



Lei geral de proteção de dados e a interoperabilidade na saúde pública

General data protection law and interoperability in public health

Ley general de protección de datos e interoperabilidad en salud pública

Miliane Fantonelli¹, Ianka Cristina Celuppi², Fernanda Maia de Oliveira³, Fernando Burigo⁴
Eduardo Monguilhott Dalmarco⁵, Raul Sidnei Wazlawick⁶

RESUMO

Descritores:
Interoperabilidade da
Informação em Saúde;
Acesso à Informação;
Segurança Computacional

Objetivo: Analisar o que vem sendo feito, no âmbito público, no tratamento dos dados coletados em saúde e, a partir das mudanças trazidas pela lei 13.709/2018, quais reverberações poderão causar na interoperabilidade. **Métodos:** Estudo de abordagem metodológica descritiva, com viés analítico. **Resultados:** O advento da lei 13.709/2018 trouxe de maneira sistemática a forma como os dados devem ser tratados. Nesse sentido, a esfera pública tem deveres específicos para tratar os dados. O trabalho destaca a necessidade de mantê-los em formato interoperável e estruturado. **Conclusão:** A Rede Nacional de Dados em Saúde (RNDS) é uma aposta para a integração de dados em saúde, conforme as demandas da LGPD. No entanto, ainda que algumas iniciativas já tenham sido tomadas, ainda não se tem efetiva aplicabilidade do modelo a despeito da lei já estar vigorando.

ABSTRACT

Keywords: Health
Information
Interoperability; Access
to Information;
Computer Security

Objective: Analyze what has been done, in the public sphere, in the treatment of data collected in health and, based on the changes brought by Law 13.709/2018, which reverberations may cause in interoperability. **Methods:** Study with a descriptive methodological approach, with an analytical focus. **Results:** The advent of Law 13.709/2018 brought in a systematic way how data should be treated. In this sense, the public sphere has specific duties to handle the data. The work focus the need to keep them in an interoperable and structured format. **Conclusion:** The National Health Data Network (RNDS) is a bet for the integration of health data, according to the demands of the LGPD. However, even though some initiatives have already been taken, the model is not yet effectively applicable, despite the fact that the law is already in force.

RESUMEN

Descriptores:
Interoperabilidad de la
Información en Salud;
Acceso a la Información;
Seguridad Computacional

Objetivo: Analizar qué se ha hecho, en el ámbito público, en el tratamiento de los datos recogidos en salud y, en base a los cambios que trae la Ley 13.709/2018, qué repercusiones pueden provocar en la interoperabilidad. **Métodos:** Estudio con enfoque metodológico descriptivo, con sesgo analítico. **Resultados:** La llegada de la Ley 13.709/2018 trajo de manera sistemática la forma en que se deben tratar los datos. En este sentido, la esfera pública tiene deberes específicos para manejar los datos. El trabajo destaca la necesidad de mantenerlos en un formato estructurado e interoperable. **Conclusión:** La Red Nacional de Datos en Salud (RNDS) es una apuesta por la integración de datos en salud, de acuerdo con las demandas de la LGPD. Sin embargo, aunque ya se han tomado algunas iniciativas, el modelo aún no es efectivamente aplicable, a pesar de que la ley ya está en vigor.

¹ Advogada, Laboratório Bridge, Universidade Federal de Santa Catarina, Florianópolis (SC), Brasil.

² Enfermeira auditora, Laboratório Bridge, Universidade Federal de Santa Catarina, Florianópolis (SC), Brasil.

³ Estudante de Graduação em Ciências da Informação, Laboratório Bridge, Universidade Federal de Santa Catarina, Florianópolis (SC), Brasil.

⁴ Analista de Desenvolvimento de Sistemas, Laboratório Bridge, Universidade Federal de Santa Catarina, Florianópolis (SC), Brasil.

⁵ Professor Associado do Departamento de Análises Clínicas, Laboratório Bridge, Universidade Federal de Santa Catarina, Florianópolis (SC), Brasil.

⁶ Professor Titular do Departamento Informática e Estatística, Laboratório Bridge, Universidade Federal de Santa Catarina, Florianópolis (SC), Brasil.

INTRODUÇÃO

O Sistema Único de Saúde (SUS) avançou consideravelmente com relação à ampliação do acesso à saúde, bem como na ampliação de diagnósticos e desenvolvimento tecnológico, garantindo maior assistência com os programas de saúde à comunidade. Com relação à Atenção Primária à Saúde (APS), os avanços são marcados na área de prevenção e promoção à saúde. Ou seja, pode-se considerar a APS como estratégia de maior impacto no SUS, considerada a porta de entrada para o acesso à saúde, com baixo custo para os entes federativos e maiores resolutividades no cuidado à população atendida. A continuidade e longitudinalidade do cuidado, característica essencial da APS, demonstra a importância da saúde integral e principalmente a aproximação da população ao sistema público de saúde⁽¹⁾.

Pensando no contexto da saúde pública brasileira, revela-se indispensável analisar a maneira como os dados vêm sendo tratados nesse âmbito. É importante fazer algumas ressalvas preliminares acerca da Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018, uma vez que ela foi pensada e promulgada dentro de um contexto nacional e global, os quais merecem ser analisados, mesmo que brevemente.

Em 2016 foi aprovado na Europa o Regulamento Geral sobre a Proteção de Dados (GDPR), e no Brasil, o Ministério da Justiça fez consulta pública sobre o assunto, que resultou no projeto de Lei 5.276. Em 2017 o projeto de Lei tramitou, tanto na Câmara dos Deputados, quanto no Senado. Em maio de 2018 entrou em vigor a GDPR na Europa e em agosto foi sancionada a LGPD do Brasil. Em 2019, a medida provisória 869 aprovou a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

Já em 2020, houve o desmembramento da entrada em vigor da LGPD e da aplicação das sanções previstas. De maneira que, entrou em vigor no dia 18 de setembro e a Lei 14.010 do mesmo ano definiu que as sanções oriundas da LGPD serão aplicadas a partir de agosto de 2021. E, por último, o Decreto 10.474 de agosto de 2020 instituiu a Autoridade Nacional de Proteção de Dados - ANPD.

Assim, diante deste pano de fundo, impõe-se o problema deste trabalho: a LGPD trará mudanças na forma como a esfera pública vem tratando os dados na saúde, no que tange à interoperabilidade? É possível vislumbrar os principais desafios para sua implementação? Objetiva-se analisar o que vem sendo feito, no âmbito público, no tratamento dos dados coletados em saúde e, a partir das mudanças trazidas pela nova lei, quais reverberações poderão causar na interoperabilidade deste tratamento. Fazendo esse paralelo entre como está sendo feito e como deverá ser realizado o tratamento dos dados na saúde pública, é possível traçar caminhos para esta adequação.

MÉTODOS

O presente trabalho foi concebido em forma de pesquisa descritiva, com viés analítico. Onde foi proposto, analisar a

luz da nova legislação o que vem sendo feito, no âmbito público, no tratamento dos dados coletados em saúde para, a partir disso, verificar as reverberações trazidas pela LGPD no que tange à interoperabilidade do tratamento dos dados, utilizando-se a modalidade de ensaio baseado em pesquisa bibliográfica e documental.

Deste modo, o trabalho está estruturado em três capítulos: o primeiro irá fazer uma contextualização do modo como vem se realizando o tratamento dos dados de saúde no SUS sob a perspectiva legal; O segundo irá analisar a LGPD no que tange aos dados sensíveis de saúde e o tratamento diferenciado à esfera pública; E, o terceiro, fará uma reflexão acerca dos possíveis ajustes no que tange a interoperabilidade dos dados no SUS.

O tratamento dos dados no SUS até o marco da LGPD

Com a instituição do SUS na Constituição Federal de 1988, a saúde tornou-se objeto de políticas públicas que visem garantir esse direito aos cidadãos residentes em território nacional. Os dados, nesta seara, tornam-se imprescindíveis para que se possa perfectibilizar o que foi colocado pela lei.

No entanto, a coleta e tratamento dos dados, na esfera da saúde pública, não contava com nenhuma legislação ou regramento específico e condensado sobre o assunto. Cabe destacar também que desde 2004, com a publicação da Política Nacional de Informação e Informática em Saúde (PNIIS), o Ministério da Saúde vem tentando desenvolver estratégias de informatização em saúde⁽²⁾. Dessa maneira, os dados que antes eram coletados, armazenados e tratados apenas na via física, também passaram a ter esses processos na via digital. Então, a saúde pública além de atentar para proteção dos dados coletados, no que tange propriamente aos direitos do titular, também precisou pensar em estratégias para garantir a sua interoperabilidade.

Interoperabilidade dos dados na saúde pública antes da LGPD

Para a Sociedade (Americana) de Sistemas de Informação e Gestão de Saúde (*Healthcare Information and Management Systems Society, Inc. - HIMSS*) e seu Comitê Diretor de Integração e Interoperabilidade (I&I) baseando-se no contexto de Rede Nacional de Informação em Saúde (*National Health Information Network - NHIN*), interoperabilidade é a capacidade de diferentes sistemas de informação de trabalharem juntos para acessar, trocar, integrar e usar dados de forma cooperativa de maneira coordenada, dentro e através das fronteiras organizacionais, regionais e nacionais, fornecendo portabilidade oportuna e contínua das informações, otimizando a saúde de indivíduos e populações globalmente, promovendo a prestação eficaz de cuidados de saúde para indivíduos e comunidades⁽³⁾.

Tendo em vista o conceito, destaca-se que em 2011 foi emitida a Portaria nº 2.073 em que abordou duas dimensões da interoperabilidade: envio/recebimento de informações e comunicação entre sistemas de informação. Assim, para alcançar a interoperabilidade em saúde foi preciso definir padrões de estrutura da informação, semântica, interface de serviços, componentes de sistema, dentre outros⁽⁴⁾.

Definiu-se então, como padrões de interoperabilidade o conjunto mínimo de premissas, políticas e especificações técnicas que normatizam e regulamentam o intercâmbio de informações entre os sistemas de saúde, em nível municipal, estadual e federal, estabelecendo condições de interação com demais atores envolvidos no processo, sejam eles públicos ou privados⁽⁴⁾. No art. 4º da referida portaria ficou posto que os padrões de interoperabilidade estariam no Catálogo de Padrões de Interoperabilidade de Informações de Sistemas de Saúde (CPIISS), publicado pelo Departamento de Informática do SUS (DATASUS/SGEP/MS), disponível para a sociedade em geral. Esta portaria já pautava, então, alguns padrões (nem todos relacionados à interoperabilidade), como o padrão Open EHR com foco na estrutura, o HL7 com foco na comunicação, o TUSS com foco na terminologia, entre outros⁽⁵⁾.

Além disso, a Nota Técnica 37 de 2011, emitida pelo Conselho Nacional das Secretarias em Saúde (CONASS), que trata sobre a portaria mencionada, traz importantes esclarecimentos sobre o que o Ministério da Saúde entende por interoperabilidade. Assim, o documento definiu três tipos de interoperabilidade: intercâmbio de informações, agregação de informações e informações computáveis.

LGPD: como deverão ser tratados os dados de saúde recolhidos pelo SUS?

O sistema de saúde brasileiro é desafiador, principalmente por instituir acesso universal, equitativo, descentralizado, com gestão dos governos subnacionais e dividir seu espaço com o setor privado de saúde, amparado constitucionalmente como suplementar⁽⁶⁾. Inúmeros atores e organizações (públicas ou privadas) estão envolvidas diretamente no processo saúde-doença dos cidadãos brasileiros, o que requer estratégias de organização e articulação entre os diversos pontos da rede de atenção à saúde, seja para o encaminhamento assistencial do usuário ou para a transmissão de seus dados de saúde. Deste modo, a implementação da LGPD no SUS precisa considerar tamanha complexidade, atentando para pontos nevrálgicos, como a interoperabilidade, os direitos do titular dos dados (acesso, correção, exclusão, informações sobre compartilhamento, conforme preconiza o artigo 18 da LGPD) e o estabelecimento de figuras como Controlador(es), Operador(es) e Encarregado(s).

A proteção dos dados no caso brasileiro apresenta uma particularidade (em relação à GDPR) que é a diferenciação de tratamento entre a iniciativa privada e o poder público, visto a necessidade de implementar políticas públicas, por exemplo. Nesse sentido, a LGPD conta com capítulo específico para tratar da administração pública⁽⁷⁾. No primeiro artigo deste capítulo, artigo 23, ela coloca que as pessoas jurídicas de direito público podem realizar o tratamento dos dados para cumprir com a sua finalidade pública, dentro das suas atribuições e competências legais. Mas, para isso, devem informar ao cidadão qual a finalidade, os procedimentos e as práticas para executar esse tratamento. E ainda, institui que seja constituído um Encarregado (responsável por aceitar e

esclarecer dúvidas dos titulares e orientar os profissionais acerca da forma correta no manuseio dos dados, de acordo com o artigo 41).

Além disso, a Lei também trata, no artigo 25, da necessidade de se manter os dados em formato interoperável e estruturado para o uso compartilhado. Isso possibilita a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação ao acesso das informações pelo público em geral. Também cabe destacar que o poder público não pode transmitir os dados a entidades privadas. Exceto para os casos de execução descentralizada, a qual exija a transferência, exclusivamente para esse fim específico e determinado; ou, quando os dados forem acessíveis publicamente; ou, quando houver previsão legal, convênio, contrato que respalde a ação; ou, quando a transferência objetivar a prevenção de irregularidades, a proteção, a segurança e a integridade dos dados, e apenas para essas finalidades, consoante o artigo 26.

Acerca do consentimento, interessante colocar que a Lei regulamenta de tal forma que a administração pública poderá tratar os dados, desde que vise a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, conforme o artigo 7º, de maneira que, diante dessa hipótese, dispensa o consentimento. Mas, a comunicação e o uso compartilhado dos dados exigem o consentimento do titular, salvo nas hipóteses previstas em Lei (dados públicos e na execução descentralizada respaldada contratualmente e com fim específico), de acordo com o artigo 27.

A Autoridade Nacional poderá exigir do poder público realização de operações no tratamento dos dados, para se adequar à Lei. E, quando houver irregularidades, a Autoridade poderá emitir informe com medidas cabíveis para cessar a violação, bem como exigir do poder público a emissão de relatórios de impacto à proteção dos dados. As penalidades pelo não cumprimento da lei, talvez sejam os pontos de maior diferença entre a iniciativa privada e o poder público. Isso porque na administração pública, apesar de contar com rol amplo de sanções, nenhuma delas é pecuniária. Dentre as sanções que poderão ser aplicadas aos órgãos públicos, de acordo com o artigo 52 da lei, estão (a) a advertência, com indicação de prazo para adoção de medidas corretivas, (b) a publicização da infração após devidamente apurada e confirmada a sua ocorrência, (c) o bloqueio dos dados pessoais a que se refere a infração até a sua regularização, (d) a eliminação dos dados pessoais a que se refere a infração, (e) a suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, (f) a suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, (g) a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Assim, essa breve análise buscou demonstrar a maneira como a esfera pública será tratada pela Lei geral de

proteção de dados. Isso porque, o escopo do trabalho é explorar o viés da saúde pública.

Rede Nacional de Dados em Saúde: uma aposta para integrar os dados na saúde pública e mantê-los em formato interoperável conforme a LGPD

Acerca da interoperabilidade preconizada pela LGPD, cabe mencionar o projeto da Rede Nacional de Dados em Saúde (RNDS). Ela é uma plataforma de integração de dados em saúde, iniciativa do Departamento de Informática do SUS (DATASUS) da Secretaria Executiva. Ao longo do seu desenvolvimento, a RNDS irá se constituir uma desejada infovia de saúde, ou seja, uma plataforma informacional de alta disponibilidade, segura e flexível, que favorece o uso ético aos dados de saúde, permitindo o surgimento de novos serviços, inovação, pesquisa e desenvolvimento⁽⁸⁾. Dessa maneira, primeiro cabe compreender do que se trata a RNDS.

Os objetivos da RNDS compreendem (a) melhoria no atendimento, com o acesso às informações em saúde, maior transparência, registro de atendimento, melhor oferta dos serviços de saúde, (b) acompanhamento do paciente, (c) eficiência na gestão do recurso público com a organização das informações, o mapeamento de necessidades, o planejamento de ações, a ampliação do monitoramento e o combate às fraudes e (d) inovação em saúde, com o uso de telessaúde, de inteligência artificial, tecnologias emergentes, valorização da qualidade dos dados e integração com internet das coisas⁽⁸⁾.

O Ministério da Saúde⁽⁸⁻⁹⁾ explica que tal solução tecnológica refere-se a um repositório de documentos responsável por armazenar informações de saúde dos cidadãos. Utiliza para isso a tecnologia *Blockchain*, na qual diferentemente do modelo de banco de dados centralizado, ela realiza a validação de registros/informações em inúmeros servidores. Assim, dificulta, por exemplo, a fraude de algum prontuário que está centralizado em um único servidor, agregando maior segurança na transmissão/armazenamento dos dados em saúde. Esta solução também é importante para evitar a sobrecarga de solicitações de acesso e gerar lentidão em um único servidor, de modo a distribuir as informações em uma rede de servidores⁽¹⁰⁾.

A implementação da RNDS se daria a partir de março de 2020, com o projeto piloto, em Alagoas. No entanto, com o Covid-19, o projeto foi redirecionado para receber e compartilhar informações que pudessem dar o devido suporte para cidadãos e profissionais de saúde no combate ao novo coronavírus. Dessa forma, o Ministério da Saúde, com apoio dos laboratórios públicos e privados, permitirá a recepção e o compartilhamento dos resultados dos exames relacionados ao Covid-19⁽⁸⁾.

A maneira como a implementação se dará é a partir da disponibilização de contêineres virtuais em nuvens para cada estado da Federação, cuja responsabilidade é do DATASUS. E, como o escopo da RNDS foi redirecionado, ele agora permitirá “o compartilhamento de resultados de exame da COVID-19 realizados em qualquer lugar do país, por meio de serviços desenvolvidos de acordo com o padrão HL7 FHIR e

utilizando a terminologia LOINC”⁽⁸⁻⁹⁾.

De posse dessas informações, deve-se inserir a questão da LGPD já mencionada no trabalho. Em junho deste ano o Datasus⁽¹¹⁾ lançou a cartilha com ações para adequação da RNDS à LGPD. Assim, foi posto que os dados de saúde devam ser coletados, processados e armazenados de acordo com padrões de confidencialidade e segurança proporcionais à sua sensibilidade, o que vai ao encontro das diretrizes estabelecidas para segurança no tratamento dos dados.

Além disso, o acesso aos dados da RNDS se dará de duas maneiras: o titular poderá acessar os dados por meio do aplicativo Conecte SUS, mediante autenticação de acesso aos serviços públicos digitais do governo. Enquanto os profissionais da saúde poderão solicitar acesso pelo perfil profissional vinculado ao aplicativo Conecte SUS, mediante autenticação do Certificado Digital ICP-Brasil de instalações do Prontuário Eletrônico do Paciente previamente habilitado para o estabelecimento de saúde. A cartilha também estabelece que o acesso pelos profissionais deve estar restrito ao contexto de atendimento⁽¹¹⁾.

Outro padrão que deve ser seguido para a conformidade da LGPD é o rastreamento dos acessos aos dados, ou seja, a RNDS deve ser capaz de identificar de forma inequívoca que dado foi acessado, por qual profissional, em que estabelecimento de saúde se deu a consulta, quando (data/hora) essa consulta foi realizada e qual a origem do documento exposto no Portal Conecte SUS. Segundo a cartilha com ações para adequação da RNDS à LGPD, todos esses requisitos de rastreamento serão implementados de modo que o titular possa acompanhar a trajetória de acesso aos seus dados de saúde⁽¹¹⁾.

Como medida de segurança adotada pela RNDS revela-se a instituição da certificação digital para acesso aos dados de saúde. O Certificado Digital é o documento eletrônico que possibilita a troca segura de informações entre duas partes, com a garantia da identidade do emissor e integridade da mensagem. Para isso, são geradas duas chaves de criptografia: uma pública e outra privada. A chave pública fica em posse do estabelecimento e é utilizada para assinar, enquanto a privada é utilizada para verificar a integridade e autenticar o documento. Essa chave compõe um sistema de criptografia assimétrica, onde os dados só conseguirão ser acessados se o receptor tiver a chave correta para decodificá-los. Essas duas chaves são geradas aleatoriamente por funções matemáticas e trabalham em conjunto. Aderente à LGPD, todo acesso realizado ao RNDS é identificado pelo Certificado Digital e todos os dados enviados ao RNDS serão assinados e o cidadão tem a opção de não autorizar o uso desses dados. Todas as transações ficam armazenadas, permitindo rastreabilidade, possibilitando um alto grau de segurança.

Embora a cartilha divulgada pelo Datasus trate das adequações à LGPD, ela não menciona a questão da interoperabilidade. Foi a Portaria 1.434 de 2020, a qual instituiu a RNDS, que fez importantes alterações acerca da questão dos padrões de interoperabilidade em saúde. Ela atribuiu novas categorias e terminologias acerca do

que o SUS entende por interoperabilidade: modelo de informação ou informacional, modelo computacional, interoperabilidade semântica e interoperabilidade sintática⁽⁸⁾.

Além disso, a portaria em vigor alterou a forma de divulgação dos padrões de interoperabilidade, os quais agora são separados pelas referidas categorias, conforme o art. 233. Os padrões de interoperabilidade sintática e modelos de informação serão disponibilizados no site do Datasus. As terminologias, ontologias, classificações e outros recursos semânticos constarão no site do Repositório em Terminologias em Saúde. E, quanto aos aspectos relacionados à governança, gestão e políticas específicas de interoperabilidade em saúde estarão no site da Saúde Digital.

Outro ponto que merece ser destacado é a possibilidade de adoção de novos padrões de interoperabilidade, de acordo com o art. 234, desde que demonstrem, no mínimo: os custos de adoção do padrão, os esforços necessários para a adoção do padrão, a adoção por outros órgãos ou instituições do setor de saúde brasileiro em caráter não experimental ou acadêmico, a adoção pelo setor de saúde dos governos de outros países, especialmente por aqueles que sejam parceiros do Brasil ou com os quais o Brasil coopere e as vantagens de sua adoção em relação a outros padrões que atendam à mesma finalidade⁽⁹⁾.

A RNDS, nesse sentido, conforme mencionado optou por utilizar o padrão HL7 FHIR. O Datasus explica que esse padrão é rápido, flexível, gratuito e de ampla adoção mundial⁽¹²⁾. A especificação HL7 FHIR tem como propósito redução dos empecilhos para interoperar em larga escala eliminando os silos de informações geradas pelos sistemas de registro eletrônico em saúde⁽¹³⁾.

Visualizando os desafios para a implementação do padrão HL7 FHIR podemos apontar a questão a adoção como a principal, já que o padrão em si suporta nativamente o Protocolo RESTful⁽¹⁴⁾ que é padronizado em todo o mundo. O padrão, em si, oferece uma série de vantagens, mas na prática a sua implementação é mais complexa por requerer uma adaptação que demandará tempo e necessitará de um suporte substancial às organizações⁽¹⁵⁾, prejudicando a adoção mundial.

Outro ponto, foi a troca da implementação do padrão openEHR pelo padrão HL7 FHIR⁽¹²⁾. Outros sistemas de saúde, como o NHS (*National Health Service*), sistema de saúde público do Reino Unido, semelhante ao SUS, o qual também teve que se adequar à GDPR, utiliza atualmente o openEHR. Assim, ao se definir a adoção do padrão HL7 retoma-se, do início, o trabalho da interoperabilidade.

No que tange ao que se entende por “vantagem”, a portaria explica no art. 235 que isso significa que os padrões de interoperabilidade em saúde devem ser abertos/livres ou sem custos de utilização, tenham menor custo e complexidade de adoção, inclusive para os demais entes federados, tenham maior adoção pelo setor de saúde brasileiro em caráter não experimental ou acadêmico, tenham maior adoção pelos governos de outros países, especialmente por aqueles que sejam parceiros do Brasil

ou com os quais o Brasil coopere e estejam em versões estáveis⁽⁹⁾.

Caso o padrão, por motivos de viabilidade técnica, não seja aberto/livre ou sem custos, deve ser observada a seguinte ordem de preferência: 1) serem desenvolvidos pelo Ministério da Saúde, Agência Nacional de Saúde Suplementar - ANS ou Agência Nacional de Vigilância Sanitária – Anvisa ou 2) pelos órgãos públicos de saúde dos Municípios, Estados ou Distrito Federal e por último 3) privados ou pagos⁽⁹⁾.

Ademais, a portaria estabelece no art. 236 que os padrões adotados pelos municípios, estados e distrito federal podem ser distintos, desde que seja garantida a interoperabilidade com os padrões nacionais. Caberá, dessa forma, ao Datasus avaliar esses novos padrões e gerir os seus usos, emitindo atos normativos para esta finalidade, conforme o art. 238⁽⁹⁾.

Ocorre que, embora o Ministério da Saúde tenha pensado e projetado a RNDS, oficialmente ela ainda se encontra no patamar de projeto piloto. Assim, a RNDS ainda não está implementada plenamente, o que, se estivesse feito, muito ajudaria na formulação de políticas públicas de controle da pandemia no Brasil, além de resguardar a segurança dos dados dos titulares, que é o escopo principal da LGPD. Fato é que a Lei está em vigor, e em termos práticos pouco foi feito. Embora tenha sido divulgada a cartilha de adequação da RNDS à LGPD e a portaria mencionada também trate da questão da interoperabilidade, ainda há muitas lacunas que deverão ser supridas para que se garantam os dados em formato estruturado e interoperável, conforme menciona a LGPD. Lacunas que só surgirão a partir do momento em que a RNDS começar a ser plenamente implementada. Até lá, estaremos em uma espécie de limbo entre o entendimento antigo, de 2011, dos formatos de interoperabilidade e o novo entendimento que vem junto com a RNDS.

CONCLUSÃO

Diante do exposto no trabalho, ficou claro que o assunto da proteção dos dados na saúde pública é um tema que continua sendo explorado, principalmente depois que se deu a informatização da saúde. Nesse sentido, a LGPD trouxe importantes mudanças: os dados não devem ser coletados irrestritamente e sim com uma finalidade, a qual deve ser repassada ao titular, bem como os procedimentos e as práticas para executar o tratamento dos dados. Além disso, a lei impõe que seja definido um encarregado, que ficará responsável pela comunicação entre o controlador, os titulares dos dados e a ANPD.

Embora a coleta dos dados na saúde pública seja, ao fim e ao cabo, para realizar políticas públicas, será necessário informar ao titular acerca do uso compartilhado dos dados. E, ainda, trouxe a questão do dever de manter os dados em formato interoperável e estruturado para o uso compartilhado, que é onde se focou o trabalho.

Isso responde ao primeiro questionamento do presente trabalho: a LGPD trará mudanças na forma como a esfera pública vem tratando os dados na saúde, no que tange à interoperabilidade? Chegamos à conclusão que

sim. A partir de agora será preciso atentar para todas as questões dos direitos do titular, da proteção dos dados, e da interoperabilidade, sob pena do enfrentamento das sanções colocadas pela lei.

Nesse sentido, a RNDS, ainda que não tenha sido projetada com o intuito específico de interoperabilidade dos dados, conforme preconiza a LGPD, por ela ser um centralizador que pretende a integração de dados em saúde, é também uma aposta que a partir dela se consiga atender às demandas da lei de proteção aos dados. Mas, recai-se ao segundo questionamento da pesquisa: é possível vislumbrar os principais desafios para implementação das mudanças impostas pela LGPD? Sim, demonstra-se factível antever os entraves que se impõem. Isso porque a lei já está vigorando e (a) mesmo que as sanções sejam aplicadas apenas no próximo ano, (b) o Datasus tenha divulgado uma cartilha de adequação à LGPD, (c) o Ministério da Saúde tenha emitido uma portaria de

implementação da RNDS e como irá funcionar a questão da interoperabilidade, ainda não há nada concreto sobre o assunto, pois a RNDS ainda não foi, de fato, plenamente implementada.

E, especificamente sobre a questão da interoperabilidade o padrão adotado pelo Datasus – HL7 FHIR – embora seja um padrão referência, em termos de qualidade, o esforço que demandará a factual implementação é bastante grande, o que pode comprometer a interoperabilidade em si, na prática. Essas questões implicam lacunas que demonstram que a LGPD e a interoperabilidade ainda não ganharam plena eficácia na esfera da saúde pública.

AGRADECIMENTOS

Os autores agradecem ao Ministério da Saúde, o qual financiou essa pesquisa como parte integrante do Projeto e-SUS APS Etapa 4.

REFERÊNCIAS

1. Fernandes VC, Sousa CL. Aspectos históricos da saúde pública no Brasil: revisão integrativa da literatura. *Journal of Management & Primary Health Care*. 2020 Jan;12(1):1-7. [cited 2020 Jul 20]. Available from: <https://www.jmphc.com.br/jmphc/article/view/579>.
2. Fornazin M. A informatização da saúde no Brasil: uma análise multi-paper inspirada na teoria ator-rede (Doctoral dissertation). [cited 2020 Jul 20]. Available from: <https://bibliotecadigital.fgv.br/dspace/handle/10438/13744>.
3. Healthcare Information and Management Systems Society - HIMSS Board of Directors. Interoperability Definition and Background. HIMSS.org, 2005. [cited 2020 Aug 14]. Available from: <https://www.himss.org/sites/hde/files/d7/HIMSSorg/Content/files/AUXILIOHIMSSInteroperabilityDefined.pdf>
4. Ministério da Saúde. Portaria nº 2.073, de 31 de agosto de 2011. Regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde, nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar. *Diário Oficial da União*. 2011. [cited 2020 Mai 20]. Available from: http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html
5. Sales OM, Pinto VB. Tecnologias digitais de informação para a saúde: revisando os padrões de metadados com foco na interoperabilidade. *Revista Eletrônica de Comunicação, Informação e Inovação em Saúde*. 2019 Mar 29;13(1). [cited 2020 Aug 31]. Available from: [http://docs.bvsalud.org/biblioref/2019/04/987731/tecnologias-digitais-de-informacao-para-a-saude-revisando-os-pa_UBN\]JdM.pdf](http://docs.bvsalud.org/biblioref/2019/04/987731/tecnologias-digitais-de-informacao-para-a-saude-revisando-os-pa_UBN]JdM.pdf).
6. Celuppi IC, Geremia DS, Ferreira J, Pereira AM, Souza JB. 30 anos de SUS: relação público-privada e os impasses para o direito universal à saúde. *Saúde em Debate*. 2019 Aug 5;43:302-13. [cited 2020 Jun 20]. Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-11042019000200302&lng=en&nrm=iso.
7. 7 Brasil. Lei N. 13.709, de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da República Federativa do Brasil* (14 ago. 2018). 2018. [cited 2020 Mai 20]. Available from: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
8. Ministério da saúde. A RNDS. 2020. [cited 2020 Mai 20]. Available from: <https://rnds.saude.gov.br/>.
9. Ministério da saúde. Portaria nº 1.434, de 28 de maio de 2020. [cited 2020 Ago 31]. Available from: <https://www.in.gov.br/en/web/dou/-/portaria-n-1.434-de-28-de-maio-de-2020-259143327>
10. Drescher D. *Blockchain basics*. Berkeley, CA: Apress; 2017.
11. Datasus. Ações para adequação da RNDS à Lei geral de proteção de dados. 2020. Brasília: Ministério da Saúde. [cited 2020 Jun 30]. Available from: <https://rnds.saude.gov.br/wp-content/uploads/2020/06/A%C3%A7%C3%B5es-para-a-Adequa%C3%A7%C3%A3o-da-RNDS-%C3%A0-LGPD-%E2%80%93-24.11.2020.pdf>.
12. Datasus. Padrão de interoperabilidade para troca de informações de resultados de exames. 2020. Brasília: Ministério da Saúde. [cited 2020 Nov 16]. Available from: <https://rnds.saude.gov.br/wp-content/uploads/2020/07/Apresenta%C3%A7%C3%A3o-Modelos-RNDS-20200405.pdf>
13. Rades P R, Portabilidade entre paradigmas de interoperabilidade, Mensagens HL7™ versão 2.x versus HL7™ FHIR™. InterOpera, XVI Congresso Brasileiro de Informática em Saúde [Internet]. 2018 Oct 01-04:865-887p. [cited 2020 Sep 2] Available from: http://www.sbis.org.br/biblioteca_virtual/cbis/Anais_CBIS_2018_Artigos_Completos.pdf.
14. Ferreira Filho, Otávio Freitas. *Serviços semânticos: uma abordagem RESTful* [dissertation]. São Paulo: University of São Paulo, Escola Politécnica; 2010 [cited 2020 Nov 16]. Available from: <https://www.teses.usp.br/teses/disponiveis/3/3141/tde-11082010-120409/en.php>
15. Rishi Saripalle, Christopher Runyan, Mitchell Russell. *Journal of Biomedical Informatics, Using HL7 FHIR to achieve interoperability in patient health record*, 2019. [cited 2020 Nov 15]. Available from: <https://www.sciencedirect.com/science/article/pii/S1532046419301066>