ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Internet das Coisas e *blockchain* no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados

Internet of Things and blockchain used in the Brazilian Unified Health System: how to protect sensitive data considering the imminence of the Data Protection Law

Internet de las cosas y cadena de bloques utilizado en el Sistema Único de Salud brasileño: cómo proteger los datos confidenciales ante la Ley General de Protección de Datos

Maria Amália Arruda Camara[1]
Gabriel Henrique Albuquerque Lins[2]
Fábio Henrique Cavalcanti de Oliveira[3]
Evellyn Millene Alves Camelo[4]
Nataly Regina Fonseca Carvalho de Medeiros[5]

Resumo

Objetivo: O Sistema Único de Saúde (SUS) vem investido nas tecnologias da internet das coisas – *Internet of Things* (IoT), em inglês – para coletar dados dos pacientes. Esse artigo aponta as fragilidades quanto à privacidade de usuários do SUS e propor uma solução teórica, ainda a ser testada a partir de uma infraestrutura pautada em armazenamento pessoal de dados – *personal data stores* (PDS), em inglês – ou, a partir da segurança da *blockchain*. **Metodologia:** realizou-se revisão narrativa da literatura nacional e internacional relacionados a instrumentos, políticas e casos voltados a tecnologias de informação e comunicação na saúde a fim de apontar as fragilidades quanto à privacidade de usuários desse sistema. **Resultados:** percebeu-se que ainda existe uma falta de transparência no tratamento dos dados pessoais e pouco *accountability* por parte dos cidadãos, se fazendo necessária uma mudança de estratégia tecnológica e de governança. **Conclusão:** o PDS, de fato, empodera o usuário na medida que dá maior controle e transparência sobre o tratamento de seus dados. No entanto, essa solução, em um sistema como o utilizado pelo Departamento de Informática do SUS, pode comprometer a precisão dos dados usados nas políticas públicas, ao mesmo tempo que pode comprometer alguns direitos dos cidadãos, pois são dados salvos em registros e os metadados estão disponíveis publicamente. A implementação do PDS ainda não possui perspectiva de resultado ótimo. Ainda existem algumas restrições metodológicas quanto aos direitos dos cidadãos ou à eficiência do Estado, mas é um passo no empoderamento civil e uma melhoria exigida por lei quanto à privacidade e à proteção de dados pessoais.

[1] Doutora em Ciência Política, Universidade Federal de Pernambuco, Recife, Pernambuco, Brasil; professora adjunta, Universidade de Pernambuco, Recife, Pernambuco, Brasil. https://orcid.org/0000-0002-7663-3029. E-mail: amalia.camara@upe.br
[2] Mestrando em Neuroengenharia, Instituto Internacional de Neurociências Edmond e Lily Safra, Instituto Santos Dumont, Macaíba, Rio Grande do Norte, Brasil. https://orcid.org/0000-0003-3208-3720. E-mail: gabrielh.lins@outlook.com
[3] Mestre em Inovação Terapêutica, Universidade Federal de Pernambuco, Recife, Pernambuco, Brasil; professor assistente, Universidade de Pernambuco, Recife, Pernambuco, Brasil. https://orcid.org/0000-0002-0181-7624. E-mail: fabiohcavalcanti@upe.br
[4] Graduanda em Fonoaudiologia, Centro Universitário São Miguel, Recife, Pernambuco, Brasil. https://orcid.org/0000-0002-8810-6920. E-mail: evellynmillenea@gmail.com
[5] Graduanda em Medicina, Centro Universitário Maurício de Nassau, Recife, Pernambuco, Brasil. https://orcid.org/0000-0003-4415-395X. E-mail: natalyreg@gmail.com

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Palavras-chave
Blockchain. Privacidade. *Big data*. Sistema Único de Saúde. Confidencialidade.

Abstract
Objective: Brazilian Unified Health System (SUS, in Portuguese) has invested in Internet of Things (IoT) technologies to collect data from patients. This article aims to point out the weaknesses regarding the privacy of users of the SUS and to propose a theoretical solution, yet to be evaluated, and based on a Personal Data Storages (PDS) infrastructure or on blockchain security. **Methods:** aA narrative review of national and international literature related to instruments, policies, and cases related to information and communication technologies in health was conducted to point out the weaknesses regarding the privacy of users of this system. **Results:** there is still a lack of transparency in the treatment of personal data and little accountability on the part of citizens, making it necessary to change the technological and governance strategy. **Conclusion:** PDS empowers users as it gives greater control and transparency over the treatment of data. However, this solution, in a system like the one used by their Computer Department, can compromise the accuracy of the data used in public policies, while it can compromise some citizens' rights, as this data is saved in records and the metadata is publicly available. The implementation of a solution like this does not yet have the prospect of an optimal result, without any methodological restriction on citizens' rights or the efficiency of the State, but it is a step in civil empowerment and an improvement required by law concerning privacy and protection of personal data. The implementation of the PDS does not yet have the prospect of an optimal result. There are still methodological restrictions regarding the rights of citizens or the efficiency of the State. But it is a step in civil empowerment and an improvement required by law in terms of privacy and the protection of personal data.
Keywords
Blockchain. Privacy. Big data. Unified Health System. Confidentiality.

Resumen
Objetivo: el Sistema Único de Salud de Brasil (SUS) ha invertido en tecnologías de Internet de las cosas (IoT) para recopilar datos de los pacientes. Este artículo tiene como objetivo señalar las debilidades con respecto a la privacidad de los usuarios del SUS y proponer una solución teórica, aún por probar basada en una infraestructura basada en Personal Data Storages (PDS) o almacenamiento personal de datos, basado en la seguridad de *blockchain*. **Metodología:** se realizó una revisión narrativa de la literatura nacional e internacional relacionada con instrumentos, políticas y casos relacionados con las tecnologías de la información y la comunicación en salud con el fin de señalar las debilidades en cuanto a la privacidad de los usuarios de este sistema. **Resultados:** se notó, entonces, que aún existe falta de transparencia en el tratamiento de estos datos personales y poca rendición de cuentas por parte de la ciudadanía, por lo que es necesario cambiar la estrategia tecnológica y de gobernanza. **Conclusión:** se concluye que PDS, de hecho, empodera a los usuarios ya que brinda un mayor control y transparencia sobre el tratamiento de sus datos. Sin embargo, esta solución, en un sistema como el utilizado por el Departamento de Computación del SUS, puede comprometer la precisión de los datos utilizados en las políticas públicas, al mismo tiempo que puede comprometer algunos derechos civiles, ya que estos datos se guardan en registros y metadatos están disponibles públicamente. La implementación de una solución como esta todavía no tiene la perspectiva de un resultado óptimo, sin ninguna restricción metodológica sobre los derechos de los ciudadanos o la eficiencia del Estado, pero es un paso en el empoderamiento civil y una mejora requerida

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

por la ley con respecto a la privacidad y protección de datos personales. La implementación del PDS aún no tiene la perspectiva de un resultado óptimo. Aún existen algunas restricciones metodológicas en cuanto a los derechos de los ciudadanos o la eficiencia del Estado. Pero es un paso en el empoderamiento civil y una mejora requerida por la ley en términos de privacidad y protección de datos personales.

Palabras clave
Cadena de bloques. Privacidad. Macrodatos. Sistema Único de Salud. Confidencialidad.

Introdução

Este estudo traz uma discussão específica a respeito das tecnologias da internet das coisas – *Internet of Things* (IoT), em inglês, no Sistema Único de Saúde (SUS) no Brasil e como são coletados e tratados os dados dos usuários dessas tecnologias. Considerando que o tema traz uma interface da Ciência, Tecnologia e Inovação em Saúde (CT&I/S) com o Sistema de Informação em Saúde (SIS), bem como o fato dessa interface configurar um componente importante para os setores econômico e social do país, para o alcance do objetivo almejado neste estudo, tipifica-se os temas nesta introdução em função dos textos normativos encontrados nas políticas públicas de saúde (1).

Na busca pela compreensão da Ciência, Tecnologia e Inovação em Saúde, põe-se a inovação em saúde como área de interesse que, como dito por Marge Tenório e demais autores, envolve um campo de estudos de excelência, uma vez que possui a capacidade de mobilizar uma infraestrutura de CT&I/S articulada com a base industrial, além de promover a sua consolidação (1).

O caráter conceitual da inovação na saúde vem de um arcabouço legal e governamental situado na Política Nacional de Saúde, associado à concepção do que é a Ciência, Tecnologia e Inovação em Saúde (CT&I/S), e como o Estado percebe esse tema nas deliberações de suas políticas públicas (1). No Brasil, a instituicionalização da CT&I/S se dá pela criação da Secretaria de Ciência e Tecnologia no Ministério da Saúde, em 2003, depois denominada de Secretaria de Ciência Tecnologia e Inovação em Saúde (SCTIE) (1). É a partir dessa secretaria que há propositura de Agendas Nacionais de Prioridades de Pesquisa em Saúde (ANPPS), bem como os conceitos intrínsecos da economia da saúde e da avaliação da tecnologia da saúde (ATS).

Formalizada em 2004, a Política Nacional de Ciência, Tecnologia e Inovação em Saúde (PNCTS) incluiu, entre suas estratégias, a ATS como instrumento que contribui para o aprimoramento da capacidade regulatória do Estado na incorporação de tecnologias nos sistemas de saúde (2). Independentemente de quais tecnologias devem ser incorporadas ou

não à saúde, as tecnologias de comunicação e informação fazem parte desse conjunto tecnológico e inovador a ser avaliado.

Já a economia da saúde (ES), segundo Del Nero (3), é um ramo do conhecimento que tem por objetivo a otimização das ações de saúde, ou seja, o estudo das condições ótimas de distribuição dos recursos disponíveis para assegurar à população a melhor assistência à saúde e o melhor estado de saúde possível, tendo em conta meios e recursos limitados. No contexto atual, cabe aos servidores a realização do planejamento, avaliação de qualidade e atividades estratégicas, relacionadas à gestão de contratos e projetos de TIC (4) para a aquisição da melhor solução de implantação dos SIS.

A ATS tem como premissa o estabelecimento de diretrizes e protocolos clínicos, regulação de preços de medicamentos e política formal de avaliação, incorporação e gestão de tecnologias no âmbito do SUS (1), por meio da realização de estudos como complementação das evidências científicas para subsidiar a tomada de decisões. As metodologias usadas são capazes de subsidiar estudos econômicos para temas diversos, sejam tecnologias de edição de genes, avanços no conhecimento dos mecanismos de diferenciação celular que oferecem larga estrada para a pesquisa biomédica, bem como a incorporação de tecnologias outras, como as da área de tecnologias da informação e comunicação (TICs), na qual os Sistemas de Informação em Saúde se inserem.

O artigo tem como objetivo apontar as fragilidades quanto à privacidade dos usuários do Sistema Único de Saúde (SUS) e propor uma solução teórica, ainda a ser testada, com base em uma infraestrutura de *personal data stores* (PDS) e na segurança da *blockchain.*

Metodologia

Foi utilizada uma metodologia de um estudo teórico-normativo (5). Trata-se de um ensaio analítico (6), amparado em extensa revisão narrativa da literatura nacional e internacional sobre instrumentos, políticas e casos voltados a tecnologias de informação e comunicação na saúde

Autores como Reinaldo Guimarães e Del Nero formam o arcabouço motivador da economia, política e gestão de tecnologias em sistemas de saúde. Khan Ian e Steele e A. Clarke motivam o estado da arte em IoT. Por fim, Alessi, Camillò, Giangreco, Matera, Pino e Storelli são fundamentais na construção de uma proposta para a estruturação de dados sensíveis.

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Foram realizadas buscas não sistemáticas de teses e artigos nas principais bases de dados científicas, resultando em 34 documentos[6]. Outras fontes de dados incluíram capítulos de livros, textos técnicos e jornalísticos, legislação e portarias do Governo federal. As buscas foram realizadas utilizando-se, individualmente e em combinação, os seguintes termos: *dados pessoais*, *dados sensíveis*, *privacidade*, *lei geral de proteção de dados pessoais*, *Regulamento Geral sobre a Proteção de Dados*, *proteção de dados*, *Internet das coisas*, *Sistema Único de Saúde*. Utilizou-se ainda na busca, os acrônimos dos termos, em português e inglês.

Sistema de Informação em Saúde (SIS)

A área da saúde é influenciada por expressivo número de variáveis internas e externas que interferem nos processos saúde-doença e na administração de programas, serviços e unidades de saúde (7). Muitas dessas variáveis são, por si, informações de saúde de tal relevância, que as diversas formas jurídicas, seja da administração direta, indireta, fundações, associações, entidades privadas filantrópicas, beneficentes e que visam lucro, exigem, por força legal, múltiplos controles e prestações de contas (7).

A eficiência no uso das informações em saúde deve estar a cargo de sistemas que, dispostos em cada área de atendimento, compõem uma gama de informações estratégicas para a melhor gestão em saúde. A escolha e o correto uso dos SIS estão relacionados, tanto como fator de inovação tecnológica, bem como a otimização do uso de recursos para a realização dos diversos processos desempenhados pelos profissionais, tanto no cuidado direto, como na administração da saúde (8). A partir de 2020, com a entrada em vigor pleno da Lei nº 13.709/2018 (9) – Lei Geral de Proteção de Dados (LGPD) – no Brasil, deve-se levar em consideração também o compartilhamento e tratamento de dados pessoais sensíveis por meio desses sistemas[7].

A LGPD inaugura uma preocupação mais aprofundada sobre como tratar dados pessoais, especialmente os dados sensíveis, sem ferir direitos e garantias individuais. Antes disso, os sistemas de informação visavam eficiência no compartilhamento das informações médicas e registros oficiais para fins administrativos, sem particular cautela com a segurança da informação, com o estabelecimento de uma governança de dados ou mesmo um patamar

[6] Foram consultados 28 artigos científicos nacionais e internacionais no Google Scholar e 6 artigos jornalísticos do sistema de saúde brasileiro.
[7] Até o momento da submissão deste artigo, a LGPD já havia passado por 3 prorrogações, sendo a última com previsão para início de vigência para maio de 2021.

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

ético de preservação da privacidade dos indivíduos, já que não havia a obrigatoriedade legal ou coercibilidade jurídica. No SUS, os sistemas de informação em saúde foram desenvolvidos considerando a necessidade de uso da informação, gestão, monitoramento, repasse financeiro de ações e eventos, além de controle de produtividade.

Mais recentemente, o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) reforçou o objetivo de organizar e apresentar a estratégia dasTICs e o conjunto de resultados esperados durante o período de 2019 a 2021 do Sistema de Informação do SUS (DATASUS) do Ministério da Saúde (4). O Plano Diretor enfatiza a necessidade do conjunto mínimo de dados da atenção à saúde, bem como fortalece a estratégia de *e-saúde* para o Brasil. As motivações que veiculam o uso democrático dessas tecnologias, sob a égide de leis, decretos e resoluções, encontram-se representadas no PDTIC. Com a sistematização das tecnologias de informação e comunicação, pode-se prover uma melhor organização dos dados em saúde e serem traçados panoramas mais confiáveis para auxiliar médicos e governantes na tomada de decisões.

O princípio da integralidade do SUS, que aparece no inciso II do art. 7 º da Lei Orgânica do SUS informa que a "integralidade de assistência, entendida como conjunto articulado e contínuo das ações e serviços preventivos e curativos, individuais e coletivos, exigidos para cada caso em todos os níveis de complexidade do sistema" (10). Na sua atualidade, reforça, estrategicamente, a necessidade de se gerar dados de forma mais ágil, segura e eficiente para a gestão em Saúde.

Na mesma lógica de eficiência na gestão em saúde, por meio do uso de suas diversas informações geradas, a expectativa é de que a informação funcione como ferramenta para orientar a tomada de decisão e a produção de conhecimentos válidos. Informações de diferentes naturezas e de diferentes fontes seriam o substrato por excelência desses processos, gerando fluxos de informações relevantes à gestão (11).

À frente do PDTIC encontra-se o Departamento de Informática do SUS (DATASUS), que reúne sistemas dos mais variados, desde o Sistema de Regulação Nacional (SISREG), passando pelo Cadastro Nacional de Estabelecimentos de Saúde (CNES), Sistema de Informação Ambulatorial (SIA), Sistema de Informação Hospitalar (SIH), até o Conjunto Mínimo de Dados (CMD) do SUS.

A validação desses fluxos informacionais inter-sistemas, por meio de procedimentos protocolos estabelecidos pelo DATASUS, sugere a responsabilização daqueles que, circunstancialmente, estiverem tratando dados. Esses procedimentos devem ser feitos por

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

meio da certificação digital, mecanismo tecnológico utilizado para identificar e autenticar usuários, senhas, sites e sistemas eletrônicos, contendo um conjunto de informações codificadas e criptografadas referentes à entidade para a qual o certificado foi emitido, seja uma empresa, uma pessoa física ou computador, redundando em segurança e agilidade das ações, de maneira responsável e sustentável (7).

O uso da Internet das Coisas no SUS

A regulamentação sobre a Internet das Coisas, mais conhecida pelo acrônimo IoT (*Internet of Things*, em inglês) foi instituída no Brasil pelo art. 2º, I do Decreto nº 9.854/2019 (35), o qual a define como

> A infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade. (35)

Na aplicação da Internet das Coisas na área médica, temos o conceito de tecnologias em saúde. Segundo o Ministério da Saúde (12), inicialmente o Brasil convergiu essas tecnologias aplicadas à saúde pela Comissão de Elaboração da Política Nacional de Gestão de Tecnologias em Saúde (PNGTS) – Portaria MS/GM n° 2.510/2005 (11) –, e desde então muito tem-se debatido sobre a agregação de valor proporcionada por recursos tecnológicos no tocante à administração da saúde pública, tendo sido incorporado seus usos às diretrizes e planos do SUS:

> A tecnologia em saúde se refere à aplicação de conhecimentos com objetivo de promover a saúde, prevenir e tratar as doenças e reabilitar as pessoas. São exemplos de tecnologias em saúde: medicamentos, produtos para a saúde, procedimentos, sistemas organizacionais, educacionais, de informação e de suporte e os programas e protocolos assistenciais por meio dos quais a atenção e os cuidados com a saúde são prestados à população. As tecnologias em saúde estão presentes desde a prevenção de doenças até o tratamento e recuperação da saúde das pessoas. (12)

Foi a Lei nº 12.401/2011 (36) que regulamentou a participação civil e dos pacientes na incorporação de tecnologias aplicadas ao sistema público brasileiro e criou a Comissão Nacional de Incorporação de Tecnologias no SUS (CONITEC). Tal contexto regulatório e institucional denota uma clara relevância dada ao tema pelas agências governamentais do país, incitadas pela participação da sociedade civil na elaboração de políticas de saúde no Brasil a partir de organizações não-governamentais, que tiveram um papel relevante nas três

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

últimas décadas e se intensificaram no arcabouço normativo nos últimos 10 anos. As ONGs, que surgiram no contexto dos movimentos de participação civil no Brasil, apoiaram características democráticas importantes na formatação do SUS, em especial a preocupação com o empoderamento informativo dos pacientes. A participação de organizações da sociedade civil no desenvolvimento de políticas sociais, em especial das políticas voltadas para o uso de tecnologias da informação e comunicação é característica primordial para uma mudança de infraestrutura institucional e tecnológica responsável (12). Tem-se constatado um avanço expoente quanto à valorização da incorporação das tecnologias para a estruturação e extrapolação dos dados em saúde de forma sustentável, democrática e transparente.

Outra legislação relevante foi a Resolução nº 7, de 24 de novembro de 2016, que definiu o prontuário eletrônico como modelo de informação para registro das ações de saúde na atenção básica (13). Posteriormente, houve a aprovação da Lei nº 13.787/2018, publicada em 28 de dezembro de 2018, sobre a digitalização e uso dos sistemas de informação no tocante à guarda, armazenamento e manuseio do prontuário eletrônico dos pacientes (13).

Atualmente, muito se tem debatido sobre a telemedicina e uso da tecnologia da informação em saúde. A telemedicina já é uma realidade no SUS, pois em lugares de vazios assistenciais ela se faz essencial. Segundo o Ministro da Saúde (12), o conjunto de dados gerados pelos atendimentos e serviços prestados por meio da telemedicina, somados a interações com sistemas e equipamentos baseados em IoT, poderiam servir de base para a análise e entendimento de situações acerca de vacinação e enfrentamento de doenças. Entretanto, como as novas tecnologias estão sendo integradas aos poucos nos serviços de saúde, esse novo cenário ainda carrega incertezas: como garantir a expansão das TICs e ordenar os dados, de modo a não extrapolar o direito individual à privacidade, tratado no art. 5.º, inciso X da Constituição Federal?

Até meados do início de 2020, os avanços estavam ocorrendo de forma gradativa (14). Com a pandemia do COVID-19, houve uma emergência em saúde pública quanto ao uso de aparatos tecnológicos e consultas virtuais, bem como os prontuários e dispositivos eletrônicos foram rapidamente incorporados à prática clínica. (15,16)

Na saúde pública, essas aplicações podem causar um profundo remodelamento no SUS, pois a dinâmica das informações e projeções baseadas em dados irão interferir diretamente nas tomadas das decisões e monitoramento dos pacientes (6). A coleta de dados em tempo real e a sua análise direcionada são as principais características da Internet

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

das Coisas, em tempos de população em progressiva integração com o meio digital, utilizando equipamentos como *smart watches*, sensores de presença e apoio domésticos, entre outros (11).

Os Ministérios da Saúde e da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) fundaram o projeto *Câmara da Saúde 4.0*, descrito como o

> ambiente de discussões entre membros de instituições públicas e privadas para formular ideias de projetos que possam ajudar, no futuro, a saúde brasileira alinhado a estratégia da saúde digital para o Brasil, que já vem sendo construída por meio do Programa Conecte SUS. (15)

Algumas aplicações que se firmaram com a implementação desse projeto foram justamente o monitoramento de pacientes de maneira remota, por meio de recursos tecnológicos que podem ser vestidos (*wearable tech*), como roupas e relógios com sensores e aplicativos de celular. O sistema poderia identificar alterações agilmente, levando a um decréscimo no percentil de doenças graves e complicações, decorrentes do atraso de tomada de decisões. Esses dados podem vir a alimentar o prontuário eletrônico dos hospitais e serviços públicos de saúde (15).

Contrastando com as implicações questionáveis, as mudanças trazidas pelo recente uso e aplicação de *wearable tech* e outras tecnologias em fases de teste e adequações apontam proveitos de alta relevância, diminuindo os picos letais iminentes das doenças crônicas e comorbidades que precisam ser continuamente monitoradas. É válido ressaltar que as políticas de aprimoramento a serem adotadas para a utilização das ferramentas de IoT objetivam o maior acesso à conectividade e o aumento dos centros de competências de redes (16). Portanto, a seguridade desses dados individuais coletados por meios eletrônicos deve ser essencial e métodos de criptografia e segurança necessitam de uma maior atenção.

Ao ser apresentada a novas formas de monitoramento remoto e ao baixo custo dos sensores contidos nos instrumentos modernos, a parcela da população usuária se torna detentora de informações pessoais que posteriormente virão a ser consultadas pelos profissionais de saúde devidamente autorizados, bem como pelos próprios titulares dos dados, para saber como melhor analisar e verificar possíveis alterações de sinais vitais. As vantagens da disseminação desse conteúdo proporcionam uma sociedade com maior instrução, gerando melhorias na relação médico-paciente e na apresentação do quadro a ser diagnosticado e/ou tratado. Com o montante informativo que passará a possuir, o paciente, por exemplo, poderá, comum sistema simplificado de visualização de dados como

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

curvas de glicose para controle de diabetes, entres outros, acompanhar seu próprio tratamento. Em contrapartida, torna-se agravante o risco de deduções errôneas por parte do paciente, devido à falta de embasamento em artigos científicos na maioria dos domínios virtuais; entretanto, a facilitação da consulta ao clínico responsável e a aproximação digital ao serviço de saúde podem vir a ser uma forma de evitar esse tipo de comportamento (18).

Torna-se evidente que, assim como toda nova tecnologia a ser aderida, o avanço na implantação das IoTs trará desafios consigo. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE), em 2017, a estatística de disseminação da informação digital em termos de acesso e conectividade revela que 59% da população em áreas rurais e 19,9% em região urbana ainda não dispõem de acesso à internet, principal meio para as inovações propostas (17).

O impacto das novas tecnologias na saúde se dá, portanto, em nível socioestrutural, governamental, empresarial e político. Políticas públicas são imprescindíveis para uma futura disseminação da IoT em benefício dos pacientes.

Internet das Coisas na saúde e a proteção de dados sensíveis

O compartilhamento de dados pessoais com os provedores de diferentes serviços representa um risco real à privacidade contemporânea. Isso se dá devido a problemas corriqueiros, tais quais o tratamento inadequado dos dados, a falta de conhecimento dos usuários sobre como seus dados estão sendo compartilhados, o compartilhamento incorreto e o excesso de dados que os próprios usuários finais expõem inadvertidamente. O compartilhamento de informações pessoais, na era da IoT, nos obriga a considerar não apenas dados pessoais, mas também o compartilhamento de dispositivos pessoais. Torna-se fundamental considerar a conscientização e a centralidade dos usuários no compartilhamento, bem como resiliência quanto terceiros mal-intencionados.

A tecnologia da *blockchain* (17) consiste apenas em uma cadeia de blocos, mas não no sentido tradicional dessas palavras. Nesse contexto, a palavra *bloco* significa uma informação digital, que está armazenada em um banco de dados público, a *cadeia*.

A *blockchain* são compostos de informações digitais, que se organizam em três partes: os blocos que armazenam informações sobre as *transações*, ou compartilhamento de dados; os blocos que armazenam informações sobre *quem* está participando das transações; e os blocos que armazenam informações que os *distinguem* de outros blocos, ou metadados diferenciais (17).

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

O uso da *blockchain* tem sido central na discussão a respeito da segurança dos dados sensíveis sanitários. Parte da doutrina (18) diz que, por causa de seu próprio desenho, apresenta um risco em si à privacidade, na mesma medida que promove a transparência e o *accountability*. Contudo, alguns autores já levam em consideração que a *blockchain* pode gerar soluções, especialmente nas áreas de integridade, certificação e disponibilidade, como, por exemplo a distribuição das *gateways* baseada em *blockchain*, de forma a neutralizar possíveis vulnerabilidades[8] (19). Os dados, assim, seriam armazenados e trocados na forma de blocos para apoiar a descentralização da informação e superar a vulnerabilidade[9]. Para tornar as soluções descentralizadas utilizáveis de verdade, existe um grande desafio que vai além da simples conformidade com a LGPD (20).

A exemplo do que ocorre na Europa, a Autoridade Europeia implementou, a fim de fortalecer a proteção de dados confidenciais de cada membro da União Europeia (UE), uma espécie de resolução que protege dados sensíveis em todos os mecanismos de certificação. A questão do tratamento de dados pessoais e dados sensíveis é um problema tão severo que, a partir de 25 de maio de 2018, em todos os estados membros da UE, o novo Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* [GDPR]) passou a vigorar (19). De acordo com o artigo 42 do GDPR, a certificação em si não é requisito obrigatório nos processos de tratamento de dados, mas, para qualquer serviço que possa entrar em contato com dados sensíveis, poderia ser implementado de forma essencial na redução de riscos. A abordagem descentralizada para compartilhamento de dados pessoais, como a utilizada na União Europeia, pode ser compatível não apenas com os requisitos de centralidade dos usuários, mas também com leis protetivas de dados pessoais como a LGPD, representando uma novidade para os sistemas de gerenciamento de compartilhamento de dados pessoais prontos para IoT, com base em um ambiente distribuído. Isso é possível na medida em que se incorpora o mecanismo de consentimento descrito nas bases legais da LGPD, dentro de um verdadeiro protótipo descentralizado desenvolvido para compartilhar dados e dispositivos pessoais.

A navegação pela internet, com ou sem interação com outros usuários, fornece perfis detalhados de dados altamente valiosos. Os sujeitos desses perfis podem não ter ideia de que esses dados sequer existem, de que são coletados, e de que são processados por

[8] A exemplo, T. Lyons, L. Courcelas, K. Timsit, C. Marcelo, P. Jurcys, G. Kousiouris, Wirth, Christian; Kolain, Michael, X. Zheng, R. R. Mukkamala, R. Vatrapu e J. Ordieres-Mere.
[9] A exemplo, Alessi, M., Camillo, A., Giangreco, E., Matera, M., Pino, S., & Storelli, D., T. Kirkham, S. Ravet, S.Winfield, and S. Kellom¨aki, I. Drago, M. Mellia, M. M. Munaf`o, A. Sperotto, R. Sadre, e A. Pras.

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

terceiros sobre os quais o usuário nunca ouviu falar. A GDPR passa a ser um marco dos esforços contínuos da União Europeia para proteger os dados pessoais de seus cidadãos e tornou-se um padrão global do mínimo necessário na proteção da privacidade.

No Brasil, esse movimento não foi diferente. Foram necessários oito anos de debates e redações legislativas até que, em agosto de 2018, o então presidente Michel Temer sancionou LGPD. Dado o *vacatio legis* de dois anos, entre prorrogações e vetos[10], a Lei finalmente entrou em vigor em agosto de 2020 e trouxe novas responsabilidades para pessoas físicas e jurídicas que lidam com dados pessoais. Em comparação à GDPR, é uma legislação mais enxuta, o que permite dúvidas quanto a sua execução, deixando pontos em aberto, que ainda deverão ser definidos pela União.

Conforme a legislação brasileira, os usuários devem ser informados e cientes dos dados que compartilham e com que finalidade serão tratados. O tratamento de dados pessoais por qualquer parte requer o consentimento do titular dos dados ou qualquer uma das outras dez bases legais previstas no art. 7º da LGPD. O veículo mais imediato para garantir o acesso legal a dados pessoais e garantir a proteção desses dados é o consentimento do titular (artigo 8º, seção I, Dos Requisitos para o Tratamento de Dados Pessoais). O consentimento também é a base legal mais frágil pois, a qualquer momento, o consentimento pode ser retirado. São, portanto, imprescindíveis os esforços para que as pessoas tenham controle sobre seus dados pessoais, saber o que estão compartilhando e com quem, por meio de quais aplicativos tecnológicos totalmente compatíveis com a LGPD, mas também se faz de máxima importância o reconhecimento das outras bases legais encontradas nos incisos do art. 7º da referida norma.

Personal Data Storages (PDS): uma solução viável?

Personal Data Storages (PDS) ou, em português, armazenamento pessoal de dados, funciona como um cofre ou armário pessoal de dados. É um serviço que permite armazenar, gerenciar e implantar dados pessoais importantes de maneira altamente segura e estruturada (21). Cada usuário não tem apenas controle sobre seus dados. Eles são reais proprietários, detentores da posse dos dados e, portanto, podem decidir quais serviços podem acessar o armazenamento de dados pessoais e, eventualmente, que tipo de dados

[10] A vigência da lei foi precedida de inúmeras intercorrências legislativas. A vigência inicial (prevista para agosto de 2020) foi adiada por medida provisória para maio de 2021. A Câmara dos Deputados propôs a vigência a partir de 31 de dezembro de 2020, porém o Senado, ao não apreciar a MP no prazo legal, manteve a vigência original. Com a sanção presidencial a lei já entrou em vigor desde agosto de 2020.

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

pode ou não ser recuperado por cada um desses serviços. Uma descrição geral dos sistemas de gerenciamento de dados pessoais foi fornecida por Bus e Ngyuen (22). Para eles, um PDS atua em três níveis: infraestrutura, gerenciamento de dados e interação do usuário. E é sobre esses três níveis que um sistema como o SIS deve se pautar para ter o PDS como solução para os dados sensíveis que circulam dentro dele.

Em vez dos dados pessoais serem pertencentes a silos centralizadores de informações, os PDS prometem devolver o controle aos usuários, permitindo que eles sejam proprietários de seus dados e controlem o acesso por meio de permissões granulares. O usuário pode inserir dados sobre si próprio e evidências de sua identidade, permitindo que outras pessoas acessem ou usem tais dados indiretamente para fornecer serviços.

Uma possível resposta à típica perda de controle sobre os próprios dados é uma solução que também pode ser aplicada às informações sensíveis e à maneira como as informações são divulgadas para serviços de terceiros, especialmente, os serviços de saúde. A ideia é que o titular dos dados seja o único proprietário e gerente do processo de compartilhamento, a partir de um sistema de gerenciamento de dados pessoais. Esse não é um conceito novo, mas evoluiu com o tempo, considerando os modernos dispositivos pessoais de IoT, dentro da classe maior de *dados sensíveis*. Conforme o conceito legal trazido dentro da LGPD, dado sensível é todo aquele dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

O compartilhamento de dados no ambiente distribuído representa um desafio. Se, por um lado, existe a oportunidade de estruturar uma ferramenta tecnológica para gerenciar dados pessoais capaz de incorporar o paradigma de *privacy by design*, por outro lado, ainda existem muitos problemas que devem ser abordados para estar em *compliance* total com as leis protetivas dos dados pessoais (21).

A aplicabilidade da *blockchain* e como ela pode se aproximar da conformidade com a LGPD é amplamente estudada e prevista em muitos campos (23), mesmo que ainda não tenha alcançado uma abordagem pacífica. Isso mostra que existe um forte entendimento em torno da *blockchain* e de seu potencial de lidar com informações sensíveis, fornecendo até sugestões de conformidade de uma perspectiva legal (24). No entanto, as tecnologias distribuídas têm o potencial de praticamente capacitar os usuários com controle efetivo sobre seus dados pessoais: dar a eles consciência total, gerenciar a dificuldade de gerar ou

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

fornecer o *consentimento*, dar informações sobre o processamento do compartilhamento de dados pessoais e sem nenhuma autoridade central ou terceiros de má fé.

Para ser utilizável em ambientes reais, esse sistema descentralizado de gerenciamento de dados pessoais pronto para IoT deve resolver a aparente dificuldade da *blockchain* em ser certificada pela lei. Para tanto, Alessi, Camillò, Giangreco, Matera, Pino eStorelli estenderam as funcionalidades oferecidas pelo protótipo *personal data storages* (PDS) (25), tendo como elemento de novidade um plano tecnológico de armazenamento de dados pessoais descentralizado pronto para IoT com ação de *consentimento* dos usuários, conforme descrito na legislação, em um ambiente distribuído habilitado para *blockchain*.

Existem dois lados importantes do mercado de PDS: os usuários que são os sujeitos dos dados e as organizações que desejam usá-los (e atualmente os coletam e controlam). Para este artigo, levou-se em consideração apenas os dados dos usuários do SIA/SUS.

São vários os exemplos de PDSs disponíveis na literatura, e como a descentralização no tratamento de dados pessoais foi alavancada (20). Alguns dos exemplos levados em consideração são MyDex (26), IRMA (27), OpenPDS (28), OnenameBITNATION (29). Os exemplos mostraram que, embora a descentralização fosse fundamental para aumentar a segurança, a conscientização e a inclusão do usuário no processo de compartilhamento de dados, é imprescindível uma abordagem para lidar com a divulgação e o compartilhamento de dados pessoais, juntamente com campanhas e políticas públicas sobre o compartilhamento de dispositivos IoT. Nesse caso, o Decreto nº 9.854/2019 (35) sobre a IoT no Brasil denota um enorme avanço, estabelecendo as bases normativas para possíveis políticas e campanhas nessa área. Além disso, ao lidar com dados pessoais, um PDS moderno precisa estar condizente com a regulamentação da LGPD. Existem questões específicas ao se tentar fazer uma tecnologia descentralizada funcionar sob essas condições legais e deixá-la em conformidade legal com esse novo cenário.

Embora o PDS seja promotor de maior empoderamento dos usuários e de segurança de seus dados, teria que lidar com tensões entre as leis protetivas de dados pessoais e a *blockchain*. Essas tensões giram principalmente em torno de três questões (30) que teriam que ser observadas no SIS/SUS e que ainda precisam ser trabalhadas antes do término da vacância da LGPD:

i) A identificação e obrigações dos controladores e processadores de dados. Embora existam muitas situações em que os controladores e processadores de dados possam ser identificados e cumpram suas obrigações, também há casos em que é bastante difícil, e

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

talvez impossível, identificar um controlador de dados específico, principalmente quando as transações de *blockchain* são escritas pelos próprios titulares de dados.

ii) O anonimato dos dados pessoais. Essa é a tensão mais corriqueira nos estudos sobre privacidade. Há debates intensos sem consenso sobre o que é preciso para anonimizar dados pessoais a ponto da saída resultante poder ser potencialmente armazenada em uma rede *blockchain* (20). Um exemplo disto, o *hash*[11] (31) de dados, que não pode ser considerado uma técnica de anonimização em muitas situações. Ainda há casos em que o uso do *hash* para gerar assinaturas digitais exclusivas de dados que são armazenados fora da cadeia é potencialmente concebível em uma *blockchain*.

iii) O exercício de alguns direitos do titular dos dados. Se os dados pessoais forem registrados em uma rede *blockchain*, é praticamente impossível retificá-los ou removê-los. A definição do que pode ser considerado apagamento no contexto de *blockchains* ainda está em discussão. Assim, em um sistema distribuído, vários direitos fundamentais passam a ser fragilizados em nome da privacidade e proteção de dados pessoais. Exemplos desses direitos são: o direito de retificar dados pessoais imprecisos, sem demora injustificada, no art. 18, III da LGPD; o direito de excluir o dado, a partir da retirada de seu consentimento a qualquer momento, ou expresso pedido para exclusão do dado, conforme visto no art. 18, VI, exceto nas hipóteses previstas no art. 16 da LGPD; e, principalmente, o direito ao esquecimento, um dos principais desafios para os desenvolvedores de *blockchain*, advindo da obrigação de apagar os dados pessoais onde quer que eles possam ser armazenados. No Brasil, o direito ao esquecimento possui assento constitucional e legal, considerando que é uma consequência do direito à vida privada (privacidade), intimidade e honra, assegurados pelo art. 5º, X da Constituição Federal (32) e pelo art. 21 do Código Civil (33), mas com vias de ser viabilizado pela LGPD (20), apesar de, nesta, não haver expressa prescrição. O professor da Faculdade de Direito da Universidade do Estado do Rio de Janeiro e diretor do ITS–Rio, Carlos Affonso Souza (34), falou, em maio de 2019, no seminário internacional *Lei Geral de Proteção de Dados: a caminho da efetividade* sobre o direito ao esquecimento e como isso está causando reflexos no Poder Judiciário:

> Acho que esse é um tema importante, uma vez que a LGPD, mesmo trazendo uma série de direitos aos cidadãos, não trata do direito ao esquecimento. Nenhuma decisão judicial pode garantir que exista o esquecimento na sociedade. Ele está ligado, diretamente, à preservação da imagem, privacidade e honra das pessoas. A própria arquitetura da rede de

[11] Uma função *hash* é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo.

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

> computadores parece que foi feita para manter a lembrança, não para o esquecimento. (34)

Criar procedimentos para a proteção dos dados, resguardando a segurança jurídica e transparência, na prática, indica uma limitação da própria garantia de alguns direitos do titular, a partir da viabilidade computacional do cenário de *blockchain*. Dessa maneira, não há como garantir o direito ao esquecimento, mas sim, a responsabilidade sobre o tratamento do dado pessoal sensível em questão.

Considerações finais

Já existe uma clara identificação do uso de tecnologias IoT usadas no SUS. No estado atual da implementação dessas novas tecnologias, o processo lógico de tomada de decisões e os principais focos de aplicação no SUS têm sido nas áreas de monitoramento dos pacientes e gestão de dados de saúde. Tentando buscar tanto diagnósticos mais precisos, atendimentos mais eficientes e uma maior fluidez e agilidade no serviço de saúde como um todo, percebe-se uma tendência na utilização de IoT na área.

A Coleta de Dados Simplificada (CDS) passa a ser um dos componentes da estratégia e-SUS. Sua infraestrutura de coleta de dados sensíveis pelo SUS ainda é bastante centralizada nas autoridades sanitárias. Isso leva a identificação de fragilidades dessa coleta e tratamento de dados na forma como o SIS/SUS é hoje concebido, especialmente quanto à preservação da privacidade, perseguida pela Lei Geral de Proteção de Dados.

Esse artigo traz como contribuição uma proposta teórica de uso de *personal data storage* PDS como possível solução para a redução dos riscos à privacidade e a identificação das fragilidades na implementação dessa solução pelo SIS/SUS, pois não foram encontrados artigos científicos que trabalhassem sobre essa abordagem e escopo no Brasil. A aplicação de PDS em sistemas informacionais complexos que compartilham dados sensíveis como os de saúde do SUS hoje demonstram fragilidades na preservação da privacidade de seus usuários. Embora, ainda seja uma discussão inicial de propositura teórica, este artigo incita contribuições futuras de abordagem prática e testes de diferentes métodos de PDS na remodelagem da infraestrutura informacional do SIS/SUS.

Referências

1. Tenório M, Mello GA, Viana ALD. Políticas de fomento à ciência, tecnologia e inovação em saúde no Brasil e o lugar da pesquisa clínica. Ciência e saúde coletiva [Internet]. Maio

2017 [citado em 13 ago. 2020]; 22(5):1441-1454. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232017002501441&lng=en

2. Brasil. Ministério da Saúde. Estratégia e-Saude para o Brasil. Resolução nº 19, 22 de junho de 2017. Aprova e torna público o documento Estratégia e-Saúde para o Brasil, que propõe uma visão de e-Saúde e descreve mecanismos contributivos para sua incorporação ao Sistema Único de Saúde (SUS) até 2020. [citado em 13 ago. 2020]. Disponível em: http://portalarquivos.saude.gov.br/images/pdf/2017/julho/12/Estrategia-e-saude-para-o-Brasil.pdf

3. Del Nero CR. O que é economia da saúde. In: Piola SF, Vianna SM, organizadores. Economia da saúde: conceitos e contribuição para a gestão em saúde. Brasília: Ipea; 2002. p. 5-21.

4. Guimarães R. Sobre uma política de ciência e tecnologia para a saúde. Saúde debate [Internet]. Mar. 2019 [citado em 13 ago. 2020];43(120):181-193. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-11042019000100181&lng=en

5. Hintikka J. Some Main Problems of Deontic Logic. In: Hilpinen, R. Deontic Logic: Introductory and Systematic Readings. D. Dordrecht: Reidel Publishing Company; 1981. p. 36-45.

6. Rother ET. Revisão sistemática X revisão narrativa. Acta paul. enferm. [Internet]. Jun. 2007 e [citado em 20 set. 2020];20(2):v-vi. Disponível em: https://doi.org/10.1590/S0103-21002007000200001

7. Novaes HMD, Elias FTS. Uso da avaliação de tecnologias em saúde em processos de análise para incorporação de tecnologias no Sistema Único de Saúde no Ministério da Saúde. Cad. Saúde Pública [Internte]. 2013; 29(Suppl 1):s7-s16. Disponível em: https://doi.org/10.1590/0102-311X00008413

8. Bittar OJ, Nogueira V, Biczyk M, Serinolli MI, Novaretti MCZ, De Moura MMN. Sistemas de informação em saúde e sua complexidade. Rev. Adm. Saúde [Internet]. Jan./Mar. 2018 [citado em 20 set. 2020] ;18(70). Disponível em: http://dx.doi.org/10.23973/ras.70.77

9. Brasil. Lei nº. 13.709, de 14 de agosto de 2018 [Internet]. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília. 2018. [citado em 30 set. 2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

10. Brasil. Lei nº. 8080, de 19 de setembro de 1990 [Internet. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Brasília, 1990 [citado em 30.set.2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8080.htm

11. Brasil. Ministério da Saúde/Secretaria Executiva. Portaria nº 676, 17 de julho de 2019 [Internet]. Plano Diretor de Tecnologia da Informação e Comunicação. Brasília, 2019 [citado em 30 set. 2020]. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2019/08/PDTIC-2019-A-2021-FINAL-14-DE-AGOSTO-2019.pdf

12. Ministério da Saúde. Entendendo a Incorporação de Tecnologias em Saúde no SUS: como se envolver [Internet]. Brasília, 2016 [citado em 30 set. 2020], 34 p. Disponível em: http://conitec.gov.br/images/Artigos_Publicacoes/Guia_EnvolvimentoATS_web.pdf

13. Brasil. Ministério da Saúde. Resolução nº 7, de 28 de novembro de 2016. Define o prontuário eletrônico como modelo de informação para registro das ações de saúde na atenção básica e dá outras providências. 28 nov 2016; Seção 1, 108.

14. Maldonado JMSV, Marques AB, Cruz A. Telemedicina: desafios à sua difusão no Brasil. Cad. Saúde Pública [Internet]. 2016;32:1-12. Disponível em: https://doi.org/10.1590/0102-311X00155615

15. Garcia MVF, Garcia MAF. Telemedicina, segurança jurídica e COVID-19: onde estamos? J. Bras. Pneumol [Internet]. 2020;46(4):e20200363. Disponível em: https://doi.org/10.36416/1806-3756/e20200363

16. Caetano R, Silva AB, Guedes ACCM, Paiva CCN, Ribeiro GR, Santos DL *et al*. Desafios e oportunidades para telessaúde em tempos da pandemia pela COVID-19: uma reflexão sobre os espaços e iniciativas no contexto brasileiro. Cad. Saúde Pública [Internet]. 2020;36(5); e00088920. Disponível em: https://doi.org/10.1590/0102-311x00088920

17. IBGE Educa [Internet]. O uso da internet, televisão e celular no Brasil [Internet]. Brasília: IBGE; 2018 [citado em 8 ago. 2020]. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html

18. Vigna P, Casey MJ. The Truth Machine: The Blockchain and the Future of Everything. London: Harper Collins Publishers; 2018.

19. Lee Y, Park J, Park J. A blockchain-based smart home gateway architecture for preventing data forgery. Human-centric Computing and Information Sciences. 2020;10(1):21-32

20. Alessi M, Camillò A, Giangreco E, Matera M, Pino S, Storelli D. A Decentralized Personal Data Store based on Ethereum: Towards GDPR Compliance. Journal of Communications Software and Systems [Internet]. 2019 [citado em 14 ago. 2020.];15(2):79-88. Disponível em: https://doi.org/10.24138/jcomss.v15i2.696

21. Bus J, Nguyen MHC. Personal Data Management - A Structured Discussion. Digital Enlightenment Forum [Internet]. 2013 [citado em 14 ago. 2020]. Disponível em: https://www.academia.edu/13229965/Personal_Data_Management_A_Structured_Discussion doi 10.3233/978-1-61499-295-0-270

22. Huang K, Zhang X, Mu Y, Rezaeibagha F, Du X. Scalable and redactable blockchain with update and anonymity. Information Sciences. 06 fev. 2021: 546:25-41.

23. Sethuraman S, Rangan V. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security. Dez. 2019;2020(1):1-40

24. Ferguson RI, Renaud K, Wilford S, Irons A. PRECEPT: a framework for ethical digital forensics investigations. Journal of Intellectual Capital [Internet]. 2020;21(2):257-290. Disponível em: https://doi.org/10.1108/JIC-05-2019-0097

25. Alessi M, Camillò A, Giangreco E, Matera M, Pino S, Storelli D. Make Users Own Their Data: A Decentralized Personal Data Store Prototype Based on Ethereum and IPFS. In: Annais of 3rd International Conference on Smart and Sustainable Technologies (SpliTech). 2018. p. 1-7.

26. MyDex [Internet]. 2020 [citado em 14 ago. 2020]. Disponível em: https://mydex.org/

27. Irmacard. Choose IRMA: Put a digital passport on your own mobile [Internet]. [citado em 14 ago. 2020]. Disponível em: https://www.irmacard.org/#faqs

28. OPENPDS. Personal Data with Privacy [Internet]. 2012 [citado em 14 ago. 2020]. Disponível em: https://openpds.media.mit.edu/

29. Bitnation. Bitnation Pangea: Bitnation Governance 2.0 [Internet]. Out. 2017. [citado em 14 ago. 2020]; Disponível em: https://tse.bitnation.co/

30. Brasil. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal; 1988 [citado em 13.ago.2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

31. Brasil. Lei 10.406, de 10 de janeiro de 2002 [Internet]. Institui o Código Civil. [citado em 13 ago. 2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm

32. Justiça Federal. Regulação, efetividade e segurança jurídica dominam debates no último dia do seminário sobre a LGPD [Internet]. 28 maio 2019 [citado em 13 ago. 2020]. Disponível em: https://www.cjf.jus.br/cjf/noticias/2019/05-maio/regulacao-efetividade-e-seguranca-juridica-dominam-debates-no-ultimo-dia-do-seminario-sobre-a-lgpd

33. Brasil. Decreto nº 9.854, de 25 de junho de 2019 [Internet]. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. [citado em 19 dez. 2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm

34. Brasil. Lei nº 12.401, de 28 de abril de 2011 [Internet]. Altera a Lei nº 8.080, de 19 de setembro de 1990, para dispor sobre a assistência terapêutica e a incorporação de tecnologia em saúde no âmbito do Sistema Único de Saúde - SUS. [citado em 19 dez. 2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12401.htm

ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitário

Colaboradores

Camara MAA contribuiu com a concepção, análise e interpretação de dados, redação, revisão crítica e aprovação da versão final do artigo. Lins GHA contribuiu com a concepção, análise e interpretação de dados, e redação do artigo. Oliveira FHC contribuiu com a concepção, análise e interpretação de dados, e redação do artigo. Camelo EMA e Medeiros NRFC contribuíram com a análise e interpretação de dados e revisão crítica do artigo.

Submetido em: 30/03/20
Aprovado em: 04/02/21

Como citar este artigo

Camara MAA, Lins GHA, Oliveira FHC, Camelo EMA, Medeiros NRFC. Internet das Coisas e *blockchain* no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados. Cadernos Ibero-Americanos de Direito Sanitário. 2021 jan./mar.;10(1):93-112.

https://doi.org/10.17566/ciads.v10i1.657