titular independente de coação física, moral, mental ou artifício que o induza. O fato de ser informado exige que o titular seja comunicado acerca do uso e compartilhamento de seus dados de forma clara e de fácil entendimento. Já a finalidade determinada refere-se à necessidade de demonstração clara e específica sobre quais serão as utilidades do tratamento das informações, sendo vedadas autorizações genéricas e usos que escapem ao contexto final[33]. Em diversos países da União Europeia tem sido preconizado também o 'consentimento ativo', que seria a vedação da obtenção do consentimento de forma implícita, pela mera inação do titular dos dados em não se opor ao tratamento, sem engajamento direto do titular, por assim dizer[34].

Atualmente, cada serviço vinculado ao SUS possui autonomia para desenvolver seu próprio modelo de consentimento e assentimento informado para a realização de consultas, exames e procedimentos. Na maioria dos casos, não há itens específicos sobre a coleta e o tratamento dos dados em si. Não há padronização nem exigência de requisitos mínimos a serem contemplados. Alguns são utilizados em meio físico, outros em digital. Variam de acordo não apenas com a instituição, mas também conforme sua aplicabilidade. Há, por exemplo, termos diferentes para internação hospitalar, realização de procedimento cirúrgico e hemodinâmico, anestesiologia, parto e intervenções obstétricas, amputações, exames videolaparoscópicos, solicitação de cópia de prontuários e documentos, recusa de tratamento medicamentoso e/ou invasivo, abandono de tratamento e alta à revelia.

Uma das principais dificuldades de adequação do SUS à LGPD, provavelmente, dirá respeito a essa variabilidade de modelos e vias de coleta não padronizadas e não normalizadas. Para além disso, há milhares de bytes já coletados e armazenados nos equipamentos do SUS para os quais não foi solicitado consentimento. A depender de eventual necessidade de utilização, o consentimento e/ou a anonimização serão mandatórios. Enfim, no universo complexo e grandioso do sistema público de saúde brasileiro, ainda não se sabe como a Autoridade Nacional de Proteção de Dados (ANPD) e seus prepostos tratarão dessas questões a fim de desempenhar as tarefas de zelar pela proteção dos dados pessoais e fiscalizá-los, bem como disposto no art. 55-J, I e IV, da LGPD.

Anonimização de dados sensíveis e hipóteses de compartilhamento

De acordo com o art. 5º, XI, da Lei 13.709/2018, a anonimização consiste na utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. O art. 12º da norma esclarece que os dados anonimizados não serão considerados pessoais para os fins da Lei, salvo quando o processo de anonimização for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis [custo e tempo necessários], puder ser revertido. Isto é, dados anonimizados são aqueles que não permitem identificar o titular a quem originalmente se referem ainda que se utilizem meios técnicos razoáveis e disponíveis para tanto.

Conforme mencionado, há no SUS uma infinidade de dados ainda não anonimizados, tampouco pseudonimizados (art. 13, § 4º) que transitam via sistemas digitais e meio físico entre instituições de todas as instâncias federativas. Isso se torna problemático principalmente em municípios ou grupos populacionais pequenos, em que, pelo número restrito de titulares, os riscos de identificação dos indivíduos são mais importantes.

A questão da confidencialidade e do sigilo dos dados é um dos princípios basilares da ética em saúde. Um exemplo recente da dificuldade técnica de abordagem dessa questão consiste na revogação da Resolução CFM nº 2.227, de 6 fevereiro de 2019[35], vinte dias após sua publicação, por via da Resolução 2.228, de 26 de fevereiro de 2019. A Resolução 2.227/2019 foi duramente criticada pela comunidade científica em razão da insegurança jurídica gerada por conta da insuficiência de regras claras para a instituição da telemedicina nos serviços e do débil controle dos dados envolvidos.

Outro ponto crítico que se vislumbra na relação SUS-LGPD é a questão do livre compartilhamento de informações entre instituições [de igual ou distinta esfera federativa]. Não há, até o momento, uma clara regulamentação acerca do intercâmbio de informações entre instituições componentes ou correlatas ao SUS. Assim, por exemplo, nos casos de pedidos de informação advindos do Judiciário, Defensorias Públicas e Ministérios Públicos, habitualmente procurados por pacientes do SUS que não têm seu direito à saúde assegurado, questiona-se: Secretarias Municipais e Estaduais de Saúde devem fornecer dados sensíveis do usuário baseadas no exercício regular de direitos em processo administrativo (art. 7º, VI) ou na tutela da saúde (art. 7º, VIII), ainda que não haja consentimento formal do titular do dado? E entre as próprias instâncias do Executivo [Secretarias Municipais, Estaduais e Ministério da Saúde], dados sensíveis não anonimizados poderão trafegar, baseados nas mesmas prerrogativas?

Atualmente [2020], por vezes, esse fluxo é obstado por gestores ou profissionais que se veem inseguros diante de vazios regulamentares, da omissão legal e da ausência de normatização e padronização. Algumas dúvidas ainda carecem de aclaramento: todos os pedidos de informações que envolvam dados em saúde deverão passar, obrigatoriamente, pelo controlador dos sistemas? Esse controlador será centralizado em esfera federal ou haverá controladores de Estados e Municípios? De todo modo, um dos possíveis impactos indesejáveis e negativos do estabelecimento de fluxogramas formais seria o potencial agravamento da

morosidade nas ações e processos dos serviços públicos de saúde que dependam dessa circulação de informações.

A temática na anonimização de dados trazida pela LGPD possui alcance e dimensão ainda não perfeitamente mensuráveis. Algumas situações imprevistas mesmo após a implementação das adequações para o atendimento da Lei certamente surgirão no cotidiano dos serviços. O tratamento e a elaboração de tais casos demandará análises e estudos que considerem não apenas o caso em particular, mas também o situem no contexto geral do regramento em informação de dados que vigora no país. Um exemplo fático pode ser visualizado no contido na Lei nº 17.066, de 11 de janeiro de 2017[36], do Estado de Santa Catarina, e nos Projetos de Lei nº 140/2017[37] e nº 192/2018[38], em trâmite no Senado Federal. Esses dispositivos tratam da publicidade das filas de espera para consultas e procedimentos do SUS. De acordo com o art. 4º, III, da Lei nº 17.066/2017, as listas de espera devem conter o nome completo dos inscritos habilitados para a respectiva consulta, exame, intervenção cirúrgica ou procedimento. Em alguns casos, a Lei menciona que a identificação será realizada por meio do número do Cartão Nacional de Saúde (CNS) ou do Cadastro de Pessoas Físicas (CPF). Certamente, essa aparente incompatibilidade entre a lei estadual catarinense de publicização das filas do SUS e a LGPD merece ser debatida. Enfim, o que se está a dizer é que exatamente esses casos de inconciliabilidade ou contraposição entre situações que envolvem a gestão prática do sistema público de saúde e as regras da LGPD deverão ser paulatinamente problematizados e apreciados.

Segurança dos Dados e Boas Práticas de Governança

Com relação à segurança dos dados, a principal limitação a ser enfrentada pelo sistema público de saúde brasileiro no atendimento à LGPD diz respeito à: a) ausência de uma política nacional única de segurança de dados de saúde; b) limitação de recursos orçamentários [desfinanciamento do SUS] para a adaptação de todos os sistemas informatizados mencionados às regras da LGPD. Como se tratam de sistemas com diferentes finalidades, atributos técnicos e riscos, torna-se ainda mais dispendiosa a tarefa.

Assim, o sistema público de saúde, acostumado a tratar milhares de bytes cotidianamente, terá de definir medidas de segurança que garantam o sigilo e o 'bom uso' dos dados coletados e armazenados em suas bases de Municípios, Estados e União; algo que até então só vem sendo feito, efetivamente, na interface entre SUS e a pesquisa. Tradicionalmente, os Comitês de Ética em Pesquisa (CEP) vinculados a instituições de ensino superior e a hospitais têm se constituído no único 'filtro' formalmente organizado relativo à manipulação de informações pessoais de saúde no país. As diretrizes éticas nacionais para pesquisas envolvendo seres humanos utilizadas pelos CEPs estão definidas na Resolução MS/CNS nº 466/2012[39]. Ocorre que sua limitação deflui justamente de se tratar de normativa vinculada apenas à pesquisa, não diz respeito a outras ações e serviços disponibilizados pelo SUS e por seus prestadores privados.

Oportuno consignar que o Plano Diretor de Tecnologia da Informação 2019/2021 do DATASUS cita a necessidade de implantar a LGPD no Ministério da Saúde por meio da preparação para compliance. Entretanto, não apresenta o modo como a operação será materializada. A meta de execução é de cumprimento de 75% das atividades programadas até 2021[40].

Ante o exposto, evidente a necessidade de ágil ação por parte de gestores do SUS de modo a adequar-se, tão brevemente quanto possível, às exigências técnicas, organizacionais e legais que defluem da LGPD. A revisão da estrutura existente e a readequação aos novos moldes é caminho inevitável e, ao mesmo tempo, desafiador.

EVENTUAIS CAMINHOS PARA A HARMONIZAÇÃO DO SUS À LGPD

Diante do desafio que o SUS está prestes a enfrentar a fim de compatibilizar sua estrutura de tecnologia em informação às novas exigências da LGPD, a sensação que se tem é a de que, de fato, há muito a ser feito. Considerando-se sobretudo o cenário de desfinanciamento do sistema público de saúde e a clara insuficiência dos recursos a ele destinados[41], as adversidades para o cumprimento da tarefa apresentam-se ainda mais onerosas.

Em um primeiro momento, os esforços provavelmente se concentrarão no exercício de compreensão sobre as normas trazidas pela LGPD, seus impactos e alcance sobre a estrutura da tecnologia da informação do SUS, a revisão do modelo de governança até então adotado e o levantamento das instituições [integrantes e contratualizadas] que serão afetadas.

Em um segundo passo, se faz necessária a avaliação sobre: i) o estágio de maturidade em que se encontra a atual estrutura de informação do SUS, ii) os fluxos de dados existentes, iii) os setores do SUS que serão mais fortemente impactados, iv) o alcance das medidas a serem planejadas [nacional, estadual, municipal], v) os responsáveis pela definição e implantação do plano estratégico a ser desenvolvido, vi) as metodologias processuais, físicas, tecnológicas e humanas fundamentais para a aderência aos requisitos da LGPD.

Na sequência, importante a definição: i) do plano a ser seguido para a efetiva proteção dos dados e para o atingimento dos requisitos da LGPD, ii) das políticas e diretrizes internas, iii) da organização do ambiente tecnológico e do modelo de governança a ser empregado, iv) das soluções propostas, v) da gestão de terceiros [prestadores contratados pelo SUS], vi) do monitoramento e tratamento de incidentes, vii) da dotação orçamentária e de recursos humanos.

Por fim, tende a ocorrer a implementação dos componentes do modelo de governança de proteção de dados delineado nas fases anteriores, com finalidade de alinhar adequadamente as camadas do sistema e a tecnologia da informação para garantir, ao fim e ao cabo, desempenho, capacidade, maior eficiência do sistema público de saúde e garantia aos direitos fundamentais de privacidade e dignidade humana.

A partir dos desafios e fragilidades elencados no desenvolvimento do presente artigo, as autoras propõem sugestões e caminhos concretos, consubstanciados no quadro 02, para que os gestores do SUS possam pensar o sistema a partir do impacto da LGPD.

Quadro 02 - Síntese das sugestões para harmonização do SUS à LGPD

(continua)

Desafio identificado na pesquisa	Eixo temático	Sugestão de encaminhamento para solução
Pulverização legislativa pré LGPD.	Organização, padronização, planejamento e governança.	Apensação, para tramitação conjunta, de proposições que tratem de tema afeto à LGPD.
Ausência de informação, no Plano Diretor de Tecnologia da Informação 2019/2021 do DATASUS, sobre o planejamento para a implantação da LGPD no âmbito do Ministério da Saúde.	Organização, padronização, planejamento e governança.	Divulgação detalhada, no Plano Diretor de Tecnologia da Informação do DATASUS, do plano de ação definido para a implantação da LGPD no Ministério da Saúde, nas Secretarias de Estados da Saúde e nas Secretarias Municipais de Saúde.
Ausência de padronização quanto aos modelos de consentimento e assentimento informado no SUS e generalizada ausência de itens específicos sobre o consentimento para a coleta, o tratamento e o eventual compartilhamento dos dados.	Organização, padronização, planejamento e governança.	Padronização mínima quanto aos parâmetros essenciais a constarem nos termos de consentimento livre e esclarecido, inclusive no que se refere à coleta, ao tratamento e ao eventual compartilhamento dos dados dos pacientes.

(conclusão)

Desafio identificado na pesquisa	Eixo temático	Sugestão de encaminhamento para solução
Diversidade de sistemas e plataformas de informação do SUS [epidemiológicos, demográficos e de produção de serviços].	Organização, padronização, planejamento e governança.	Unificação, na medida do razoável, de plataformas/sistemas eletrônicos do SUS assemelhados ou de temáticas afins.
Ausência de regulamentação mínima quanto ao fluxo de informações entre órgãos integrantes do SUS [nível nacional, estadual e municipal] e entre o SUS e órgãos externos.	Compartilhamento	Regulamentação mínima acerca dos critérios e limites dos fluxos de informação [compartilhamento de dados] entre instâncias do SUS e entre o SUS e órgão externos [Judiciário, Defensoria Pública, Ministério Público, entre outros].
Escassez de debate acadêmico, teórico e prático acerca da necessidade de adaptação do SUS aos dispositivos da LGPD.	Debate	Criação de Comitê/Comissão com representantes técnicos e políticos da União, Estados e Municípios, para acompanhamento do debate e planejamento das ações de amoldamento do SUS à LGPD, especialmente por meio da aproximação institucional com o Conselho Nacional de Proteção de Dados Pessoais e Privacidade.
Ausência de divulgação das ações já realizadas e das deliberações do Conselho Nacional de Proteção de Dados Pessoais e Privacidade.	Publicidade	Divulgação das ações e deliberações desenvolvidas pelo Conselho Nacional de Proteção de Dados Pessoais e Privacidade em tempo hábil para adaptação do SUS ao atendimento das exigências, por meio, por exemplo, de notas técnicas ou informes periódicos.
Ausência de divulgação/publicização acerca das características quanti e qualitativas dos dados pessoais dos usuários armazenados pelos órgãos gestores em saúde [Ministério da Saúde, Secretarias de Estado da Saúde e Secretarias Municipais de Saúde].	Publicidade	Publicização, em quantidade e qualidade, das características [tipo, quantidade, cronologia] dos dados sensíveis dos pacientes armazenados pelo Ministério da Saúde, pelas Secretarias de Estado da Saúde e pelas Secretarias Municipais de Saúde.
Ausência de divulgação/publicização acerca dos mecanismos e estratégias adotadas pelos órgãos gestores em saúde [Ministério da Saúde, Secretarias de Estado da Saúde e Secretarias Municipais de Saúde] para a proteção dos dados dos usuários do SUS.	Publicidade	Publicização referente à política de proteção de dados elaborada por instituições de saúde públicas e privadas, com detalhamento das ferramentas e estratégias adotadas, bem como sobre o grau de segurança garantido.
Ausência de financiamento adequado do sistema público de saúde, condizente com a robustez de sua estrutura.	Financiamento	Financiamento e dotação orçamentária compatíveis com a reestruturação do sistema de tecnologia e de informação do SUS para o atendimento dos pressupostos da LGPD.

Fonte: elaborado pelas autoras (2020).

Enfim, os caminhos que o SUS terá de trilhar para atender às exigências estabelecidas na LGPD são complexos e demandarão esforços conjuntos de gestores, técnicos e sociedade civil. Essa última terá em mãos um instrumento legítimo e valioso para exigir que seus dados pessoais e sensíveis sejam resguardados dentro de um mínimo ético e legal, sob pena de os infratores responderem a sanções duríssimas, que podem

atingir multas de R$ 50.000.000,00 (art. 52, II, da Lei), além de penalidades administrativas, civis e penais e eventuais demandas judiciais individuais e/ou coletivas por parte da sociedade civil, o que obrigaria, por uma via mais dura e custosa, a adaptação do sistema à lei.

CONSIDERAÇÕES FINAIS

As transformações comunicacionais ocorridas nas últimas décadas expuseram fragilidades tecnológicas até então latentes quanto à preservação de direitos fundamentais absolutamente caros ao Estado Democrático de Direito. Privacidade individual, intimidade, honra, direito de imagem e dignidade humana auferiram destaque e *status* de verdadeiros direitos pétreos frente às ameaças cibernéticas. Nesse cenário, surgiram iniciativas com o objetivo de desenvolver estratégias e instrumentos para enfrentar a problemática da exposição descomedida de dados [pessoais, especialmente], tutelando o direito à privacidade e, ao mesmo tempo, não obstando os benefícios advindos do avanço tecnológico. Como resultado, despontaram normativas de proteção da vida privada e dos dados pessoais gerais e sensíveis.

No Brasil, isso se traduziu na recente promulgação da Lei 13.709/2018[10], denominada de LGDP, sancionada no dia 14 de agosto de 2018, a qual marca nova fase quanto à proteção das informações pessoais dos indivíduos. Diante do contido na norma, inúmeras instituições do país deverão adotar medidas para adequar-se às novas regras. O objetivo do presente manuscrito foi o de apontar em que medida a estrutura do sistema público de saúde brasileiro será impactada pela publicação da LGPD e indicar eventuais caminhos a serem trilhados nesse sentido. Para atingir esse propósito a pesquisa empregou uma abordagem qualitativa, descritiva e exploratória, com utilização do método indutivo, por meio da revisão bibliográfica de artigos e ordenamento jurídico.

Como resultados, foram apresentados: o histórico do arcabouço jurídico brasileiro quanto à proteção de dados, os principais pontos abordados pela LGPD, os sistemas de informação do SUS e os espaços primordiais de conexão entre as determinações da LGPD e o sistema público de saúde brasileiro: consentimento, anonimização e governança.

Ao final, concluímos pela evidente necessidade de ágil ação por parte de gestores do SUS de modo a adequar-se, tão brevemente quanto possível, às exigências técnicas, organizacionais e legais que defluam da LGPD. Indicamos, de maneira preambular, possíveis caminhos a serem trilhados no sentido de superar os desafios, organizados em cinco eixos temáticos: i) organização, padronização, planejamento e governança; ii) compartilhamento; iii) debate; iv) publicidade; e v) financiamento. As principais sugestões formuladas dizem respeito a: a) apensação legislativa de propostas tangenciais à proteção de dados pessoais; b) divulgação detalhada, no Plano Diretor de Tecnologia da Informação do DATASUS, do plano de ação a ser adotado para a implantação da LGPD no Ministério da Saúde, nas Secretarias de Estados da Saúde e nas Secretarias Municipais de Saúde; c) padronização mínima quanto aos parâmetros essenciais a constarem nos termos de consentimento utilizados no SUS, no sentido de conterem informação sobre a coleta, o tratamento e o eventual compartilhamento dos dados dos pacientes; d) unificação de plataformas e sistemas eletrônicos do SUS; e) regulamentação mínima acerca dos critérios e limites dos fluxos de informação [compartilhamento de dados] entre instâncias do SUS e entre o SUS e órgão externos; f) criação de um comitê interinstitucional de saúde para acompanhamento da implantação do Conselho Nacional de Proteção de Dados Pessoais e Privacidade; g) divulgação das ações e deliberações do referido Conselho em tempo hábil para a adaptação do SUS e o atendimento das exigências; h) publicização, em quantidade e qualidade, das características [tipo, quantidade, cronologia] dos dados sensíveis dos pacientes armazenados pelo Ministério da Saúde, pelas Secretarias de Estado da Saúde e pelas Secretarias Municipais de Saúde; i) publicização da política de proteção de dados elaborada por instituições de saúde públicas e privadas; e j) financiamento compatível com a reestruturação do sistema de tecnologia do SUS. Enfim, a revisão, a readequação e a adaptação do

SUS à LGPD e aos novos paradigmas em segurança da informação parecem caminhos inevitáveis e, ao mesmo tempo, desafiadores.

REFERÊNCIAS

1. Rocha ESB, Nagliate P, Furlan CEB; Rocha Jr K, Trevizan MA; Mendes IAC. Gestão do conhecimento na saúde: revisão sistemática de literatura. Rev Latinoam Enfermagem [Internet]. 2012 [citado em 2019 jun. 7];20(2):09 telas. Disponível em: http://www.scielo.br/pdf/rlae/v20n2/pt_24.pdf.

2. Carvalho ARS. Os dados no contexto da quarta revolução industrial. Proteção de dados pessoais: privacidade versus avanço tecnológico. Cadernos Adenauer [Internet]. 2019 [citado em 2019 jun. 7];3:93-112. Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573.

3. Ramos LCP, Gomes AVM. Lei geral de dados pessoais e seus reflexos nas relações de trabalho. Scientia Iuris [Internet]. 2019 [citado em 2019 jun. 7];23(2):127-46. Disponível em: http://www.uel.br/revistas/uel/index.php/iuris/article/view/35794. doi: http://dx.doi.org/10.5433/2178-8189.2019v23n2p127.

4. Fugazza GQ, Saldanha GS. Privacidade, ética e informação: uma reflexão filosófica sobre os dilemas no contexto das redes sociais. Encontros Bibli [Internet]. 2017 [citado em 2019 jun. 7];22:91. Disponível em: https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2017v22n50p91. doi: https://doi.org/10.5007/1518-2924.2017v22n50p91.

5. Capurro R, Eldred M, Nagel D. It and privacy from an ethical perspective digital whoness: identity, privacy and freedom in the cyberworld. In: Buchmann J, editor. Internet Privacy: a multidisciplinary analysis. München: Acatech; 2012.

6. Doneda D. Considerações sobre a tutela da privacidade e a proteção de dados pessoais no ordenamento brasileiro. In: Conrado M; Pinheiro RF, coordenadores. Direito privado e Constituição: ensaios para uma recomposição valorativa da pessoa e do patrimônio. Curitiba: Juruá; 2009. p. 87.

7. Pinheiro PP. Nova lei brasileira de proteção de dados pessoais e o impacto nas instituições públicas e privadas. Thomson Reuters – Revistas dos Tribunais [Internet]. 2019 [citado em 2019 jun. 7];1000:309-23.

8. Sarlet IW, Keinert, TMM. O direito fundamental à privacidade e as informações em saúde: alguns desafios. In: Keinert TMM, Sarti FM, Cortizo CT, Paula SHB, organizadores. Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde; 2015. p. 113-45.

9. Pinheiro PP. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação; 2018.

10. Brasil. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 [Internet]. 2018 [citado em 2019 jun. 7]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

11. Brasil. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal [...]. [Internet]. 2011 [citado em 2019 jun. 7]. Disponível em: https://legislacao.presidencia.gov.br/ficha/?/legisla/legislacao.nsf/Viw_Identificacao/lei%2012.527-2011&OpenDocument.

12. Brasil. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. [Internet]. 2014 [citado em 2019 jun. 7]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

13. Brasil. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. [Internet]. 1990 [citado em 2019 jun. 7]. Disponível em: https://legislacao.presidencia.gov.br/ficha/?/legisla/legislacao.nsf/Viw_Identificacao/lei%208.078-1990&OpenDocument.

14. ONU. Declaração Universal dos Direitos Humanos. [Internet]. 1948 [citado em 2019 jun. 7]. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos.

15. Brasil. Decreto n. 592, de 6 de julho de 1992. Promulga o Pacto Internacional sobre Direitos Civis e Políticos. [Internet]. 1992 [citado em 2019 jun. 7]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm.

16. Brasil. Lei n. 10.406, de 10 de janeiro de 2002. Institui o Código Civil. [Internet]. 2002 [citado em 2019 jun. 7]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm.

17. Brasil. Constituição da República Federativa do Brasil. [Internet]. 1988 [citado em 2019 jun. 7]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

18. Crespo DL, Filho DR. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da lei geral de proteção de dados pessoais. Revista de Direito Privado [Internet]. 2019 [citado em 2019 jun. 7];20(98):161-86.

19. União Europeia. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo: Serviço das Publicações da União Europeia. [Internet]. 2014 [citado em 2019 jun. 7]. Disponível em: https://rm.coe.int/16806ae65f.

20. Mendes LS, Bioni BR. O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira: mapeando convergências na direção de um nível de equivalência. Revista de Direito do Consumidor [Internet]. 2019 [citado em 2019 jun. 7];124:157-80. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1173.

21. Brasil. Projeto de Lei n. 268, de 27 de abril de 1999. Dispõe sobre a estruturação e o uso de bancos de dados sobre a pessoa e disciplina o rito processual do habeas data. [Internet]. 1999 [citado em 2019 jun. 7]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/40242.

22. União Europeia. Regulamento nº 2016/679 do Parlamento Europeu e do Conselho. Revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia [Internet]. 2016 [citado em 2019 jun. 7]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT.

23. Tepedino G. O reconhecimento pelo STF do direito fundamental à proteção de dados. Revista Brasileira de Direito Civil – RBDCivilm [Internet]. 2020 [citado em 2020 jun. 28];24:11-3. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/587. DOI: 10.33242/rbdc.2020.02.001.

24. Brasil. Medida Provisória n. 959, de 29 de abril de 2020. Prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD [Internet]. 2020 [citado em 2020 jun. 7]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm.

25. Blum RO, Schuch S. Compartilhamento e comercialização de dados pessoais em ambiente on-line. Contraponto jurídico. São Paulo: Editora RT; 2019.

26. Doneda D. Da privacidade à proteção dos dados pessoais. Rio de Janeiro: Renovar; 2006.

27. Rodotá S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar; 2008.

28. Mendes LS, Doneda D. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor [Internet]. 2018 [citado em 2019 jun. 7];120:469-83. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116.

29. Klee AEL, Pereira Neto AN. A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. Cadernos Adenauer [Internet]. 2019 [citado em 2020 jun. 7];3:11-33. Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573.

30. Kameda K. E-saúde e desafios à proteção da privacidade no Brasil. Politics [Internet]. 2013 [citado em 2019 jun. 7]. Disponível em: https://politics.org.br/edicoes/e-sa%C3%BAde-e-desafios-%C3%A0-prote%C3%A7%C3%A3o-da-privacidade-no-brasil.

31. Binenbojm G. Da supremacia do interesse público ao dever de proporcionalidade: um novo paradigma para o direito administrativo. Revista de Direito Administrativo [Internet]. 2005 [citado em 2019 jun. 7];239:1-31. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/43855. doi: http://dx.doi.org/10.12660/rda.v239.2005.43855.

32. Ventura M, Coeli CM. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança. Cad. Saúde Pública [Internet]. 2018 [citado em 2019 jun. 7];34(7):1-4. Disponível em: https://www.scielo.br/pdf/csp/v34n7/1678-4464-csp-34-07-e00106818.pdf. doi: https://doi.org/10.1590/0102-311x00106818.

33. Bioni BR. Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP; 2015.

34. Carolan E. The continuing problems with online consent under the EU's emerging data protection principles. Computer Law and Security Review [Internet]. 2016 [citado em 2019 jun. 7];32(3):462-73. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364916300322. doi: https://doi.org/10.1016/j.clsr.2016.02.004.

35. Conselho Federal de Medicina. Resolução CFM nº 2.227, de 6 fevereiro de 2019. Define e disciplina a telemedicina como forma de prestação de serviços médicos mediados por tecnologias [Internet]. 2019 [citado em 2020 jun. 9]. Disponível em: http://www.portal.cfm.org.br/images/PDF/resolucao222718.pdf.

36. Santa Catarina. Lei n. 17.066, de 11 de janeiro de 2017. Dispõe sobre a publicação, na internet, da lista de espera dos pacientes que aguardam por consultas (discriminadas por especialidade), exames e intervenções cirúrgicas e outros procedimentos nos estabelecimentos da rede pública de saúde do Estado de Santa Catarina [Internet]. 2017 [citado em 2020 jun. 9]. Disponível em: http://leis.alesc.sc.gov.br/html/2017/17066_2017_lei.html.

37. Brasil. Projeto de Lei n° 140, de 9 de maio de 2017. Altera a Lei n° 8.080, de 19 de setembro de 1990, que dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências, a fim de determinar celeridade e transparência na realização de procedimentos no âmbito do Sistema Único de Saúde [Internet]. 2017 [citado em 2020 jun. 9]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/129137.

38. Brasil. Projeto de Lei n. 192, de 20 de abril de 2018. Altera a Lei nº 8.080, de 19 de setembro de 1990, que dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências, com o objetivo de assegurar celeridade na realização de procedimentos indicados no âmbito do Sistema Único de Saúde. [Internet]. 2018 [citado em 2020 jun. 9]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133007.

39. Brasil. Conselho Nacional de Saúde. Resolução nº 466, de 12 de dezembro de 2012. Aprova as diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos [Internet]. 2012 [citado em 2020 jun. 9]. Disponível em: http://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf.

40. Brasil. Ministério da Saúde. Secretaria Executiva. Plano diretor de tecnologia da informação e comunicação 2019/2021 [Internet]. 2019 [citado em 2020 jun. 9]. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2019/08/PDTIC-2019-A-2021-FINAL-14-DE-AGOSTO-2019.pdf.

41. Mendes A, Carnut L, Guerra LDS. Reflexões acerca do financiamento federal da Atenção Básica no Sistema Único de Saúde. Saúde Debate [Internet]. 2018 [citado em 2020 jun. 9];42(1):224-43. Disponível em: https://www.scielo.br/pdf/sdeb/v42nspe1/0103-1104-sdeb-42-spe01-0224.pdf. doi: https://doi.org/10.1590/0103-11042018s115.