ARMAZENAMENTO DESCENTRALIZADO NO SISTEMA ÚNICO DE SAÚDE BRASILEIRO (SUS) USANDO INTERPLANETARY FILE SYSTEM (IPFS) E BLOCKCHAIN | *DECENTRALIZED STORAGE IN THE BRAZILIAN UNIFIED HEALTH SYSTEM (SUS) USING INTERPLANETARY FILE SYSTEM(IPFS) AND BLOCKCHAIN*

CAROLINE NUNES
STEPHANE MA
MARCELO SILVEIRA TEIXEIRA FILHO

RESUMO | Este artigo analisa o Sistema Único de Saúde (SUS), que mantém eletronicamente dados médicos, incluindo informações pessoais dos pacientes, relatórios, diagnósticos e prescrições médicas. No entanto, o modelo de armazenamento centralizado utilizado atualmente mostra-se inadequado para armazenar estas informações sensíveis. Tem-se como objetivo propor um novo sistema de um armazenamento descentralizado de dados médicos compatível com a Lei Geral de Proteção de Dados (LGPD), usando o IPFS (*Interplanetary File System*) e a tecnologia *Blockchain*. O artigo é um estudo exploratório e descritivo, utilizando-se de um amplo arcabouço bibliográfico e consulta em fóruns de tecnologia. Como principal resultado, tem-se que o novo modelo preserva a privacidade do paciente e facilita o acesso de dados médicos por entidades autorizadas, como prestadores de serviços de saúde. Conclui-se que a implementação do sistema proposto permitiria uma maior transparência, integridade, integração e segurança no sistema utilizado atualmente pelo SUS.

PALAVRAS-CHAVE | Blockchain. InterPlanetary File System (IPFS). Sistema Único de Saúde (SUS).

ABSTRACT | *This article analyzes the Unified Health System (SUS), which electronically maintains medical data that includes patients' personal information, diagnostic reports, and medical prescriptions. However, the centralized storage model used today is inadequate to store this sensitive information. The objective is to propose a new system of decentralized storage of medical data compatible with the General Data Protection Law (LGPD), using IPFS (Interplanetary FileSystem) and Blockchain technology. The article is an exploratory and descriptive study, using a wide bibliographic framework and consultation on technology forums. As a main result, the new model preserves patient privacy and facilitates access to medical data by authorized entities, such as health service providers. It is concluded that the implementation of the proposed system would allow greater transparency, integrity, integration and security in the system currently used by SUS.*

KEYWORDS | *Blockchain. InterPlanetary File System (IPFS). Unified Health System (SUS).*

1. INTRODUÇÃO

Em 1988, a Constituição brasileira definiu a saúde como direito universal e de responsabilidade do Estado. O progresso rumo à cobertura universal de saúde no Brasil foi alcançado por meio da implementação do Sistema Único de Saúde (SUS), criado em 1990. Sucede que o SUS não acompanhou efetivamente a revolução tecnológica que se seguiu, mantendo um sistema de informações fragmentado, ineficiente, pouco seguro e sem à transparência devida. A falta de investimentos no setor tecnológico do SUS torna o sistema incompatível com a Lei Geral de Proteção de Dados (LGPD).

Em meio à pandemia do COVID-19, o uso de novas tecnologias para cumprimento dos fins e modernização da máquina pública vem sendo considerado em diversos níveis da Administração, reforçando a ideia de proteção necessária aos dados pessoais. Destaca-se aqui o Projeto Legislativo de nº 3443/2019, que dispõe sobre a Prestação Digital dos Serviços Públicos na Administração Pública - Governo Digital, que visa desburocratizar e impulsionar o processo de segurança da informação no serviço público através do uso de tecnologias como o *Blockchain,* que revolucionou o registro de distribuição dos dados, visando a sua descentralização para segurança quanto ao seu armazenamento.

Assim, em função da pandemia, com a edição da Lei n. 13.979 de 2020, foi autorizado através do art. 6º[1] o uso de dados pessoais para políticas públicas voltadas ao controle da infecção viral, em decorrência do estado de emergência declarado pela Portaria nº. 188, de 3 de fevereiro de 2020 do Ministério da Saúde. O processo de levantamento dos dados da Sars-Cov-2 acelerou não somente a averiguação da doença, mas como, igualmente, colocou em evidência discussões quanto a forma de coleta, compartilhamento e preservação das informações a fim de resguardar a proteção desses dados sensíveis essenciais ao combate da doença. Durante a pandemia, as falhas no

1 Art. 6º. É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.

sistema do SUS ficaram ainda mais evidentes, tendo inclusive culminado em um vazamento de dados de mais de 200 milhões de brasileiros[2].

Com a popularização da tecnologia *blockchain*, é possível perceber uma nova onda de transmutação tecnológica no horizonte, podendo ter um efeito duradouro sobre o Sistema Único de Saúde brasileiro (SUS). O fato de que as informações adicionadas no *Blockchain* são imutáveis e invioláveis, faz desta tecnologia uma solução perfeita para o SUS. Além disso, esta tecnologia poderia fornecer registros em um banco de dados acessível de forma globalizada. A tecnologia se torna ainda mais poderosa associada a um protocolo de armazenamento descentralizado, como o *InterPlanetary File System* (IPFS).

O presente artigo propõe uma nova estrutura distribuída baseada em *blockchain* e IPFS, e um conjunto de mecanismos para garantir acesso seguro aos documentos e prontuários médicos.

A pesquisa objetiva fazer um estudo sobre o atual modelo tecnológico do SUS, analisando o banco de dados do sistema de saúde brasileiro, sua regulamentação, adequação à LGPD e à problemática em torno do compartilhamento e armazenamento das informações coletadas, sugerindo, por fim, uma resposta aos dilemas ora elencados com o uso da tecnologia *blockchain* aliada ao IPFS.

Este artigo é um estudo exploratório, e se utilizou de um arcabouço bibliográfico e consulta em fóruns de tecnologia, além dos principais sites de criptomoedas, como *Bitcoin* e *Ethereum*. A pesquisa também tem caráter descritivo, pois analisa a aplicação do *blockchain* no contexto organizacional do SUS e destaca as vantagens e desvantagens do uso da tecnologia, fazendo uso do procedimento documental.

Como principal resultado, tem-se que o modelo proposto adequa-se à LGPD, preserva a privacidade do paciente e facilita o acesso de dados

2 Segundo o jornal G1: "O número de registros expostos é maior que o da atual população brasileira, porque há também informações de pessoas que já morreram. Desde junho, os sistemas da pasta mostram fragilidade de proteção a dados.". G1. Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. Disponível em https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 22 Dez. 2020.

médicos por entidades autorizadas, como prestadores de serviços de saúde. Além disso, permite um maior controle dos dados pessoais pelo próprio paciente, aumentando a transparência, integridade, integração e segurança do SUS.

2. USO DE DADOS NO BRASIL

2.1. Regulamentação de dados pessoais no Brasil

A intensificação do uso de dados pessoais para estratégias governamentais voltados à saúde ganhou enorme destaque quando, em meio a uma crise global decorrente da pandemia, os governos incrementaram e aceleraram a gestão e o monitoramento das informações produzidas pelos cidadãos com fins de auxiliar no combate ao vírus Sars-Cov-2 (COVID-19).

Neste contexto, para sustentar a viabilidade e aprimorar a utilização dos dados oriundos de monitoramento do sistema de saúde, é preciso fazer um levantamento no que tange à regulamentação e legislação de dados, a fim de garantir a privacidade e a segurança dos titulares. Deve ficar bem claro que o intuito do texto não é problematizar os diversos direitos fundamentais decorrentes da forma de produção e titularidade dos dados pessoais, mas sim, questionar a segurança e disponibilidade destas informações geridas pelos diversos agentes de saúde a nível público ou até mesmo privado.

O alinhamento de políticas e regulações voltadas ao monitoramento de dados pessoais para saúde pública já vinha sendo utilizado antes mesmo da disseminação da COVID-19, já existindo, em alguns Governos, aparato legal para o tratamento destas informações, inclusive no Brasil. A exemplo, cita-se a Coreia do Sul, um dos países que melhor barrou a curva de contágio pelo vírus (COVID-19)[3]. Esse país, desde 2011, já possuía legislação sobre o tratamento de dados, a *Personal Information Protection Act*[4], previa a possibilidade do uso de dados pessoais para situações de saúde pública, inclusive permitindo a

3 CARBINATTO. Bruno. A estratégia de sucesso da Coreia do Sul contra a Covid-19: testes em massa. Revista Super. 24 de março de 2020. Disponível em https://super.abril.com.br/saude/a-estrategia-de-sucesso-da-coreia-do-sul-contra-a-covid-19-testes-em-massa/. Acesso em: 01 de setembro de 2020.

inaplicabilidade de parte de sua própria legislação sobre proteção e direitos fundamentais.

Já no Brasil, antes mesmo da edição da Lei Geral de Proteção de Dados (LGPD) em 2018, a Lei de Acesso à Informação (Lei nº. 12.527/2011) já continha dispositivo referente ao trato de dados pessoais, como no artigo 31º[5], que dispõe sobre a postura do ente público quanto aos dados pessoais coletados em suas esferas administrativas. Menciona-se, também, o Marco Civil da Internet (Lei nº.12.965/2014) que, em termos diferentes da Lei de Acesso à Informação, foi a primeira edição normativa a conceituar dados pessoais.

A Lei Geral de Proteção de Dados (Lei nº. 13.709/2018) se tornou a mais importante legislação sobre a temática do tratamento de dados pessoais, inclusive no que tange a sua utilização para políticas públicas voltadas à saúde e o interesse da sociedade.

Cumpre rapidamente conceituar que, nos temos da Lei Geral de Proteção de Dados, o art. 5º classifica os dados referentes a saúde do cidadão como dados sensíveis, sendo por definição aquele de *origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.* O tratamento destes dados pela Administração Pública é autorizado pelo art. 11º, 'da mesma lei e, principalmente pelo art. 13[6], sendo que, em relação ao titular do dado pessoal, a sua ciência e o seu consentimento sobre o tratamento, conforme art. 11º, § 2º da LGPD, poderá ser dispensado nos termos da lei.

4 "3. *Personal information processed temporarily in case it is urgently necessaryfor the public safety and welfare, public health, etc.; or*". Coreia do Sul. Personal Information Protection Act. Act No. 10465, 29 de março de 2011. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=1.

5 Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

6 Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

A relação entre o titular do dado e o Estado narrada na LGPD deve pautar-se nos princípios ali expostos, como, por exemplo, o princípio da finalidade[7] (art. 23º) - que vincula a atuação do poder público quanto ao tratamento dos dados pessoais à determinada política pública - e o princípio da adequação - que garante um encaixe entre o propósito do levantamento de dados e a política que se visa alcançar.

O desvio da finalidade ou a inadequação no manejo dos dados pessoais gera a responsabilidade do agente público. As hipóteses de incidência legal quanto aos deveres do agente público, inclusive, já são enumeradas na Lei de Acesso à Informação, anterior até a LGPD, que tipifica as condutas ilícitas por parte da administração pública.

Abre-se aqui um parêntese para deixar claro que a responsabilidade pode, também, se aplicar aos dados anonimizados, principalmente quanto às técnicas de anonimização destes dados, pois, ainda que não possuam características de dados pessoais, é necessário garantir a real impossibilidade de identificação do sujeito titular daquela informação. Fato é que, mesmo antes da LGPD, as legislações infraconstitucionais já versavam sobre a proteção do que hoje se denomina como dados sensíveis.

Aliado a observância a garantia constitucional do art. 5º, X, quanto à inviolabilidade da vida privada, honra e imagem da pessoa, o Estado tem o dever primordial da segurança[8], o qual deve ser observado não somente quanto a regulamentação das relações privadas, mas, igualmente, na implementação do sistema de informatização do Estado, em razão dos riscos de sua operação.

7 "Decorre da observância ao princípio da finalidade que a operação de tratamento de dados deve guardar direita relação com a missão institucional do órgão ou ente público detentor da base de dados sobre a qual está fundamentada a execução de política pública para o qual foi investido a lei." TASSO, Fernando Antonio, MALDONADO, Viviane Nóbrega (Coord.). BLUM, Renato Opice (Coord.). LGPD: Lei Geral de Proteção de Dados comentada. Thomson Reuter Brasil. 2019. Edição *ebook*.

8 "No quadro de uma sociedade técnica, o estado tem de intervir ante novas ameaças de uma técnica que aumentou a fonte de perigo". SALERT, Ingo Wolfgang (coord.). Direito, Inovação e Tecnologia Volume 1. Posição 976. Saraiva. 2017. Edição Kindle.

2.2. Segurança de dados no sistema de saúde

O uso de novas tecnologias para cumprimento dos fins e modernização da máquina pública vem sendo considerado em diversos níveis da Administração, reforçando a ideia de necessária proteção aos dados pessoais.

Destaca-se aqui o Projeto Legislativo de nº. 3443/2019, que dispõe sobre a Prestação Digital dos Serviços Públicos na Administração Pública - Governo Digital, visando desburocratizar e impulsionar o processo de segurança da informação no serviço público através do uso de tecnologias, como o *blockchain,* que revolucionou o registro de distribuição dos dados, buscando a sua descentralização para segurança quanto ao seu armazenamento.

Já na gestão dos dados pessoais oriundos dos usuários do Sistema Único de Saúde (SUS), principal política de saúde do Brasil, regulada pela Lei nº. 8.080/1990, é o departamento de informática denominado como Departamento de Informática do SUS – DATASUS (nomenclatura dada no Decreto Lei nº. 2.477/1998) - quem, hoje, pelo Decreto Lei nº. 9.975/2019, tem como função a determinação de políticas quanto a base de dados do SUS determinada no art. 11[9].

9 Art. 11. Ao Departamento de Informática do Sistema Único de Saúde compete: I - fomentar, regulamentar e avaliar as ações de informatização do SUS direcionadas à manutenção e ao desenvolvimento do sistema de informações em saúde e dos sistemas internos de gestão do Ministério da Saúde; II - promover a integração com universidades, com organizações da sociedade civil e com o setor privado por meio da convergência digital no âmbito do SUS; III - fomentar, definir e cumprir as políticas, os procedimentos e as diretrizes de tecnologia da informação e da comunicação para a plena operacionalização dos sistemas de informação em atividade e estabelecer as ações para a segurança da informação; IV - desenvolver, pesquisar e incorporar produtos e serviços de tecnologia da informação que possibilitem a implementação de sistemas e a disseminação de informações para ações de saúde, em consonância com as diretrizes da Política Nacional de Saúde; V - desenvolver, pesquisar e incorporar produtos e serviços de tecnologia da informação e da comunicação para atender às demandas dos sistemas internos de gestão do Ministério da Saúde; VI - manter o acervo das bases de dados necessários ao sistema de informações em saúde e aos sistemas internos de gestão institucional; VII - proporcionar aos gestores do SUS e aos órgãos congêneres o acesso aos serviços de tecnologia da informação e às bases de dados mantidos pelo Ministério da Saúde; VIII - definir programas de cooperação tecnológica com entidades de pesquisa e ensino para prospecção e transferência de tecnologia e metodologia no segmento de tecnologia da informação em saúde; IX - promover estudos de viabilidade de novas tecnologias no uso da inovação com foco em sistemas digitais para o SUS; X - apoiar os Estados, o Distrito Federal e os Municípios na informatização das atividades do SUS; XI - gerenciar a rede lógica do Ministério da Saúde; e XII - promover o atendimento ao usuário de sistemas de informação do Ministério da Saúde.

O DATASUS é hoje o órgão responsável pela implementação da Rede Nacional de Dados em Saúde (RNDS), programa de integralização das informações no sistema de saúde brasileiro, instituído pelo Programa Conecte SUS (Portaria nº. 1.434/2020) que visa a conformidade do tratamento dos dados coletados com a LGPD e Lei de Acesso à Informação[10].

A ideia do RNDS, que logo será melhor abordada, tem por uma das suas finalidades adequar o acesso aos dados sensíveis do cidadão justamente aos princípios básicos da LGPD, permitindo uma maior transparência e um controle mais adequado do compartilhamento destes dados.

Observa-se que a modernização do sistema de conectividade entre as redes utilizadas pela Administração Pública de Saúde é essencial para a garantia da segurança e da privacidade dos dados, devendo ser voltada a um mapeamento e avaliação dos acessos e controle, mas, também, ao uso de novas tecnológicas para garantia da segurança de suas informações e cumprimento das legislações de proteção de dados e demais normas sobre compartilhamento de dados entre os órgãos públicos e, até mesmo particulares.

3. TECNOLOGIA DO SISTEMA DE SAÚDE BRASILEIRO

3.1. Funcionamento do sistema de saúde brasileiro

O Sistema Único de Saúde (SUS), resultado de anos de desenvolvimento, surgiu em 1988, e sempre foi referência mundial na prestação de serviços de saúde, sendo totalmente sem custo a toda a população do Brasil. Baseada em princípios e diretrizes, consegue atender mais de 120 milhões de pessoas por ano, mas embora funcione há mais de 30 anos, ainda não se estabeleceu um sistema totalmente informatizado.

De acordo com os princípios e diretrizes do SUS, os seus serviços são descentralizados, ou seja, organizados em níveis de complexidade, com a

10 "Art. 254-C. O acesso às informações na RNDS observará o disposto na Lei nº. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), e na Lei nº. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI).

redistribuição dos seus serviços e suas responsabilidades aos diversos níveis do governo, ou seja, municipal, estadual e federal. Já a Lei nº. 8.080/90, de 19 de setembro de 1990, regulamenta a participação da iniciativa privada no SUS, em caráter complementar.

Estima-se que 47% dos hospitais do Brasil são públicos, 16% são particulares e 32% são filantrópicos (que exigem no mínimo 60% do seu serviço para pacientes do SUS). Estes hospitais públicos são distribuídos ainda entre os poderes federais, estaduais e municipais. Fica evidente que a própria existência de um sistema descentralizado de saúde como o SUS, composto de diversos hospitais em uma enorme diversidade populacional e econômica de um país tão heterogêneo, traz desafios quanto à sua gestão, organização e controle financeiro. Com cerca de 36% dos gastos dos SUS voltados a hospitais, torna-se difícil calcular os custos do tratamento fora do espectro dos hospitais especializados, como em postos de saúde. Isso se deve ao seu sistema hierárquico de gestão, sendo os gastos maiores do que de países que não utilizam o mesmo método organizacional, segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

3.2. Problemática do atual sistema informacional utilizado pelo SUS

Embora essas leis e diretrizes funcionem teoricamente de forma satisfatória, na prática há um grande problema. Atualmente, na maioria dos serviços, os prontuários dos pacientes, seus exames e histórico de atendimentos geralmente ficam retidos nos hospitais públicos, postos de saúde da família ou clínicas onde foram atendidos. Isso torna o serviço rudimentar, dispendioso e inseguro, correndo-se o risco de informações pessoais serem extraviadas. O paciente não tem acesso livre a suas informações de saúde, assim como os outros médicos, tornando difícil a transferência do cuidado. Quando é necessário prestar contas deste paciente para o setor governamental responsável, em muitos casos, todo o seu prontuário é enviado de forma impressa para a auditoria[11].

11 Informações coletadas a partir de observações feitas pelo autor durante seu trabalho na Unidade de Pronto Atendimento do Vale dos Barris [jul. 2020 - fev. 2021].

A tecnologia e troca de informações entre serviços de saúde fica, frequentemente, limitada a relatórios médicos impressos, telefone e e-mails. No sistema de Regulação, onde ocorrem as transferências de pacientes para gerir as vagas hospitalares e outras necessidades, a situação do paciente precisa diariamente ser impressa pelo médico, que entrega a um funcionário, o qual faz a atualização através de um sistema interno, a fim de que os médicos que trabalham na Regulação tenham acesso para realizar tal transferência[12].

Outro exemplo frequente são o de endemias, doenças e outros casos de notificação compulsória, que utilizam meios rudimentares de comunicação direta. Embora exista essa situação, houve um avanço recente por conta da urgência diante da pandemia do COVID-19, com uma atualização para a notificação de casos suspeitos da doença através de um *website* exclusivo[13].

No mais, há uma vasta falta de informações e comunicação entre esses serviços, prejudicando a eficiência e sucesso no atendimento do paciente por conta de possíveis divergências e falta de informações. Por se tratar de um sistema não integrado, a repetição de exames em intervalos curtos se torna uma constante. Muitos exames são custosos e, às vezes, caem no esquecimento, em que o paciente não vai buscar o resultado e o médico não tem acesso caso queira acessar de outro local, senão o local que realizou o exame[14].

Ao longo de sua vida, um paciente do SUS pode passar por diversas unidades de pronto atendimento, hospitais, postos de saúde e outros locais de serviços de saúde, como clínicas de reabilitação. No entanto, mesmo com tantos atendimentos, não há um sistema digital que integre todos esses locais e forneça os dados essenciais para o melhor entendimento do perfil do paciente e suas afecções. Em muitos casos, o mesmo paciente é atendido por dois, ou até mais hospitais públicos que são necessários para o complemento do seu tratamento, mas os médicos de ambos os hospitais não se comunicam,

12 Ibidem, 2020.

13 BRASIL. Ministério da Saúde. Secretaria de Atenção Especializada à Saúde. Departamento de Atenção Hospitalar, Urgência e Domiciliar. Coordenação Geral de Urgência. Força Nacional do Sistema Único de Saúde. Protocolo de Tratamento do Novo Coronavírus (2019-nCoV). Brasília, DF: MS, 2020. p.31.

14 Informações coletadas a partir de observações feitas pelo autor durante seu trabalho na Unidade de Pronto Atendimento do Vale dos Barris [jul. 2020 - fev. 2021].

nem tem acesso a um prontuário unificado, ficando dependentes de relatórios médicos e histórias que podem omitir fatores essenciais e, em alguns casos, serem ilegíveis caso manuscritos[15].

Além disso, parte dos profissionais de saúde passam por dificuldades quanto ao uso desses sistemas não integrados, necessitando de treinamento para o uso correto do sistema de prontuários e atendimentos para cada nova unidade de saúde em que se encontram, pois os programas são diferentes e isso torna o serviço passível de erros e menos efetivo. Ademais, na maioria das unidades hospitalares, se utilizam sistemas nada intuitivos, que prejudicam na eficiência de registros dos profissionais nos prontuários[16].

Um dos principais quesitos que prejudicam a gestão em Saúde em um sistema não informatizado e não integrado é que não há como traçar um perfil epidemiológico das doenças de forma efetiva. Um paciente pode ser registrado, por exemplo, como hipertenso em uma unidade e não ser registrado em outra, e isso pode causar vieses em dados, como falta ou duplicidade, o que prejudica a tomada de decisões dos gestores quanto às ações de saúde de uma cidade ou bairro específico e a coleta de dados para pesquisas científicas, podendo ser até fatal[17].

3.2.1. Desvantagens do uso de um sistema Centralizado de Armazenamento

Não há dúvidas, também, que um sistema informatizado centralizado do SUS já trouxe diversas falhas. Vários casos graves de vazamento de dados ocorreram no SUS nos últimos anos, a exemplo dos 2,4 milhões de dados de usuários vazados em 2019 e os milhões não especificados, causados por falhas de segurança do aplicativo E-Saúde, em 2016[18].

15 Ibidem, 2020.
16 Ibidem, 2020.
17 Ibidem, 2020.
18 SUTTO, Giovanna. **Dados pessoais de 2,4 milhões de usuários do SUS vazam na internet**, 11 abr. 2019. Disponível em: <https://www.infomoney.com.br/consumo/dados-pessoais-de-24-milhoes-de-usuarios-dos-sus-vazam-na-internet/>. Acesso em: 2 jul. 2020.

No mais, em dezembro de 2020, uma falha do Ministério da Saúde expôs dados de mais de 200 milhões de brasileiros na internet, evidenciando ainda mais a fragilidade do sistema de saúde[19].

O serviço de prontuário centralizado tem várias desvantagens. Primeiro, os dados são confiados a um só local, controlado por pessoas. O modelo atual de dados de prontuários é administrado por uma autoridade centralizada, e as informações dos usuários acabam sendo guardados por essas autoridades. Vazamentos de informações, vendas, roubos e outros eventos ficam susceptíveis de ocorrerem. Além disso, o serviço centralizado pode sofrer múltiplos ataques se houver um único ponto de falha, portanto, o sistema provedor necessita ser perfeitamente construído e protegido para garantir segurança e estabilidade operacional. No momento que o servidor centralizado falhar, todo o sistema se torna vulnerável a ataques. O potencial ataque de criminosos podem incluir desde ataques de Negação de Serviços (DDoS), ataques de canal lateral, ataques de autenticação, entre outros. Terceiro, os dados do prontuário podem ser deletados e modificados facilmente.

De forma ideal, um prontuário eletrônico deve ser mantido em um local seguro e incapaz de ser deletado e alterado, onde mesmo os detentores dos dados não podem modificá-los. Os dados do prontuário refletem as condições que acometem os pacientes e descrições de exames. Se os dados forem modificados, o verdadeiro perfil do paciente fica alterado, guiando o médico a ações imprevisíveis e possivelmente irreversíveis.

Sabe-se que há anos é tentado realizar melhorias no quesito da integralização dos dados do SUS. Atualmente, está sendo desenvolvida a Rede Nacional de Dados de Saúde (RNDS), anunciada em outubro de 2019, que consiste em compartilhar dados através da nuvem e utilizando a tecnologia *Blockchain*. Certamente, esses métodos aumentariam a segurança e trariam

19 Segundo o site G1: "CPF, nome completo, endereço e telefone estão entre os dados vazados. Esse conteúdo veio de qualquer brasileiro cadastrado no Sistema Único de Saúde (SUS) ou em plano de saúde." G1. Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml>. Acesso em: 22 Dez. 2020.

uma integração importante para esse sistema tão necessário para milhões de brasileiros. Avanços na tecnologia da saúde permitem que a população seja tratada melhor, fornecendo mais qualidade de vida, além de incontáveis vidas sendo salvas e gastos sendo efetivamente reduzidos.

É evidente a quantidade de falhas que podem ser corrigidas para ampliar o atendimento e eficiência do SUS. Segurança frágil, falta de integração de sistemas, ausência de uniformização do prontuário e falta de comunicação entre os profissionais, prejudicando o tratamento multidisciplinar, são apenas alguns dos fatores que utilizando tecnologias como *Blockchain* e IPFS seria uma eficiente solução.

4. USO DA TECNOLOGIA *BLOCKCHAIN* E IPFS PARA A MODERNIZAÇÃO DO SISTEMA NA REDE DE SAÚDE

A tecnologia *Blockchain* começou a ganhar fama em 2008, quando foi introduzida na criptomoeda *Bitcoin*. O *Bitcoin*, com cerca de 500 milhões de transações concluídas (30 de junho, 2020)[20], representa um sólido caso de que o *Blockchain* funciona. Conforme esta tecnologia foi se popularizando, percebeu-se que qualquer formato de informação poderia ser registrado em *Blockchain*, permitindo que este sistema ofereça benefícios em outros campos além do setor financeiro, incluindo a saúde.

Espera-se que o *Blockchain* revolucione a indústria e o comércio, impulsionando transformações em vários setores em escala global, permitindo soluções seguras, rápidas, confiáveis e transparentes que podem ser públicas ou privadas. A tecnologia tem a capacidade de revolucionar o setor de saúde, melhorar as cadeias de suprimentos de medicamentos, e possivelmente desestimular comportamentos antiéticos e fraudulentos na indústria de saúde.

O *Blockchain* permite a descentralização de informações de forma segura, sendo uma plataforma alternativa ideal para o sistema centralizado que é utilizado pelo SUS na atualidade. O *InterPlanetary File System* (IPFS) é um

20 Número total de transações. Disponível em: <https://www.blockchain.com/charts/n-transactions-total>. Acesso em: 02 jul. 2020.

sistema distribuído ponto a ponto que fornece espaço de armazenamento e torna os dados sincronizados entre todos os nós, removendo arquivos duplicados.

A estrutura proposta preserva a privacidade do paciente e facilita o acesso simplificado a dados médicos por entidades autorizadas, como profissionais de saúde aos órgãos oficiais de saúde. Além disso, o sistema proposto alcança consistência, integridade e segurança necessários ao Sistema Único de Saúde Brasileiro.

4.1. Fundamentos do *Blockchain*

A rede *Blockchain* é uma tecnologia que funciona como um livro eletrônico público, construído em torno de um sistema P2P (do inglês *peer-to-peer*, que significa par-a-par). Seu nome (Cadeia de blocos) se deve à maneira como o sistema funciona e armazena transações. A cada transação, as informações pertinentes são inseridas em blocos, que se vinculam para formar uma cadeia com outros blocos de informações semelhantes (UNDERWOOD, 2016).

Quando um usuário deseja adicionar uma transação ao sistema, os dados de transação são encriptados e verificados por outros computadores na rede, usando algoritmos criptográficos. Se houver consenso entre a maioria dos computadores de que a transação é válida, um novo bloco de dados é adicionado à cadeia e compartilhado por todos na rede. Assim, todos os dados que entram no *Blockchain* são interconectados e nunca podem ser excluídos ou alterados, ficando armazenados para sempre, o que faz com que as informações registradas no sistema sejam seguras, confiáveis, auditáveis e imutáveis. Falsificar uma única informação significaria falsificar toda a cadeia com milhões de blocos, o que é virtualmente impossível (UNDERWOOD, 2016).

Um dos conceitos mais importantes na tecnologia *Blockchain* é a descentralização. Nenhum computador ou organização pode ser o dono da cadeia. Em vez disso, é um livro distribuído por meio dos nós conectados à

cadeia, com inúmeras testemunhas para cada transação. Seu sistema foi projetado para construir um mecanismo de relacionamentos sem ter que confiar em um terceiro elemento, excluindo a necessidade de um intermediário para validar a operação. A combinação de informações públicas com um sistema de freios e contrapesos ajuda o *Blockchain* a manter a integridade e criar confiança entre os usuários. Esse é o mesmo objetivo perseguido pelos sistemas legais - regular as relações em uma sociedade que consiste em elementos inerentemente não confiáveis - as pessoas (UNDERWOOD, 2016).

Michael Versace, diretor global de pesquisa para estratégias digitais da empresa de IDC, declarou o seguinte: "As principais capacidades da terceira plataforma de tecnologia estão além de qualquer outra que já vimos antes. A tecnologia *Blockchain* significa que podemos alcançar resultados de valor tecnológico que não poderíamos alcançar antes"[21].

Outra grande vantagem da tecnologia *Blockchain* é a capacidade de um desenvolvedor ou empresa personalizá-la. Isso significa que um *Blockchain* pode ser completamente aberto ao público, a exemplo da *Bitcoin*, permitindo que qualquer pessoa participe, ou pode ser totalmente privada, com apenas certas pessoas autorizadas a acessar os dados, ou autorizadas a realizar transações.

4.2. Fundamentos do IPFS

O IPFS (*InterPlanetary File System* – Sistema Interplanetário de arquivos) é um protocolo construído para criar uma forma permanente e descentralizada de armazenar e compartilhar arquivos. Todos os nós estão em uma rede distribuída P2P e, portanto, formam um sistema de arquivos distribuídos[22].

Em vez de usar um endereço de localização comum, como o HTTP, o IPFS cria um código único para o arquivo, chamado *hash*, para depois

21 FINANCIALBUZZ. ***The Increased Popularity of Blockchain Technology in Various Sectors***. [S. l.], 2018. Disponível em: https://www.prnewswire.com/news-releases/the-increased-popularity-of-blockchain-technology-in-various-sectors-885208900.html. Acesso em: 4 jul. 2020.

22 Informação coletada diretamente no site do IPFS. IPFS (org.). **IPFS concepts**, 17 jun. 2020. Disponível em: https://docs.ipfs.io/concepts/. Acesso em: 7 jul. 2020.

armazenar vários pedaços desse arquivo em locais diferentes (por isso, o nome armazenamento descentralizado). Quando o usuário quer acessar o arquivo, seu próprio *hash* é usado na localização. O *hash* representa um objeto raiz, e outros objetos podem ser encontrados seguindo sua matriz. Desta forma, em vez de falar com um servidor, você ganha acesso a esse "ponto de partida" dos dados do arquivo. Isso significa que, quando os dados mudam, ele é representado por um identificador diferente (*hash*), mas a versão antiga dos dados ainda existe, inalterada, criando um controle de versão e remoção de duplicidade (KWATRA, 2018).

No mais, o sistema aproveita a proximidade física para resgatar determinado arquivo, de modo que se alguém muito próximo do computador que requisitou o arquivo tem o documento, este será obtido diretamente desta pessoa em vez de se conectar a um servidor central (KWATRA, 2018).

4.3. Funcionamento da tecnologia

O setor de saúde gera grandes volumes de documentos médicos que precisam ser armazenados, compartilhados e acessados diariamente. Por exemplo, dados médicos são criados quando um paciente é submetido a exames, como tomografia computadorizada, ressonância magnética, radiografia e exames laboratoriais. Outra fonte desses dados é quando um médico registra informações do paciente em um prontuário.

As informações médicas de um paciente devem ser armazenadas de tal maneira que sejam acessíveis pelos médicos em outros hospitais dentro da rede do SUS quando houver necessidade. No entanto, essas informações, por terem caráter sensível, devem ser mantidas em sigilo. Além disso, os arquivos armazenados no sistema devem ser imutáveis, a fim de garantir segurança e inviolabilidade. A exigência de um processo transparente para armazenar registros médicos requer uma estrutura em que os dados possam ser facilmente mantidos e acessados.

Hoje, uma razão pela qual os registros não podem ser compartilhados é por causa dos múltiplos sistemas, bancos de dados e formatos em que as

informações médicas são armazenadas. Uma abordagem P2P no setor de saúde nos aproximaria de um prontuário médico unificado — acessível por sistemas heterogêneos.

A tecnologia *Blockchain* fornece um sistema de registro descentralizado, no qual o prontuário médico de um paciente (relatório, diagnóstico, informações pessoais do paciente, prescrição médica e assim por diante) pode ser compartilhado facilmente entre os profissionais de saúde (hospitais ou médicos) dentro de um sistema totalmente integralizado e unificado. Detalhes dos registros médicos de um paciente, incluindo doenças passadas e atuais podem ser armazenados na rede *Blockchain*, fazendo com que todos os registros sejam transferíveis, permanentes e facilmente acessíveis por usuários autorizados.

A tecnologia permite que a privacidade e segurança dos dados seja mantida, com fácil acessibilidade a dados pelo paciente, médico, sistemas de saúde, farmácias e governo. Utilizando o sistema proposto, o próprio paciente é capaz de ter acesso ao seu prontuário médico de forma fácil e segura, podendo acessar seus exames, seus relatórios médicos e inclusive adquirir os receituários que forem liberados pelo profissional médico.

O profissional médico também poderá visualizar o prontuário do paciente em outra unidade hospitalar com o seu acesso registrado, podendo dar continuidade ao seu trabalho, acessando exames e planejando o tratamento contínuo sem arriscar que esses dados sejam perdidos ou acessados e alterados por outra pessoa. Evita-se, ademais, a necessidade de impressão excessiva de papéis para a efetiva comunicação entre as unidades, muitas vezes passíveis de erros e rasuras, agilizando assim o processo de regulações, cirurgias e atendimentos.

4.3.1. Armazenamento Descentralizado e o uso do IPFS

No entanto, para manter esse grande volume de prontuários, há a necessidade de um sistema de distribuição e armazenamento com uma estrutura P2P, uma vez que o *Blockchain* não foi inicialmente projetado para

armazenar uma grande quantidade de data. Armazenar um único prontuário médico em *Blockchain* seria extremamente lento e custoso, o que inviabilizaria o sistema. É aí que entra a solução de aliar o IPFS ao *Blockchain*, a fim de que os documentos sejam armazenados em IPFS e a *hash* gerada seja registrada em *Blockchain*.

O IPFS fornece uma estrutura de armazenamento distribuída P2P, em que os prontuários médicos podem ser facilmente armazenados e compartilhados. O IPFS armazena o conteúdo, gerando uma *hash* para o arquivo, enquanto remove duplicidades no sistema usando o histórico de controle de versão. Desta forma, os profissionais de saúde conseguiriam mapear as mudanças no prontuário do paciente, bem como adicionar informações sem perder o arquivo original.

A vantagem de utilizar o IPFS, e não um sistema convencional de armazenamento centralizado, é que o IPFS não possui um ponto único de falha, já que o arquivo é distribuído para vários nós na rede. Já no sistema centralizado, um possível vazamento de informações torna-se mais fácil, pois é apenas um servidor controlando toda a informação.

No mais, por sua natureza, os arquivos distribuídos em P2P não pode ser afetado por ataques de estilo "Negação direta de Serviço" (DDoS). Esses ataques são focados em bombardear servidores para derrubar sites ou serviços. No entanto, se o mesmo conteúdo está armazenado em vários pares, um ataque DDoS eficaz teria que encontrar e atingir pelo menos metade mais um dos nós do sistema, o que é virtualmente impossível[23].

4.3.2. Da segurança do sistema proposto

Como o IPFS é um protocolo aberto de armazenamento descentralizado, todo indivíduo que possua a *hash* do arquivo poderá ter acesso ao documento. Assim, arquivos sensíveis, como prontuários médicos, não são adequados para serem diretamente armazenados no IPFS.

23 Informação coletada diretamente no site do Cloudfare. CLOUDFARE (Brasil). **O que é ataque de DDoS?**, 2020. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/. Acesso em: 7 jul. 2020.

Para tornar os registros médicos privados, a fim de que apenas os autorizados tenham acesso a ele, é necessário utilizar alguma forma de criptografia antes de armazenar o arquivo. A fim de solucionar esta questão, propomos o uso da criptografia assimétrica OpenPGP (*Pretty Good Privacy*- "Privacidade bastante boa" em português), que nos permite criptografar um arquivo com a chave pública do destinatário pretendido para que só eles possam descriptografá-lo quando o recuperarem com o IPFS. Desta forma, uma parte maliciosa que recupera o arquivo do IPFS não pode fazer nada com ele, já que não pode descriptografá-lo[24].

4.4. Adequação com a LGPD

O sistema proposto deve se adequar à LGPD, uma vez que, conforme já anteriormente exposto, o SUS é abarcado pela lei e deve cumprir com suas exigências.

Um dos principais pontos trazidos pela legislação mencionada é a atenção à segurança das informações armazenadas, trazendo a seguinte redação:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão[25].

Por certo, um dos maiores desafios no sistema utilizado pelo SUS é garantir que as informações armazenadas no sistema possuam um caráter inviolável, à prova de falhas e vazamentos. Conforme previamente aduzido, o Sistema Único de Saúde, por armazenar uma grande quantidade de dados pessoais sensíveis, acaba se tornando alvo de quadrilhas especializadas em ataques cibernéticos. As principais formas de ataque são os que envolvem

24 GNUPG. ***The GNU Privacy Guard***. [S. l.], 2020. Disponível em: https://www.gnupg.org/. Acesso em: 7 jul. 2020.

25 BRASIL. Subchefia para Assuntos Jurídicos. **LEI Nº 13.709**: Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 24 jul. 2020.

sequestro de dados, aliado a crimes de extorsão (*ransomware*). No mais, pela carência de um armazenamento seguro e descentralizado, o SUS também sofre com perda de informações no seu banco de dados, seja por falha humana ou por problemas no sistema de armazenamento interno.

Outra inovação que a LGPD trouxe é que os dados dos pacientes só poderão ser coletados e registrados no sistema se existir uma autorização expressa deles, salvo algumas exceções. Essa regra abarcará tanto para novos dados cadastrados em prontuários, como os antigos que já se encontram no sistema.

Hoje, o sistema utilizado pelo SUS não disponibiliza ao paciente acesso às suas informações. No mais, como o SUS não possui um sistema completamente integralizado, informações e documentações do mesmo paciente podem existir em duplicidade ou de forma fragmentada em vários sistemas. Nos deparamos então com uma demanda urgente por um sistema que permita acesso direto do paciente aos seus dados médicos, a fim de que os pacientes passem a acessar, rastrear e controlar seus registros de saúde.

O sistema proposto neste artigo eliminaria o problema de segurança quase por completo, uma vez que o método traz a integralidade do IPFS, eliminando um órgão central de armazenamento, bem como a utilização de criptografia de chave *Blockchain* para registros de saúde, permitindo, ainda, que computadores de diversas redes do sistema tenham acesso às informações. No mais, os arquivos armazenados no sistema somente seriam acessíveis pelo próprio paciente ou por profissionais e entidades autorizadas, mantendo a camada necessária de segurança de dados sensíveis. Adicionalmente, como o sistema de armazenamento utilizado é o IPFS, o paciente poderá ter fácil acesso ao seu prontuário médico de qualquer lugar do mundo, e em tempo real.

Desta forma, a proposta traz solução para os seguintes pontos: (i) a segurança e a privacidade das informações dos pacientes, (ii) a falta de confiança entre os órgãos intermediários e (iii) incentivar a escalabilidade da interoperabilidade em saúde, mostrando-se uma solução simples e econômica para o SUS ficar em acordo com a LGPD.

5. CONCLUSÃO

O Sistema Único de Saúde apresenta falhas de segurança, não é devidamente integralizado e não possui a eficiência requerida pelo ordenamento jurídico brasileiro. A implementação de um sistema integralizado e ao mesmo tempo descentralizado pode fornecer as funcionalidades e preencher as lacunas que faltam para que o SUS seja um sistema informatizado, efetivo, econômico e simplificado. Desta forma, a proposta compensa os esforços realizados, inclusive na adequação do tratamento dos dados pessoais de acordo com a LGPD e demais leis que versem sobre compartilhamento, acesso e armazenamento das informações coletadas.

Este artigo propõe a utilização de tecnologia *Blockchain* no sistema de saúde, armazenando os dados de prontuários médicos com segurança em ambiente distribuído, o que é diferente do esquema existente de armazenamento centralizado. Adotando a tríade de IPFS, *Blockchain* e *OpenPGP* e incorporando estes elementos em uma plataforma responsiva e de fácil utilização, seria possível otimizar o sistema de saúde brasileiro, tornando-o mais transparente, seguro e integralizado.

Usando esta solução, o sistema do SUS pode ser melhorado usando a forte segurança da tecnologia *Blockchain*, que oferece uma solução tecnológica superior, mais econômica, e ainda assim eficaz. Os pacientes terão acesso e controle sobre seus dados, melhorando assim a segurança de suas informações. O sistema também poderá ser utilizado para reduzir a necessidade de intermediários para realizar o registro dos dados do paciente. Isso diminuirá os problemas dos atuais sistemas de Registro Eletrônico de Saúde, como fragmentação de dados, vazamentos e acesso não autorizado às informações do paciente.

REFERÊNCIAS

BOTEGA. Laura de Almeida. ANDRADE, Mônica Viegas. GUEDES, Gilvan Ramalho. **Brazilian hospitals' performance: an assessment of the unified health system (SUS).** Health Care Manag Sci (2020). Disponível em: https://doi.org/10.1007/s10729-020-09505-5. Acesso em: 7 jul. 2020.

BRASIL. **Portaria nº 1.434 de maio de 2020**. Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/ GM/MS. Disponível em: https://rnds.saude.gov.br/legislacao/. Acesso em: 21 jun. 2020.

BRASIL. **Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e Funções Gratificadas do Ministério da Saúde, e dá outras providências**. Decreto nº 2.477, de 28 de janeiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D2477impressao.htm. Acesso em: 25 jun. 2020

BRASIL. Datasus. **Ações para a Adequação da RNDS à Lei Geral de Proteção de Dados. Junho de 2020.** Disponível em: 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. Acesso em: 20 jun. 2020.

BRASIL. **A governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 5 jul. 2020.

BRASIL. **Lei Geral de Proteção de dados**. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 jun. 2020.

BRASIL. **Lei de Acesso à Informação. Lei nº 12.527, de 18 de novembro de 2011.** disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 7 jun. 2020.

BRASIL. Ministério da saúde. **A RNDS**. [S. l.], 2020. Disponível em: https://rnds.saude.gov.br. Acesso em: 2 jul. 2020.

CHAN. Helen. **Pervasive personal data collection at the heart of South Korea's covid-19 sucess may not translate**. Data Privacy. 26 de março de 2020. Disponível em: https://blogs.thomsonreuters.com/answerson/south-korea-covid-19-data-privacy/. Acesso em: 1 jun. 2020.

CLOUDFARE. **O que é ataque de DDoS?**, 2020. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/. Acesso em: 7 jul. 2020.

COREIA DO SUL. Personal Information Protection Act. Ato nº 1065 de 29 de março de 2011. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=1. Acesso em: 15 jun. 2020.

FEDERAÇÃO NACIONAL DE FARMACÊUTICOS. **Vazamento de dados do E-Saúde expõe informações de milhões de brasileiros.** [S. l.], 6 fev. 2018. Disponível em: https://www.fenafar.org.br/2016-01-26-09-32-20/saude/1992-vazamento-de-dados-do-e-saude-expoe-informacoes-de-milhoes-de-brasileiros. Acesso em: 6 jul. 2020.

FINANCIALBUZZ. **The Increased Popularity of Blockchain Technology in Various Sectors**, 2018. Disponível em: https://www.prnewswire.com/news-releases/the-increased-popularity-of-blockchain-technology-in-various-sectors-885208900.html. Acesso em: 4 jul. 2020.

G1. **Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet**. Disponível em https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 22 dez. 2020.

GNUPG. **The GNU Privacy Guard**, 2020. Disponível em: https://www.gnupg.org/. Acesso em: 7 jul. 2020.

GUTIERREZ, Tereza de Sousa (Coord.). **LGPD na Saúde**. Disponível em: https://lgpdesaude.com.br/. Acesso em 26 jun. 2020.

HALPIN, Harry; PIEKARSKA, Marta. **Introduction to Security and Privacy on the Blockchain**. 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2017. Disponível em: https://ieeexplore.ieee.org/abstract/document/7966963. Acesso em: 22 dez. 2020.

IPFS (org.). **IPFS concepts**, 17 jun. 2020. Disponível em: https://docs.ipfs.io/concepts/. Acesso em: 7 jul. 2020.

LESSA, Fábio José Delgado; MENDES, Antônio da Cruz Gouveia; FARIAS, Sidney Feitosa et al. **Novas metodologias para vigilância epidemiológica: uso do Sistema de Informações Hospitalares – SIH/SUS**. Informe Epidemiológico do SUS, Brasília, v. 9, 2000, Disponível em: scielo.iec.gov.br/pdf/iesus/v9s1/v9s1a01.pdf. Acesso em: 30 jun. 2020.

KWATRA, Karan. **What is IPFS?**, 14 mar. 2018. Disponível em: https://medium.com/wolverineblockchain/what-is-ipfs-b83277597da5. Acesso em: 5 jul. 2020.

MALDONADO, Viviane Nóbrega (Coord.). BLUM, Renato Opice (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada.** Thomson Reuter Brasil. 2019. Edição ebook.

MENDES, Gilmar Ferreira (Coord.). SALERT, Ingo Wolfgang (Coord.). **Direito, Inovação e Tecnologia** Volume 1. Saraiva. 2017. Edição Kindle.

METTLER, Matthias. **Blockchain technology in healthcare: The revolution starts here. In: 2016 IEEE 18th international conference on e-health networking, applications and services** (Healthcom). IEEE, 2016.

MICHAELIS. 2020. Disponível em: http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=PANDEMIA.

MINISTÉRIO DA SAÚDE. Secretaria de Atenção Especializada à Saúde. Departamento de Atenção Hospitalar, Urgência e Domiciliar. Coordenação Geral de Urgência. Força Nacional do Sistema Único de Saúde. **Protocolo de Tratamento do Novo Coronavírus (2019-nCoV).** Brasília, DF: MS, 2020. Disponível em: https://www.saude.gov.br/images/pdf/2020/April/05/Protocolo-de-Manejo-Cl—nico-para-o-Covid-19.pdf. Acesso em: 7 jul. 2020.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

NAZ, Muqaddas. ALZAHRANI, Fahad. KHALID, Rabiya. JAVAID, Nadeem. QAMAR, Ali. AFZAL, Muhammad. SHAFIQ, Muhammad. (2019). **A Secure Data Sharing Platform using Blockchain and IPFS.** Sustainability. 11. 10.3390/su11247054. Disponível em: https://www.researchgate.net/publication/337712447_A_Secure_Data_Sharing_Platform_using_Blockchain_and_IPFS. Acesso em: 1 jul. 2020.

PADRÃO, Márcio. **Dados pessoais de 2,4 milhões de usuários do SUS são vazados na internet**. In: Dados pessoais de 2,4 milhões de usuários do SUS são vazados na internet. [S. l.], 11 abr. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/04/11/dados-pessoais-de-24-milhoes-de-usuarios-do-sus-sao-vazados-na-internet.htm. Acesso em: 6 jul. 2020.

SCATENA. TANAKA. **Utilização do Sistema de Informações Hospitalares (SIH-SUS) e do Sistema de Informações Ambulatoriais (SIA-SUS) na análise da descentralização da saúde em Mato Grosso**. Inf epidemiol SUS. 2001;10(1). Disponível em: scielo.iec.gov.br/pdf/iesus/v10n1/v10n1a03.pdf. Acesso em: 2 jul. 2020.

UNDERWOOD, Sarah. (2016). **Blockchain beyond bitcoin.** Communications of the ACM, 2016.

WU, Xuguang; HAN, Yiliang; ZHANG, Minqing; ZHU, Shuaishuai. **Secure Personal Health Records Sharing Based on Blockchain and IPFS.** Chinese Conference on Trusted Computing and Information Security, [S. l.], p. 340-354, 20 fev. 2020. Disponível em: https://link.springer.com/chapter/10.1007/978-981-15-3418-8_22. Acesso em: 5 jul. 2020.

SUBMETIDO | *SUBMITTED* **|** 04/01/2021
APROVADO | *APPROVED* **|** 10/03/2021

REVISÃO DE LÍNGUA | *LANGUAGE REVIEW* **|** Anna Luiza Ferrari

SOBRE OS AUTORES | *ABOUT THE AUTHORS*

CAROLINE CASTRO NUNES
Mestra em Direito de Entretenimento pela University of Southern California, Estados Unidos. Especialista em Direito Processual Civil pela Faculdade Baiana de Direito. Fundadora da InspireIP. E-mail: caroline.nunes.2020@lawmail.usc.edu. ORCID: https://orcid.org/0000-0002-3898-1815.

STEPHANE MA
Pós-graduanda em Direito Empresarial pela Fundação Getúlio Vargas. Advogada. E-mail: stephane.ma@hotmail.com. ORCID: https://orcid.org/0000-0002-4218-398X.

MARCELO SILVEIRA TEIXEIRA FILHO
Médico graduado pela Universidade Salvador. R3 no programa de residência em Ortopedia no Hospital Santo Antônio. E-mail: marcelostfilho@gmail.com. ORCID: https://orcid.org/0000-0001-8887-9803