



cee

**Desafios para o Sistema Único de Saúde (SUS)
no contexto nacional e global de transformações sociais,
econômicas e tecnológicas - CEIS 4.0**

POLÍTICAS E INSTRUMENTOS PARA A TRANSFORMAÇÃO DIGITAL DO SUS

EQUIPE DE PESQUISA

Maria Lucia O. Falcón

José E. Cassiolato

Centro de Estudos Estratégicos da Fiocruz Antonio Ivo de Carvalho

Coordenador do CEE

Carlos Augusto Grabois Gadelha

Projeto Integrado CEE

Complexo Econômico-Industrial da Saúde e Prospecção em CT&IS

Subprojeto

Desafios do SUS no contexto nacional e global de transformações sociais, econômicas e tecnológicas – Projeto CEIS 4.0

Coordenador Geral

Carlos Augusto Grabois Gadelha

Coordenadores Adjuntos

José Cassiolato
Denis Gimenez

Equipe Executiva

Marco Aurélio Nascimento
Karla Bernardo Mattoso Montenegro
Felipe Kamia
Gabriela Maretto
Juliana Moreira
Leandro Safatle

Colaboradores

Anna Durão (Divulgação e Comunicação),
Bernardo Cesário Bahia (Pesquisa), Glaucy Silva
(Gestão Administrativa), Elisabeth Lisovsky
(Revisão Português) e Nilmon Filho (Projeto Gráfico)

Relatório de pesquisa – CEIS 4.0

Políticas e instrumentos para a transformação digital do SUS

Pesquisadores

Maria Lucia O. Falcón
José E. Cassiolato

Citar como:

FALCÓN, M.L.; CASSIOLATO, J. Políticas e instrumentos para a transformação digital do SUS. In: GADELHA, C. A. G. (Coord.). Projeto Desafios para o Sistema Único de Saúde no contexto nacional e global de transformações sociais, econômicas e tecnológicas (CEIS 4.0). Relatório de Pesquisa. Rio de Janeiro: CEE/Fiocruz, 2022.

Todos os direitos reservados ao Centro de Estudos Estratégicos da Fiocruz Antonio Ivo de Carvalho (CEE). Reprodução autorizada desde que citada a fonte.

Esta obra foi elaborada no âmbito do projeto “Desafios do SUS no contexto nacional e global de transformações sociais, econômicas e tecnológicas – CEIS 4.0”. As opiniões expressas refletem a visão dos autores, não representando a visão institucional sobre o tema.

Sumário

1	ESTADO-SOCIEDADE-MERCADO: ACUMULAÇÃO DE CAPITAL E MODO DE REGULAÇÃO EM AMBIENTES DIGITAIS NA DÉCADA 2020	5
2	NOVAS TECNOLOGIAS PARA SISTEMAS NACIONAIS DE SAÚDE, CONSEQUÊNCIAS E LIMITES: DADOS EM DLT (BLOCKCHAIN), ID (IDENTIDADE DIGITAL), UNIVERSALIDADE E UBIQUIDADE	12
3	MODELOS CONSORCIADOS POSSÍVEIS PARA O SUS DIGITAL.....	21
4	CONCLUSÕES.....	35
5	REFERÊNCIAS	41

Políticas e instrumentos para a transformação digital do SUS

Maria Lucia O. Falcón; José E. Cassiolato

“las tecnologías digitales solo proporcionan las herramientas y no pueden transformar el sector sanitario por sí solas, es necesario que los trabajadores sanitarios y los pacientes les den un uso productivo. Así que, no es conveniente digitalizar el modelo asistencial actual, sino, por el contrario, usar el potencial digital para transformar y reformar el sector” (Rafael Bengoa, ex director de Sistemas de Salud de la OMS, entrevista à Forbes¹)

A Nota Técnica 4 está voltada a compreender as mudanças tecnológicas que estão acontecendo no SUS e no CEIS no que se refere à transformação digital, em vários aspectos do sistema: na infraestrutura utilizada para transmitir e armazenar dados, nos algoritmos e Inteligência Artificial aplicado à gestão dos dados e do sistema de saúde, na prestação de serviços à distância ou telemedicina, nos custos e pagamentos dos serviços de saúde (seja público ou seja privado). Ao final, todos esses aspectos somam e se articulam em um novo formato de regulação do mercado, que está recebendo o nome de e-Saúde ou Saúde Digital.

Muitas formatações envolvem *fintechs* (para financiamento e *insurance*) e empresas prestadoras de diversos serviços vinculados à saúde, associadas à Indústria 4.0 e ao Estado 4.0. São possibilidades de uso inclusivo, democrático e promotor do desenvolvimento que as novas tecnologias podem oferecer. As consequências destes diferentes modelos para a democracia e para o desenvolvimento são especialmente relevantes para o planejamento de médio e longo prazos do CEIS e do SUS.

A Nota Técnica 3 possui 3 capítulos e a conclusão. Os capítulos se dedicam à: 1) entender as transformações digitais no âmbito do Estado e dos Direitos (civis, sociais, econômicos e políticos), como se dá a interação com a economia (mundo da produção e do trabalho - Indústria 4.0) e com a vida social mediada pelo espaço digital, especialmente no que se refere aos sistemas de saúde, além de conhecer os impactos dos dados compartilhados (pool, como no caso do Open Banking) sobre a democracia e os direitos dos cidadãos; 2) Conhecer as novas tecnologias de *ledger* descentralizadas como as blockchain e as possibilidades de melhoria em gestão de sistemas produtivos e redes de valor que elas estão criando, especialmente para os sistemas nacionais de saúde e suas interfaces com o CEIS; 3) conhecer e analisar as consequências da digitalização para novos modelos de

1 <https://forbes.es/healthcare/92190/la-explasion-de-la-salud-digital/> publicado em 25/03/2021.

sistema nacional de saúde, as escalas territoriais, consórcios entre público e privado e entre escalas federativas.

1 Estado-Sociedade-Mercado: Acumulação de capital e modo de regulação em ambientes digitais na década 2020

As transformações que o sistema de produção capitalista atravessa nessas três primeiras décadas do novo milênio são tão profundas que os estudos e análises não conseguem estabelecer uma narrativa completa, porém há importantes tendências já identificadas. Elas se apresentam como:

- a) Composição orgânica do capital (relação entre trabalho morto e trabalho vivo, isto é, parte equipamentos e máquinas ou trabalho morto/cristalizado, parte trabalho efetivo e vivo feito pelas pessoas que agrega valor ao processo produtivo) intensiva em tecnologias de informação e comunicação;
- b) Qualificação diferenciada da força de trabalho, que deve usar de maneira intensiva o trabalho intelectual e criativo e não força física, repetição ou redundância de tarefas;
- c) Redução dos tempos de produção, circulação e realização das mercadorias em geral e especialmente as novas mercadorias do espaço digital (informação em todas as suas formas – dados, imagens, áudios, *mix* real e virtual etc.);
- d) Intermediação financeira descentralizada e insubmissa aos controles de estados nacionais e blocos econômicos;
- e) Um sistema produtivo informacional contínuo e em forma de redes, sejam físicas (fibras óticas) sejam intangíveis (por satélites);
- f) Um novo agente econômico, o proconsumidor, que está produzindo e consumindo informação até quando não está ligado à rede – a ausência é uma informação em si mesma.
- g) Novos direitos digitais começam a ser assegurados, como a propriedade e uso dos dados das pessoas e empresas, a segurança dessas informações; enfim, cada vez mais é necessário testar e garantir a preservação dos direitos fundamentais constitucionais nos novos espaços digitais.

Difícil compreender que, na atual etapa de desenvolvimento capitalista, a locomotiva da acumulação de riqueza não está mais na agricultura, nem na indústria, nem no comércio, nem sequer no setor financeiro, pois todos esses setores estão subordinados ao controle da informação e dos dados das novas tecnologias. Não por acaso as maiores empresas precificadas em bolsas de valores no mundo são gigantescos oligopólios de tecnologias da informação e comunicação. Mais que dominar *hardwares* (a fabricação de computadores,

máquinas interligadas em redes ou as próprias redes de fibras ou satélites), eles dominam o *software* – a linguagem das máquinas, o que as faz coletar, processar, transmitir e realimentar as redes com informações de todo tipo, inclusive sobre o próprio processo (metadados). O terceiro milênio da era cristã se anuncia como a era do capitalismo informacional.

Nesse modo de acumulação ocorrem mudanças no papel dos produtores e dos consumidores, sendo que a atividade dos cidadãos no campo econômico torna-se completamente integrada à sua atividade social, surgindo o proconsumidor – que simultaneamente consome e produz informação enquanto usa as redes de comunicação de dados. Deve-se enfatizar que, nesses anos 2020, essas atividades informacionais não ocorrem apenas através dos computadores, mas principalmente através dos telefones celulares e seus aplicativos (*softwares*), além de toda a parafernália de *gadgets* inteligentes na IoT (Internet of Things, ou das Coisas), isto é, com *softwares* embutidos e ligados na Internet, de TVs a veículos automotivos e fábricas, além dos *wearables* (mais conhecidos são os relógios *smart*). Todos eles produzem e recebem informações continuamente. Nesse ambiente, uma questão relevante trata da propriedade e uso dos dados das pessoas/empresas pelas plataformas e empresas. Se a Internet é a tecnologia de comunicação que faz o capitalismo informacional acontecer, a cibersegurança é a nova dimensão da paz social e da defesa da propriedade.

Diante de tão profunda transformação do regime de acumulação, setores produtivos novos despontam, setores produtivos tradicionais se modernizam e adotam a digitalização, muitos postos de trabalho se extinguem e surgem novas profissões em um mercado de trabalho disruptivo. A maneira de produzir, comprar, conviver e de prestar serviços se altera radicalmente, junto com a percepção da sociedade sobre suas necessidades, o que seja conforto e qualidade de vida. Na verdade, toda a regulação dos mercados – de trabalho, de consumo de massa, de acesso a serviços – e a garantia dos direitos dos cidadãos devem ser também transformadas. Em última instância, a relação Estado-Sociedade-Mercado vem sendo reelaborada.

Se o mercado vem chamando esse estágio tecnológico e produtivo de “Indústria 4.0” – conceito pobre e que não abarca todas as dimensões da transformação em curso – deve-se à rápida compreensão do que implica a nova composição orgânica do capital: fábricas automatizadas, produtoras de mercadorias e de Big Data, geridas por inteligência artificial, com programadores atuando lado a lado com os engenheiros de produção, vendas e pagamentos mediados por *market places* digitais e Fintechs.

Numa tentativa de fazer a mesma comunicação rápida, pode-se falar em “Estado 4.0” como sendo aquele que se constitui em uma rede onde continuamente produz, coleta,

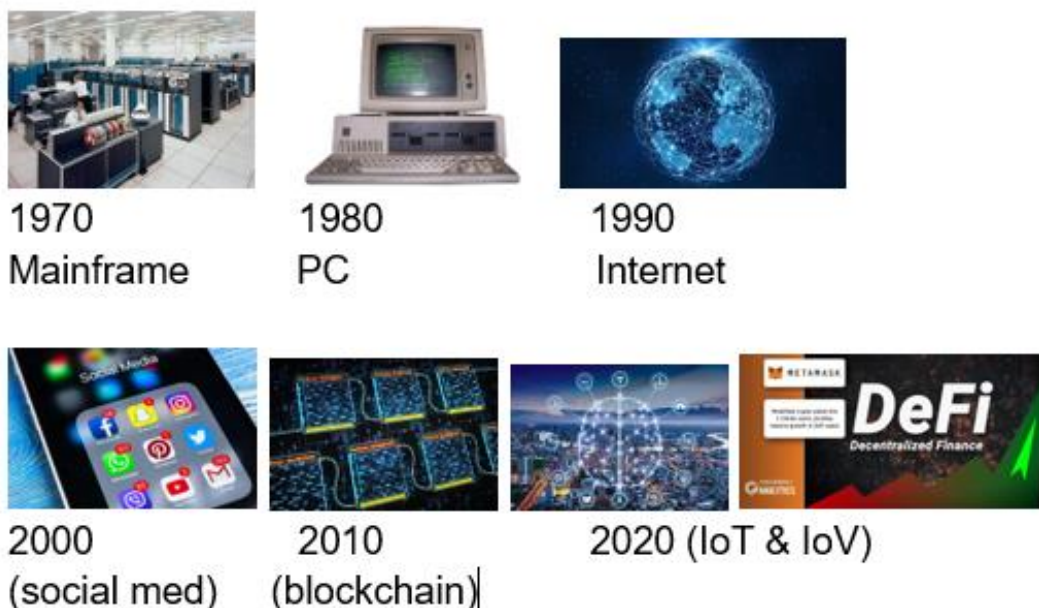
processa e redistribui informação, usa inteligência artificial para processar dados, criar padrões e tomar decisões. Os cidadãos são proconsumidores nessa rede pública e seus dados são valiosos, devendo ter garantidos seus direitos digitais. A maior parte da burocracia passa a ser automatizada, criando-se uma Identidade Digital dos cidadãos, com seus dados compartilhados (em tese segundo seu controle e sua vontade) em um “pool” semelhante ao que se conhece como “open banking”.

Na verdade, e de maneira mais fundamentada, mais do que focar nos instrumentos tecnológicos 4.0, é necessário atualizar os meios e fins do Estado no espaço digital, suas relações com os cidadãos e empresas, pactuar políticas e instrumentos adequados. Enfim, o Estado nos anos 2020 deve estar à altura das exigências de todos os números e versões das TIC – 4.0, 5.0, etc. – na defesa dos direitos das pessoas e fortalecendo as instituições do pacto democrático, sob pena de construir distopias de ficção científica, comandadas por uma elite de autocratas, “sacerdotes” dos algoritmos e oligopólios em redes informacionais.

A Figura 1 mostra a evolução das tecnologias de informação, que nitidamente evoluem para o formato em rede, com suas partes interligadas por sistemas cada vez mais potentes de transmissão de dados quase sem latência (sem atrasos), em tempo real. Esse poder tecnológico está agora avançando para intercambiar informações do espaço virtual com o espaço real, nos softwares de realidade aumentada e mista (virtual+ real).

Se os anos 1990 foram marcados pelo surgimento de uma Internet acessível ao público, os anos 2000 estabeleceram o reinado das redes sociais e suas plataformas, a década de 2010 viu o surgimento de *softwares* de dados descentralizados criptografados (*blockchain*) resultando, nos anos 2020, na Internet das Coisas e na Internet do Valor – completando uma transformação profunda na maneira de produzir, consumir e acumular riqueza. As DeFi – Finanças Descentralizadas – estão formando um sistema financeiro pouco submisso aos controles dos estados nacionais sobre moedas e outros ativos, além de mercados de capitais e investimentos com efetiva competição com os bancos e gestoras financeiras tradicionais.

Figura 1 – Evolução das TIC, 1970-2020



Fonte: Elaboração própria.

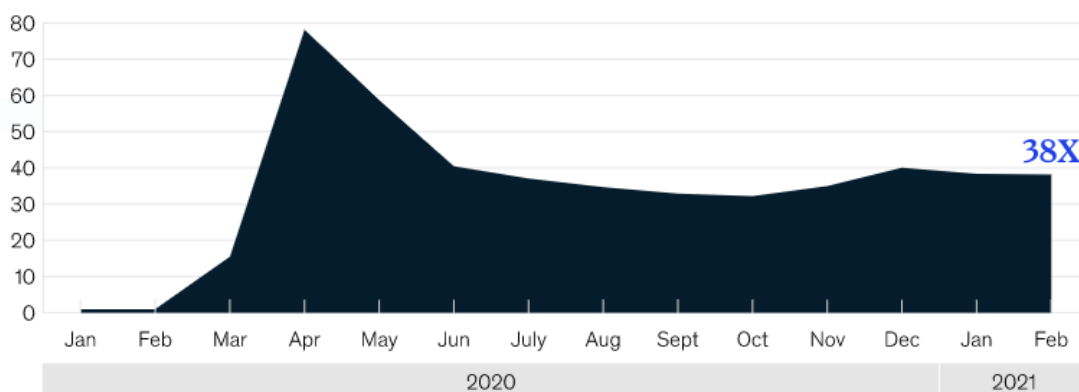
Em verdade, as TIC evoluíram a ponto de criar novos espaços e cenários num ambiente digital, que suscitam suas próprias relações de cooperação e seus conflitos. Esse fato tem sido mais percebido pela sociedade nos fenômenos midiáticos, por exemplo, as *fake news*, ou as finanças digitais em aplicativos para celulares como PIX, do comércio eletrônico; e menos percebido no que diz respeito à propriedade e uso dos dados pessoais, da cibersegurança e da privacidade. Deve-se perguntar, por exemplo, como a sociedade está tratando essas questões diante do avanço da digitalização na saúde.

Um relatório da consultoria empresarial McKinsey (2021) publicado em julho de 2021, aponta uma utilização 38 vezes maior de telemedicina entre abril de 2020 e fevereiro de 2021, como mostra a Figura 2. Além disso, o faturamento e os investimentos em serviços de telemedicina mais do que dobraram em 2020, comparativamente a 2019, tendo sido crescentes e devem continuar nessa trajetória nos próximos anos, como mostram os dados da Figura 3. Não se percebe investimentos proporcionais para preparar a sociedade (a educação em direitos digitais) para essa transformação.

Figura 2 – Crescimento no uso de telemedicina

Growth in telehealth usage peaked during April 2020 but has since stabilized.

Telehealth claims volumes, compared to pre-Covid-19 levels (February 2020 = 1)¹



¹ Includes cardiology, dental/oral, dermatology, endocrinology, ENT medicine, gastroenterology, general medicine, general surgery, gynecology, hematology, infectious diseases, neonatal, nephrology, neurological medicine, neurosurgery, oncology, ophthalmology, orthopedic surgery, poisoning/drug tox./comp. of TX, psychiatry, pulmonary medicine, rheumatology, substance use disorder treatment, urology. Also includes only evaluation and management visits; excludes emergency department, hospital inpatient, and psychiatry inpatient claims; excludes certain low-volume specialties.
Source: Compile database; McKinsey analysis

Fonte: Mckinsey, 2021 em <https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality>

Tantas e tão profundas transformações estão gerando legislações inovadoras no sentido de garantir os direitos da cidadania sem impedir a evolução tecnológica. A Carta de Direitos Digitais² da Espanha, por exemplo, é um importante guia para a regulação em um espaço digital. Na sua essência, busca atualizar e preservar os direitos constitucionais – civis, políticos, sociais e econômicos – nos espaços digitais onde passamos a trabalhar, conviver, consumir e, literalmente, existir. Está estruturada em 6 Capítulos que tratam de: Direitos de Liberdade, Direitos de Igualdade, Direitos de Participação e do Espaço Público, Direitos do Entorno Laboral, Direitos em Entornos Específicos e, por fim, de Garantias e Eficácia.

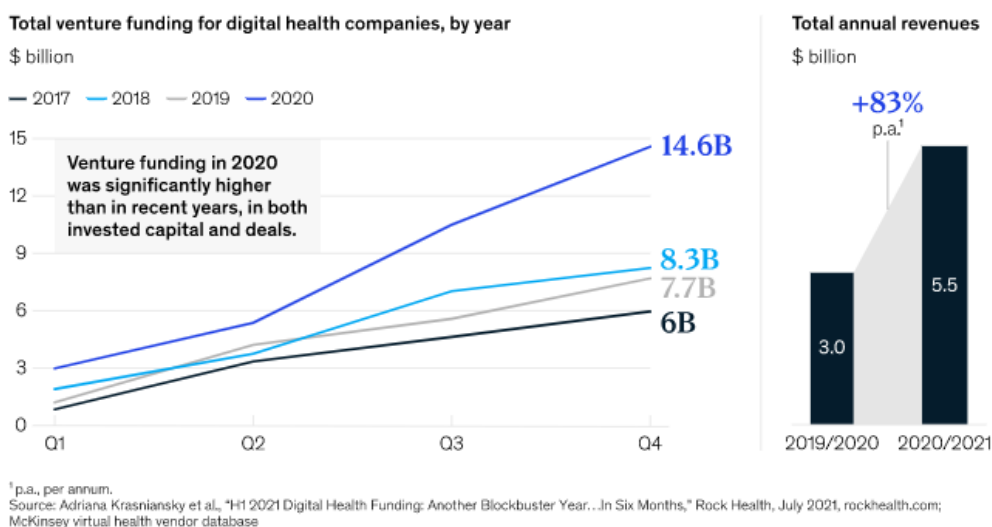
Como Direitos de Liberdade são tratados o direito à Identidade, proteção de dados, anonimato, a não ser localizado e perfilado, cibersegurança e herança digital. Como Direitos de Igualdade são tratados os temas de direito à não discriminação, ao acesso à Internet, proteção de menores de idade, acessibilidade universal, desigualdades de acesso ao espaço digital. Os Direitos de Participação e Espaço Público tratam de temas como neutralidade da

² Trata-se de um guia para orientar projetos, ações e legislações adotadas pelo Governo da Espanha, de acordo com o Plano de Recuperação e Resiliência 2030, com base nas leis já existentes: Lei Orgânica 1/1982 sobre proteção civil do direito à honra, à privacidade pessoal e familiar e à imagem; Lei Orgânica 2/1984, sobre direito à retificação de informações; Lei 34/2002 sobre serviços da sociedade da informação e de comércio eletrônico; Lei 34/2014 das Telecomunicações; Lei 7/2010 sobre Comunicação Audiovisual; Lei Orgânica 3/2018 sobre proteção de dados pessoais; Real Decreto-Lei 28/2020 e Real Decreto-Lei 10/2021 ambos sobre trabalho à distância (teletrabalho).

Internet, liberdade de expressão e de informação, receber informação veraz (combate às *fake news*), participação cidadã, educação digital e direitos da cidadania nas relações com as administrações públicas.

Figura 3- Investimentos em saúde digital entre 2017 e 2020

Investment in digital health and the revenues of telehealth players almost doubled compared to 2019.



Fonte: Mckinsey, 2021 em <https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality>

Os Direitos de Entorno Laboral e Empresarial tratam de temas como direitos trabalhistas e comportamento e práticas das empresas no espaço digital. Os Direitos em Entornos Específicos tratam de temas como acesso a dados com fins de interesse público, pesquisas científicas ou históricas, estatísticas, inovação e desenvolvimento; direito ao desenvolvimento tecnológico sustentável, liberdade de criação e acesso à cultura, liberdade diante da Inteligência Artificial, das neurotecnologias; por fim, como um dos entornos específicos, está o direito à proteção à saúde.

Vejamos o que diz a Carta sobre o direito à saúde no espaço digital:

XXIII Derecho a la protección de la salud en el entorno digital

1. Con arreglo a las normas de todo rango que resulten aplicables, todas las personas tendrán acceso a los servicios digitales de salud en condiciones de igualdad, accesibilidad y universalidad, así como a la libre elección de la asistencia presencial. Se adoptarán medidas para garantizar este acceso y evitar la exclusión de colectivos en riesgo.

2. Los poderes públicos promoverán que la investigación y la tecnología contribuyan al logro de una medicina preventiva, predictiva, personalizada, participativa y poblacional.

3. El sistema de salud promoverá el desarrollo de sistemas de información que aseguren la interoperabilidad, el acceso y la portabilidad de la información del paciente.

4. El empleo de sistemas digitales de asistencia al diagnóstico, y en particular de procesos basados en inteligencia artificial no limitará el derecho al libre criterio clínico del personal sanitario.

5. Los entornos digitales de salud garantizarán, conforme a la legislación sectorial, la autonomía del paciente, la seguridad de la información, la transparencia sobre el uso de algoritmos, la accesibilidad y el pleno respeto de los derechos fundamentales del paciente y en particular su derecho a ser informado o renunciar a la información y a consentir en el tratamiento de sus datos personales con fines de investigación y en la cesión a terceros de tales datos cuando tal consentimiento sea requerido.

6. Los poderes públicos impulsarán el acceso universal de la población a sistemas de telemedicina y teleasistencia, así como a los dispositivos tecnológicos desarrollados con fines terapéuticos o asistenciales en condiciones adecuadas de conectividad. Se procurará establecer que el acceso a estos dispositivos cuando se facilite a título gratuito por un fabricante o proveedor no pueda condicionarse a la cesión a aquellos de los datos personales del paciente. (España, 2021; p. 27)

Merece destaque a clara manutenção do princípio de universalidade dos serviços de saúde, a escolha do cidadão pelo serviço presencial ou digital, para isso todos os cidadãos devem ter acesso à Internet, que em si mesmo já compõe outro capítulo de Direitos Digitais enquanto infraestrutura vital para a inclusão social e produtiva das pessoas.

Também se enfatiza que, mediante o uso adequado da saúde digital ela prestará importantes serviços de prevenção e personalização ao nível individual, simultaneamente a uma epidemiologia e vigilância sanitária mais eficientes tanto pelo volume de informações em tempo real (*big data*) quanto pela IA identificando padrões e alertas de novos cenários populacionais.

O uso da IA não pode prescindir da avaliação criteriosa do profissional de saúde, assim como as informações dos indivíduos e seu histórico médico devem ser armazenados com segurança, em sistemas interoperáveis e com plena portabilidade para o paciente (controle sobre seus dados). Nenhum hospital ou seguradora pode reter os dados nem os guardar de forma inacessível ao sistema nacional de saúde.

Cabe sempre ao paciente/cidadão a palavra final sobre onde guardar ou não os dados, ceder as informações para pesquisa e outros usos, e ser especialmente informado quando um algoritmo (IA) tome decisões sobre sua saúde, podendo aceitar ou não tal decisão.

Por fim, os sistemas nacionais de saúde devem assegurar o direito de acesso à telemedicina e teleassistência, como também impedir que empresas de saúde privada

condicionem a oferta de equipamentos e interfaces para atendimento à distância à cessão de propriedade das informações.

Como enfatizado por Andrès (2021) “a Carta pode servir a propósitos além dos de um documento pré-legislativo. Por exemplo, ela pode ser utilizada para a promoção ativa por parte das autoridades públicas de códigos de conduta inspirados nos princípios do texto. Ou para a promoção de políticas públicas digitais. Da mesma forma, é uma ferramenta interpretativa útil para certos conceitos que são difusos na legislação atual. Ou, finalmente, constitui o início de um debate sobre novos direitos digitais que até agora não foram positivados e a forma como eles devem ser modulados, como no caso do uso de neurotecnologias”.

Em resumo, para assegurar o direito universal à saúde no estágio do capitalismo informacional, é preciso regular o mercado e estabelecer novos pactos entre Estado e Sociedade de tal maneira que fiquem assegurados os direitos constitucionais já existentes e, eventualmente, atualizar as Constituições e Leis para incluir os novos direitos digitais que interferem no espaço real-digital de vida, produção e convivência. A importância da Carta de Direitos Digitais se reveste também de oportunidade, diante da necessidade urgente de formar massa crítica na sociedade para reelaborar as normas e leis no espaço digital – um código de conduta, como formador de hábito e de consciência.

2 Novas tecnologias para sistemas nacionais de saúde, consequências e limites: dados em DLT (Blockchain), ID (identidade digital), universalidade e ubiquidade

A transformação digital da saúde não está apenas na utilização ampla da Internet das Coisas (IoT), onde máquinas com sensores (muito além da UTI, em aplicativos e *wearables*) continuamente mandam informações a máquinas de armazenamento e processamento, identificação de padrões e não conformidades, emissão de alertas e prevenção de problemas através de “*Analytics & Big Data*”. Da mesma forma, a e-saúde não significa apenas o atendimento à distância de pacientes, oferecer um diagnóstico com análise de IA, ou recomendar, prescrever e monitorar procedimentos, fármacos e atividades de maneira eletrônica e registrando tudo no histórico médico e comportamental da pessoa. Apesar da importância dos novos modelos de negócio em saúde baseados nessas tecnologias de atenção médica, onde a informação e a comunicação são o “core business”, exigindo uma formação profissional diferenciada, reservando o presencial para atendimentos de maior complexidade, a saúde digital não se define somente por esse aspecto.

Pode-se juntar todos esses elementos, que por si só já têm relevância, e o principal ainda estará em outro aspecto: a instituída relação médico-paciente, até recentemente pessoal e intransferível, agora é mediada por máquinas e suas linguagens; a memória do médico de família está num banco de dados, que por meio de outros sistemas de dados conhecerá seus

hábitos de vida e consumo, deslocamentos e medicamentos, vacinas etc.; o paciente, por seu turno, estará informado pelas redes, para bem ou para mal – como as campanhas antivacinas durante a recente pandemia de Covid-19 e uso de falsos “tratamentos precoces”; cada pessoa poderá usar aplicativos para fazer exercícios, monitorar medicamentos e indicadores vitais; produtor e consumidor de dados e informações, pode tornar-se mais proativo com sua saúde e receber recompensas das seguradoras, como num *game*, a cada objetivo alcançado.

Foi necessário uma pandemia como a de 2020-2021 para que médicos e pacientes, políticos e governos se dispusessem a permitir amplamente o uso da telemedicina, embora os cientistas de dados, epidemiologistas, bioinformatas, dentre outros, já utilizassem IA e Big Data há muito tempo, sem que a população nem os políticos se dessem conta ou se preocupassem com as suas consequências. Prestadores de serviços privados e suas plataformas mantêm os dados de seus pacientes sob controle, vendem as informações, enfim, já se sabe como é difícil hoje reunir todos os dados médicos que uma pessoa possui em diferentes unidades de saúde.

As mudanças importantes da transformação digital na saúde acontecem no âmbito dos costumes, da cultura, das regras do jogo social, enfim, das instituições sociais. Elas exigem novas normas formais para garantir os direitos de todos durante a fase de transformação. Podemos começar com o direito à Identidade Digital, para exemplificar. Para acessar os serviços de saúde digitais, públicos ou privados, é necessário identificar o beneficiário ou cliente, tendo por base um conjunto de informações que garantem que se trata efetivamente daquela pessoa, da mesma maneira que hoje se utiliza para acessar uma conta bancária. **Ter essa identidade digital protegida** - com seus dados pessoais, histórico médico e todo o imenso conjunto de informações do seu prontuário- atendimentos, diagnósticos, resultados de exames, prescrições, medicamentos etc. – **é um direito digital. Para haver universalidade no sistema nacional de saúde é preciso ter a garantia da identidade digital e da proteção dos dados.**

Para proteger os dados e, ao mesmo tempo, garantir que os serviços possam acontecer com ubiquidade, isto é, em qualquer ponto do território e por prestador público ou privado, a base de dados deve ser dotada de características de criptografia, descentralização e interoperabilidade. Tal base de dados deve permitir minimamente os seguintes produtos: identidade digital, histórico médico, receita eletrônica, monitoramento de indicadores vitais e comportamentais de relevância (como alcoolismo, tabagismo, sedentarismo etc.) e conectar-se com aplicativos em celulares e outros sensores móveis. Por fim, destaca-se a cibersegurança, pois na maioria dos países com Leis específicas de cibersegurança os sistemas de saúde e hospitais são considerados infraestruturas críticas, que devem ser protegidas prioritariamente.

Segundo a OPAS³ – Organização Panamericana de Saúde – em seu relatório após a conferência com os países associados sobre sistemas de informação para saúde (IS4H), são 8 princípios que devem guiar as tecnologias de informação e comunicação em sistemas nacionais de saúde:

1. Alcançar a conectividade universal para saúde;
2. Criar bens de saúde pública para garantir a equanimidade;
3. Acelerar os progressos para saúde digital inclusiva, especialmente para os mais vulneráveis;
4. Implantar sistemas de saúde e informação digital de código aberto, sustentáveis e interoperáveis;
5. Integrar os direitos humanos a todas as áreas da transformação digital na saúde;
6. Participar da cooperação mundial em IA e toda nova tecnologia com aplicação nos sistemas de saúde;
7. Estabelecer mecanismos para confidencialidade e segurança da informação no âmbito da saúde digital;
8. Desenhar uma estrutura de saúde pública digital renovada para a era da interdependência digital.

Para implementar a atualização das relações Estado-Sociedade-Mercado no campo da saúde é necessário: a) pactuar ao menos dois princípios como expressão de direitos digitais das pessoas – identidade digital e propriedade dos dados; b) construir uma infraestrutura segura para armazenar e processar os dados de maneira descentralizada e, ao mesmo tempo, acessível e interoperável pelos nós da rede de saúde (ubiquidade), sejam eles públicos ou privados; c) garantir o direito de acesso à Internet - como rede vital para receber serviços de saúde em telemedicina e teleassistência, prevenção e personalização dos atendimentos, elevando a esperança de vida com qualidade de vida; d) trabalhar com transparência as parcerias público-privadas no histórico médico, no atendimento à distância, no suprimento de fármacos e outros insumos, nos custos dos serviços e produtos e principalmente no uso da IA para diagnóstico, prescrição, monitoramento e gestão dos serviços de saúde.

Para atingir esses quatro objetivos para uma transformação digital do sistema nacional de saúde que seja inclusiva, universal, segura e com total transparência dos algoritmos, sem submeter os cidadãos e seus dados ao controle de plataformas privadas, a mais moderna tecnologia de dados armazenados descentralizados (DLT – *decentralized ledger technology*)

3 Ver OPS, 2021.

está disponível: é a blockchain. Ao contrário das soluções em nuvem (cloud), onde as informações são armazenadas de forma centralizada e sob controle das empresas big tech e suas plataformas, a solução de descentralização das bases de dados criptografados e organizados em cadeias de blocos impede que um ator ou poucos atores controlem o sistema, alterem informações e incluam critérios de processamento sem o conhecimento e aprovação do conjunto dos nós da rede.

O que é uma blockchain e como ela funciona? O Blockchain pode ser descrito como um registro imutável que compila as entradas de dados de forma descentralizada. Ele permite que as entidades interajam sem a presença de uma terceira parte de confiança. A cadeia de blockchain mantém um conjunto de entradas de dados em contínuo crescimento, agrupados em blocos de dados. Estes blocos são, mediante aceitação à cadeia de blocos, ligados aos blocos anteriores e futuros com protocolos criptográficos. Na forma original da blockchain, estes registros/blocos de dados são; legíveis por todos, graváveis por todos, e à prova de adulteração por todos. Isto, por exemplo, permite transações descentralizadas e gerenciamento de dados. Além disso, o blockchain permite contratos inteligentes; contratos de auto execução que não requerem nenhuma autoridade central (HASSELGREN et All, 2020; p.2).

Blockchain é, portanto, um tipo de software de código aberto que permite armazenar e transmitir informações de forma descentralizada e segura graças à matemática que lhe dá estrutura lógica, criptografando as informações numa cadeia ou sequência de blocos quase impossível de ser manipulada ou alterada. Todos os nós da blockchain – conjunto de computadores espalhados pelo mundo – possuem cópias da sequência criptografada e para incluir um novo bloco de informações o “mineiro” deve resolver matematicamente um problema (*proof of work* – *PoW* - como mecanismo de consenso), e uma vez encontrada a solução (número *hash*) a informação é validada pelos demais nós (no mínimo 51% dos nós estarão de acordo) e atualiza-se a blockchain. A mais conhecida blockchain é a que sustenta a primeira criptomoeda digital emitida em 2009, sem vínculos com um Estado ou conjunto de Estados (por ex., o Euro), a Bitcoin⁴.

Em poucos anos muitas outras criptomoedas surgiram, com diferentes características matemáticas e comerciais, causando forte impacto nos sistema financeiro e monetário global. Como se isso já não fosse suficientemente transformador, jovens cientistas de dados associados a outros empreendedores dos mais variados campos de conhecimento vem se associando para lançar um imenso número de *startups* que encontraram na tecnologia

⁴ Ver Livro Branco da Bitcoin, escrito por um pseudônimo Satoshi Nakamoto, em 2008, em <http://satoshinakamoto.me/bitcoin.pdf>

blockchain a solução, livre das plataformas big tech, para novos negócios também transformadores. Muito além das Fintech e das DeFi (finanças descentralizadas) que vem disputando intensamente com o sistema financeiro tradicional o mercado de capitais, de divisas, de seguros, de meios de pagamentos e tantas outras soluções financeiras simples, baratas e sem intermediação, as blockchain estão sendo usadas como infraestrutura para sistemas de informação (bancos de dados) e transações (compra, venda, pagamentos) em: cadeias de logística e suprimentos (principalmente exportações e importações); educação (históricos, certificados e diplomas); registro de imóveis e mercado imobiliário; saúde.

Outra importante função que uma blockchain desempenha é associar “contratos inteligentes” (*smart contracts*) às transações em sua cadeia de blocos, que implica em automaticamente executar determinados comandos preestabelecidos entre os usuários através de um algoritmo que verifica as condições de atendimento. Uma vez dada a permissão (assinatura do “contrato” com sua chave privada (senha), o processo todo se automatiza. É um recurso extremamente útil para infinitas aplicações, como será visto adiante. Os *smart contracts* são maiormente aplicados na blockchain Ethereum e outras que compõem seu “ecossistema”.

Esses contratos inteligentes são provavelmente a tecnologia de cadeia de bloqueio com maior potencial para afetar, ou mesmo revolucionar, todos os tipos de transações, desde a execução de acordos legais até o IoT (MAKRIDAKIS, 2019, p. 10).⁵

A grande contribuição oferecida pela blockchain é a capacidade de criar e manter registros incorruptíveis de trocas monetárias, de produtos ou de trabalho sem intermediário centralizado, como, por exemplo, um banco (GERHARDT, 2020; p. 4). No momento atual, percebe-se o desenvolvimento das tecnologias de segunda e terceira geração de blockchain, que vão além da captura de transferências de valor para estabelecer sistemas completos de trocas de valor usando contratos inteligentes.⁶

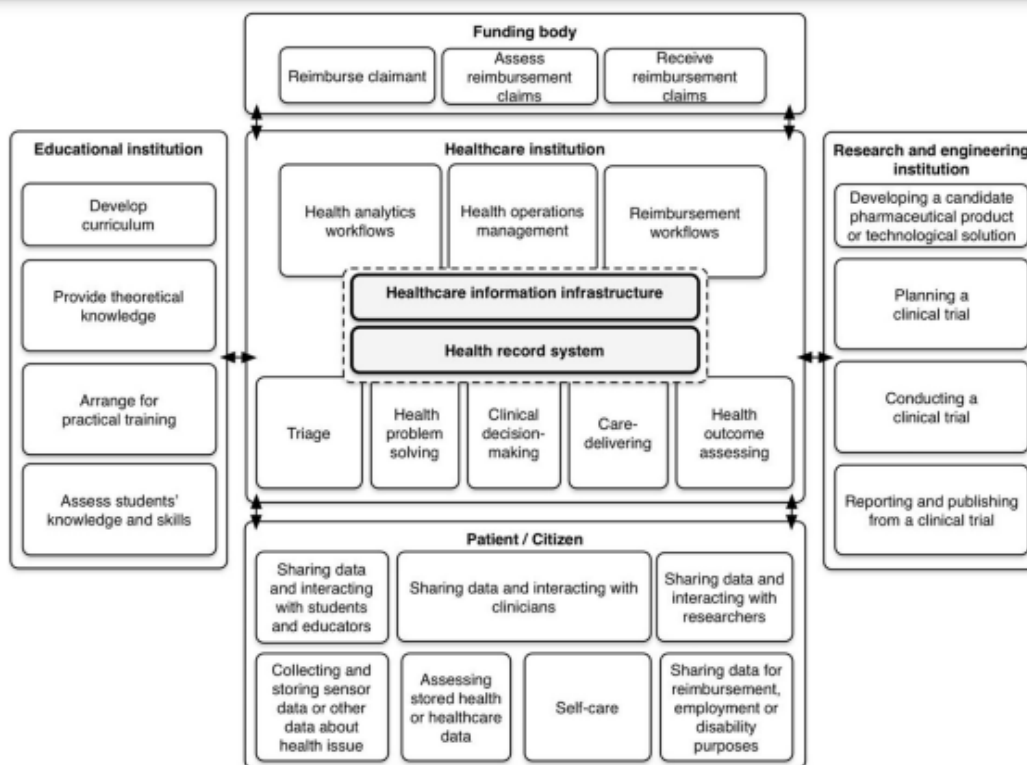
A Figura 4 mostra um modelo de intercâmbio de informações entre os atores de um sistema de saúde enquanto executam suas funções no arranjo produtivo. Todas essas informações, ao nível individual e ao nível coletivo/populacional tem relevância, interfere nos

⁵ Os contratos inteligentes encapsulam o código algorítmico que é servido por uma rede *peer-to-peer*. Por exemplo, um contrato inteligente pode ser instanciado para impor algoritmicamente os termos de um acordo sem a necessidade de um documento legal tradicional. Em tais casos, os contratos inteligentes permitem a realização de transações sem advogados ou notários. As transações são rastreáveis e irreversíveis e não exigem que os tribunais e juízes sejam executados (MAKRIDAKIS, 2019, p. 10).

⁶ Um contrato inteligente é um programa tipo "se-então" em que um determinado evento é acionado se uma determinada condição for atendida, o que pode ser avaliado por sistemas *peer-to-peer* ou automatizados. (GERHARDT, 2020; p. 4)

direitos dos cidadãos e passam a receber um adequado tratamento com a tecnologia blockchain.

Figura 4- Arranjo produtivo em saúde e sistema de informações em saúde.



Fonte: HASSELGREN et All, 2020, p.3.

Os autores consideram a vital e crescente importância de informações que circulem entre os atores do arranjo produtivo em saúde, que sejam confiáveis, imutáveis, verificáveis desde sua origem e que respeitem os direitos dos cidadãos, dentre outras garantias. Descrevem como se dá essa circulação e utilização de informações que compõem um sistema de informações em saúde.

Tanto para manter a privacidade do paciente quanto para trocar dados com outras instituições no ecossistema de saúde, o controle de acesso, proveniência, integridade dos dados e interoperabilidade são cruciais. A forma tradicional de conseguir o controle de acesso comumente assume a confiança entre o proprietário dos dados e as entidades que os armazenam. Essas entidades são frequentemente servidores totalmente responsáveis para definir e fazer cumprir as políticas de controle de acesso. Interoperabilidade é a capacidade dos diferentes sistemas, dispositivos ou aplicações de informação de conectar, de forma coordenada, dentro e além das fronteiras organizacionais, para acessar, trocar e usar os

dados cooperativamente entre as partes interessadas, com o objetivo de otimizar a saúde dos indivíduos e das populações (Idem, p.3-4).

Segundo os autores, a proveniência dos dados refere-se ao registro histórico dos dados e suas origens. No domínio da saúde, a proveniência pode, por exemplo, ser a capacidade de auditoria e transparência em RSE, e a confiança no sistema de software de RSE. A integridade dos dados é a definição de qualidade dos dados que trata da qualidade esperada dos dados. Isto significa que o grau em que a qualidade esperada dos dados é atingida ou excedida determina a integridade dos dados. Com alguns de seus principais atributos como descentralização, distribuição e integridade dos dados, e sem qualquer necessidade de intervenção de terceiro, a tecnologia blockchain tem muitas propriedades atraentes que poderiam ser utilizadas para melhorar e obter um nível mais alto de interoperabilidade, compartilhamento de informações, controle de acesso, proveniência e integridade dos dados entre as partes interessadas, caminhando assim para uma nova infra-estrutura para construir e manter a confiança.

Esse estudo de Hasselgren *et al.* também informa sobre como o sistema de saúde está efetivamente utilizando a blockchain para seus sistemas de informação e processamento, como mostra a Figura 5. A maior parte das aplicações foram desenvolvidas sobre a infraestrutura de Ethereum, são chamadas de redes públicas e utilizam como mecanismo de consenso PoW.

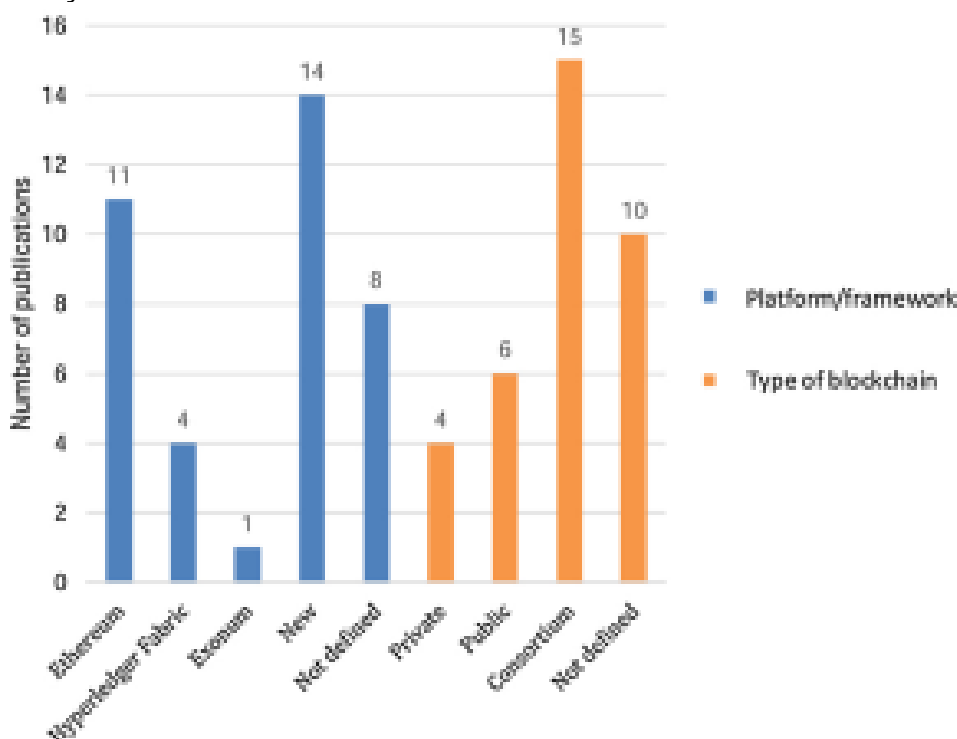
Em blockchain, o adjetivo “pública” não se refere à propriedade e sim ao acesso, livre a qualquer pessoa que pode baixar a base de dados, ser um “mineiro” validador ou apenas acessar a rede. As blockchain privadas, da mesma maneira, não significa propriedade exclusiva, mas sim o acesso de validação ou consenso que é feito apenas para nós autorizados. Os autores destacam que os consórcios são a solução principal para operar as blockchain em saúde, isto é, são blockchain em parte públicas e parte privadas.

Nas palavras de (HASSELGREN et Al, 2020, p.8), “um consórcio de blockchain parece ser a escolha preferida quando se trata do tipo de blockchain. Como o HIS trata de dados altamente sensíveis, o que geralmente implica que um número limitado de entidades deve ter acesso, um consórcio de blockchain pode ser mais apropriada do que um blockchain sem permissão pública e/ou privado para garantir que os dados não sejam acessíveis por aqueles que não têm direitos de visualização e também para cumprir com os regulamentos atuais de dados de saúde”.

É necessário esclarecer que um dos pontos críticos da blockchain pública é o consumo elevado de energia, decorrente do esforço de resolver a questão matemática do *hash* que é exigida para consenso da rede mediante PoW. Ethereum está finalizando um processo de

instalar um novo mecanismo de consenso, mais inteligente e de baixo consumo de energia, recorrendo a outras fórmulas matemáticas que assegurem a descentralização, a traçabilidade e a confiança hoje existentes. Trata-se de mecanismos de consenso baseados em um misto de *proof of stake* – PoS, onde os nós da rede mantem um investimento na criptomoeda ou token usado como meio de pagamento das transações – com fórmulas de probabilidade para aleatoriedade dos nós que farão a validação do *hash*. Um exemplo disso é a blockchain Avalanche⁷, com seu token AVAX, que usa um mecanismo de consenso chamado SNOW.

Figura 5 – Tipos de blockchain e plataforma tecnológica utilizada em sistemas de informação em saúde



Fonte: HASSELGREN et Al, 2020, p.7

Outros autores recentemente vem investigando os impactos e as possibilidades da tecnologia blockchain em saúde, com indicações muito positivas devido às características desse tipo de DLT. MAKRIDAKIS (2019) aponta que registros médicos precisos e detalhados são essenciais para o bem-estar dos pacientes, pois contêm informações valiosas sobre sua história médica, necessárias para fins de diagnóstico e para melhorar a decisão do médico examinador sobre o(s) tratamento(s) sugerido(s). Argumentando que as preocupações com privacidade, incluindo o armazenamento seguro de dados médicos, são fundamentais, o que significa que as informações médicas devem ser prontamente disponibilizadas ao pessoal

⁷ Ver página de Avalanche em <https://www.avax.network/>

médico qualificado, especialmente para casos de emergência ele pondera que tais informações devam ser protegidas de partes não autorizadas (as companhias de seguro médico estariam extremamente interessadas nos registros médicos de clientes potenciais ao decidir se devem ser aceitos/rejeitados e quais os prêmios a serem cobrados). Makridakis conclui que a tecnologia Blockchain oferece uma solução ideal para fazê-lo, pois a segurança é garantida, enquanto a pessoa envolvida pode decidir quem, quando e que partes de seus registros médicos podem ser divulgadas. Dada a importância de ter registros médicos verdadeiros e continuamente atualizados para todos os seus cidadãos, os países estão encorajando o desenvolvimento de tal sistema que converteria todas as informações médicas disponíveis atualmente em formato digital, usando o mesmo sistema não apenas em um único país, mas até mesmo em nível regional ou global, para que as informações pudessem ser compartilhadas mesmo quando viajando longe de casa. (MAKRIDAKIS, 2019, p.7)

Da mesma forma, AGBO (2020) entende que a base de dados em saúde é seu ponto crítico atualmente, exigindo uma solução com confiança, interoperabilidade das diversas fontes de dados, sob controle dos proprietários dos dados, isto é, dos pacientes /cidadãos, tanto para atendimento pessoal quanto para pesquisa epidemiológica, desenvolvimento de protocolos, fármacos etc.

Agbo (2020) sugere que, ao defender um atendimento personalizado e proativo, os serviços de saúde devem aproveitar o conhecimento oculto em dados maciços que são gerados a partir de vários dispositivos de monitoramento médico e registros médicos de pacientes (PMRs).

“A transformação de dados em conhecimento é a marca registrada da medicina moderna. Tal conhecimento oferece potenciais significativos a serem utilizados para promover tratamentos personalizados (Shae; Tsai, 2018) e para a detecção precoce de doenças em análises preditivas (Agbo; Mahmoud; Eklund, 2018a; 2018b). No entanto, os esforços para extrair conhecimento dos dados podem ser inúteis se esses dados forem armazenados em diferentes bancos de dados com pouca ou nenhuma capacidade interoperável; além disso, tais dados podem ser armazenados em formatos que dificultam o compartilhamento de dados. Além disso, os dados coletados podem ser incompletos, não confiáveis ou potencialmente comprometidos (Mettler, 2016). Enquanto isso, o acesso aos dados médicos pelos interessados na saúde ainda deve ser controlado, pois a segurança e a privacidade dos dados dos pacientes devem ser protegidas. Portanto, os serviços de saúde modernos devem ser projetados para serem colaborativos, abertos e transparentes, sem comprometer a integridade dos dados ou a privacidade dos pacientes, os proprietários e fornecedores finais desses dados.” (AGBO, 2020, p.82).

A saúde, de fato, representa uma área significativa onde existem várias oportunidades para a aplicação de conceitos de blockchain. Na pesquisa e educação biomédica, blockchain tem sido aplicado com sucesso em vários casos. Em ensaios clínicos, por exemplo, blockchain pode ser aplicado para evitar a manipulação dos resultados da pesquisa clínica (Radanović; Likić, 2018). De fato, como o blockchain permite a anonimização de dados de saúde, os pacientes podem ser encorajados a disponibilizar seus dados de saúde para estudos clínicos (Boulos, Wilson & Clauson, 2018) e a integridade desses dados pode ser certificada com base na imutabilidade do blockchain. Além disso, dada a natureza transparente e aberta do blockchain, a pesquisa gerada a partir de dados baseados em blockchain seria mais fácil de replicar. Há também o potencial do blockchain para revolucionar o processo de revisão por pares para publicações de pesquisa clínica com base em suas propriedades de transparência, imutabilidade e descentralização (Roman-Belmonte et al, 2018). Da mesma forma, Funk et al (2018) defendem o uso potencial do blockchain na educação das profissões da saúde (AGBO, 2020, p.83)

Em suma, parece estar se tornando mais claro a importância de um sistema de informações em saúde em DLT, dos quais a blockchain é a tecnologia com mais amplo e longo período de testes em diversos setores e aplicações, suportando, até o momento, a condição de inovação segura e de progresso muito rápido para sistemas de informação de código aberto, descentralizados e sem intermediação, capaz de cumprir os direitos digitais dos cidadãos.

3 Modelos consorciados possíveis para o SUS digital

Os sistemas nacionais de saúde, como o SUS no Brasil, encontram-se numa encruzilhada rumo à digitalização. Como se já não fosse suficientemente disruptiva, essa transformação tem impactos e consequências sobre todo o funcionamento do Estado, seu sistema de informações orçamentárias e o próprio gerenciamento das funções públicas. Busca-se, neste tópico, entender em que consiste essa transformação, suas possibilidades e consequências para o SUS e, em seguida uma primeira leitura do que isso implica para o próprio funcionamento do Estado.

O modelo atual dos sistemas de saúde trata a informação de maneira opaca aos cidadãos e apresenta uma série de características que já não são aceitáveis na economia digital, resultando em serviços com menor qualidade para a sociedade e para as pessoas. É um sistema disperso, inseguro e com muitas perdas de valor ao longo do fluxo produtivo. As principais características dos sistemas de saúde “analógicos” são:

1. Pagamentos de saúde com muitos intermediários, comissões e impostos

2. Controle de dados armazenados por governos e empresas privadas de saúde ou seguros, centralmente em cada empresa e fragmentadas
3. Baixa conectividade e interoperabilidade entre níveis de governo ou entre empresas prestadoras de serviços, fornecedores, setor financeiro, etc.
4. Dados pessoais de conteúdo médico e financeiro quase inatingíveis para cidadãos e espalhados em diferentes silos de informações
5. Muitos intermediários
6. Uso de informações valiosas sem autorização ou recompensa ao usuário
7. Sérios problemas de segurança, crimes e perda de informações ao longo do tempo
8. Os cidadãos não sabem os custos dos serviços de saúde

Para atualizar os sistemas nacionais de saúde, a proposta é utilizar uma infraestrutura em blockchain, descentralizada e segura, dotada de *smart contracts* e com autorizações e análises gerenciais realizadas rotineiramente por IA, cujas principais características são:

1. Pagamentos imediatos para serviços e produtos de saúde seja P2B ou B2B
2. Controle de dados pessoais e pagamentos feito pelos cidadãos
3. Informações se tornam de valor reconhecido
4. Unificação de dados em uma base descentralizada/distribuída, com acesso mediante autorização pelos oráculos científicos e gerenciais
5. Segurança também por criptografia com chaves pública (como a conta de banco) e privada (senha pessoal)
6. Dados imutáveis e rastreáveis, com privacidade garantida
7. Autogestão e sistema sem intermediários
8. Interoperabilidade entre os nós da cadeia (atores públicos e privados, saúde, financeiro, logística, supervisão e fiscalização etc.)
9. Ubiquidade dos serviços
10. Pode recompensar usuários e fornecedores automaticamente
11. Redução de custos em geral e também em seguros contra golpes ou erros do sistema

No Brasil, segundo relatório da OECD de 2019, do ponto de vista do *funding*, o sistema nacional de saúde opera com 43% dos recursos de origem pública (Estado) e os demais 57% de origem privada (empresas e seguros, ou recursos das famílias), como mostra a Figura 6. Todos esses atores que pagam pelos serviços de saúde devem ter a mesma base de dados em um sistema interoperável com outras necessidades e redes de interesse da sociedade. Da mesma maneira, o ICEX/Espanha descreve o mercado brasileiro de serviços de saúde no Quadro 1, a partir de dados da ABIIS, ABIMO e Banco Mundial, levando em conta os subsetores de laboratórios, médico-hospitalares, radiologia/imagem, odontologia, implantes, material de consumo médico-hospitalar, TIC para saúde.

Considerando a estrutura do mercado brasileiro de serviços de saúde dividido entre SUS (sistema público), SAMS (sistema suplementar, privado, de seguros de saúde) e Sistema Privado (desembolso direto), muitas novas empresas estão surgindo no nicho de e-saúde. O ICEX avalia que o mercado brasileiro é sem dúvida uma excelente oportunidade para as empresas espanholas e, mais especificamente, para o setor de saúde eletrônica ou digital, que, embora esteja em um estágio inicial de desenvolvimento, tem uma projeção e expectativas muito altas. Parte dessas expectativas se deve ao fato de que o governo brasileiro se comprometeu a desenvolver o setor em 2016 com vistas a 2020, que embora tenha sido atrasado pela pandemia, atualmente dentro do sistema de saúde pública (SUS), produtos e tecnologias voltados para a saúde digital já estão começando a ser desenvolvidos e implementados. Finalmente, o desenvolvimento e o uso da telemedicina no Brasil nos anos anteriores ajudou muito a aliviar a COVID-19, e se apresenta como o nicho de mercado com o maior crescimento em 2020. (ESPAÑA/ICEX, 2021, p.6-7)

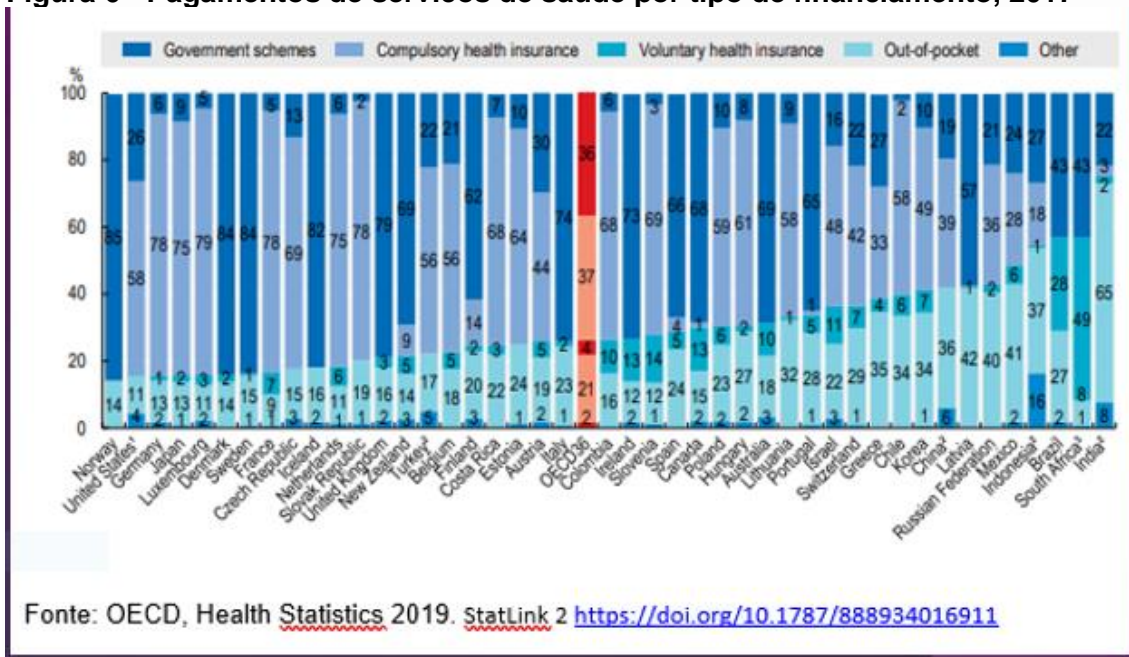
Quadro 1- Dados sobre setor de serviços de saúde no Brasil

Métricas	Datos
Población (millones de habitantes) 2020	211
PIB 2020 (millones de USD)	3.078.900
Crecimiento del PIB real	-4,1 %
PIB per cápita 2020 (USD)	14.560
Gasto total en sanidad (% PIB)	9,51 %
% del gasto sanitario a cargo de los pacientes	57,14
Facturación de dispositivos médicos	5,8 %
Esperanza de vida H/M (2019)	73,1 / 80,1
Brasil es el 7.º mercado mundial en el área de salud	
Más de 5.200 hospitales y más de 45.000 clínicas especializadas	
6.215 millones de USD en importaciones de dispositivos médicos (2020)	

Fonte: ESPAÑA/ICEX, 2021, p. 1.

O Brasil possui em 2021 **747 healthtechs**, segundo publicação da revista Medicina S/A, divididas em nove categorias distintas. A maior parte dessas startups volta-se para soluções relacionadas à Gestão e Prontuários Eletrônicos (25%). Em seguida, estão as que atuam com Acesso da Informação (16,7%) e como Marketplace (12,6%). As *healthtechs* de Telemedicina (11,8%) e aquelas que se voltam às áreas Farmacêutica e Diagnóstico (10%) também possuem fatias importantes deste mercado. Quanto à distribuição por Estados, a maior concentração está no Sudeste, liderado por São Paulo, com 44% das *healthtechs*, Minas Gerais, com 10,4%, e Rio de Janeiro, com 9,1%. Rio Grande do Sul aparece logo em seguida, com 8,9%. A região Norte do País, especificamente Manaus, abriga apenas 0,4% do total. (<https://medicinasa.com.br/healthtechs-brasil/>)

Figura 6 - Pagamentos de serviços de saúde por tipo de financiamento, 2017



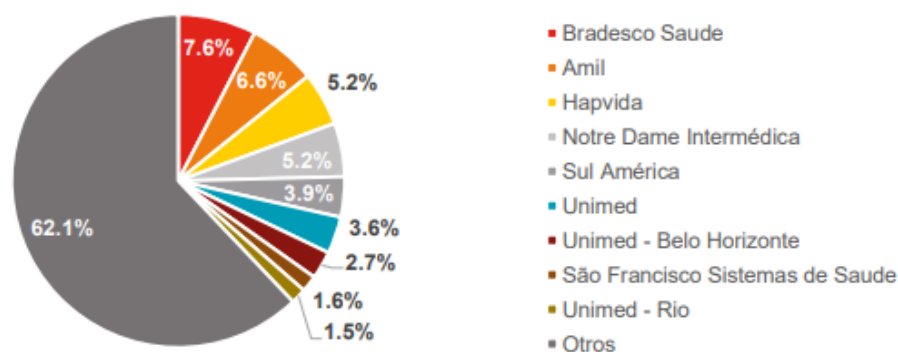
São listadas como relevantes pelo ICEX no mercado privado as empresas e suas fatias de mercado como mostra a Figura 7. Já a pesquisa Medicina/SA e Doctoralia destaca as seguintes *healthtechs*: [Amplimed](#), [Anestech](#), [Benner](#), [Bionexo](#), [Doc24](#), [Doctoralia](#), [Elsevier](#), [Mobile Saúde](#), [MV](#), [Nexodata](#), [Pixon](#), [Pluginbot](#), [Rfxcel](#), [Vibe Saúde](#). Seus serviços digitais são bem amplos e se apresentam como inovação e solução viável para uma população que hoje é atendida pela SAMS e SPrivada, com atendimento remoto integrado ao prontuário eletrônico, com tecnologia e inteligência de dados perioperatórios buscando eficiência e segurança para anesthesiologias e centros cirúrgicos, soluções e processos para atendimento médico digital, inteligência em compras na saúde para hospitais e clínicas, serviços de telemedicina; Inteligência artificial e consultórios inteligentes, atenção dada à jornada do paciente, tornando-a cada vez mais completa e inclusiva, apoio à operadoras de saúde com soluções inovadoras para telemedicina e autoatendimento, prontuário eletrônico e prescrição eletrônica com gestão de logística integrada, robôs e atendimento à distância, telemedicina para a atenção primária e dezenas de Apps para adolescentes, prevenção, saúde mental, etc.

A pesquisa mostra também que, se por um lado, durante a pandemia a maioria das unidades privadas de saúde e seus pacientes adotaram a telemedicina (57%), por outro lado a tecnologia foi utilizada de maneira pouco profissional e insegura. De fato, “a telemedicina oferece um universo de possibilidades, principalmente na hora da escolha da ferramenta para realização do atendimento. Na pesquisa realizada, mais da metade das clínicas e hospitais (51%) ainda opta por plataformas de vídeo tradicionais gratuitas como – Zoom, Skype, WhatsApp ou Google Meet – mesmo que elas possam colocar em risco fatores como

segurança, armazenamento de dados, produtividade e experiência do paciente”.. (<https://medicinasa.com.br/pesquisa-clinicas-hospitais/>)

Figura 7 - Principais empresas de saúde privada no Brasil, 2020

CUOTA DE MERCADO DE LOS PRINCIPALES GRUPOS DEL SECTOR PRIVADO
Segmentación por porcentaje de participación en el sector privado



Fonte: ESPANHA/ICEX, 2021, p.6

No sistema público não é diferente, como informa uma reportagem sobre a vacinação e o sistema ConectSUS:

Falhas, inconsistências e até suspeitas de clonagem de dados rondam o ConecteSUS, ferramenta do governo federal que funciona como uma carteira digital de vacinação. O sistema entrou no ar neste ano e deveria servir para atestar que vacina cada brasileiro tomou e quantas doses. Mas já existem relatos de dados divergentes e até inexistentes sobre as vacinas contra a Covid-19⁸.

Além dos problemas de acesso à saúde por desigualdades territoriais e de renda, um estudo da OECD mostra que a América Latina tem dificuldades adicionais no avanço da saúde digital devido à falta de infraestrutura e custos de TIC, que somados à falta de profissionais qualificados para colocar em funcionamento um sistema de saúde complexo, resulta num cenário de reprodução e agravamento de desigualdades no acesso à saúde e na própria esperança de vida / qualidade de vida das populações carentes e excluídas.

A conclusão geral da pesquisa da OCDE, baseada na análise dos questionários e da documentação existente é que a maioria da região Latino-americana ainda se encontra em um estágio inicial de adoção e utilização das TICs na saúde. Um dos principais obstáculos para a implementação da saúde eletrônica na região é a falta de profissionais com as

⁸ (<https://saude.ig.com.br/2021-08-10/covid-falhas-conectesus-prejudicam-controle-vacinacao-brasil.html>)

habilidades e a experiência necessárias para desenvolver e implementar projetos de saúde eletrônica. Outro grande obstáculo tem sido as deficiências na infraestrutura tecnológica devido a conexões instáveis, largura de banda e espectro limitados, e altos custos de serviços (muitas vezes com altos custos iniciais (OECD, 2020).

Por fim, é necessário também compreender a urgência na regulação dos serviços de saúde digital no Brasil. Muitos países, nos seus planos de recuperação após a pandemia, tem assumido investimentos e mudanças regulatórias para implementar a e-saúde. A Alemanha aprovou o Digital Health Care Act já em 2019 e seu plano prevê inclusive apoio ao desenvolvimento de inovações em App que terão seus serviços/assinaturas pagas pelo reembolso público de saúde – Lei de Logística Digital em Saúde. De maneira geral, a União Europeia está discutindo a lei de serviços digitais e mercados digitais e já publicou normativo sobre IA – Livro Branco de IA. A França, além da regulação, já possui uma plataforma “Minha Saúde” com atendimentos e serviços de saúde digitais. Israel faz a regulação da e-saúde via portarias do seu ministério (MOH) e conta com mais de 500 startups de saúde digital em operação.

A Espanha acelerou a transformação digital com a pandemia e no seu plano de recuperação está um capítulo inteiro de investimentos e novas regulações para e-saúde, apoiados também nos programas da EU Horizonte Europa, Digital Europe y Europe4Health; a Estratégia de Saúde Digital está sendo analisada no Conselho Interterritorial de Saúde. Este Conselho se reveste de importância pois é o fórum onde as comunidades autônomas pactuam com o governo central todas as medidas e políticas de saúde. Justamente por isso a cada reunião do Conselho o governo de Madrid se contrapõe às demais CCAA e ao governo central, adotando há muitos anos uma política privatista da saúde. Alguns dados sobre os custos de serviços de saúde pública em Madrid mostram que os contratados junto a fundações privadas são até 6 vezes maiores que os da rede pública (dados publicados por El Diálogo⁹ em 20/07/20218). Especificamente um gestor da Fundação Jiménez considera muito rentável vender serviços para Madrid:

“La Fundación Jiménez Díaz pertenece al grupo Quirónsalud, que también gestiona tres hospitales de la red pública de Madrid (Villalba, Móstoles y Valdemoro). Quirónsalud es la antigua Capiro y fue comprada en 2017 por 5.760 millones de euros por el gigante alemán Fresenius, un gran grupo europeo de sanidad privada que admite que el negocio más rentable de la adquisición de Quirónsalud procede de los conciertos que tiene firmados con la sanidad pública, especialmente, la madrileña.” (Op Cit, p.3)

⁹ https://www.eldiario.es/madrid/fundacion-jimenez-diaz-comunidad-madrid_1_1929596.html

Durante a pandemia, os recursos extraordinários para a saúde durante 2 anos foram repassados às Comunidades Autônomas para enfrentar as despesas emergenciais, mas a política de Madrid manteve-se voltada à contratação de serviços privados, o que tem resultado em muitos conflitos públicos entre o Conselho Interterritorial de Saúde, os movimentos sociais e sindicais madrilenhos - que reivindicam o fortalecimento da rede pública - e o governo central. Assim, pode-se afirmar que as novas tecnologias podem melhorar serviços e reduzir custos, porém tudo depende da escolha entre público, privado, e da regulação entre as duas redes de serviços.

Voltando ao Conselho Interterritorial e ao documento Estratégia de Saúde Digital, este conta com 4 objetivos:

- Capacitar e envolver as pessoas em seus cuidados de saúde e facilitar sua relação com os serviços de saúde.
- Maximizar o valor dos processos para melhorar o desempenho e o rendimento do sistema de saúde pública, apoiando o trabalho dos profissionais e a governança das organizações.
- Adotar políticas de gerenciamento de dados e governança que tornem as informações interoperáveis e de qualidade disponíveis e criem, nesse sentido, um Espaço Nacional de Dados de Saúde para a geração de conhecimento científico e a avaliação dos serviços.
- Adaptar a evolução do SNS às exigências da sociedade atual, aplicando políticas de inovação voltadas para a Medicina 5P (População, Preventiva, Preditiva, Personalizada e Participativa).

Além disso, a Estratégia está estruturada em três linhas principais de ação: o desenvolvimento de serviços digitais de saúde destinados às pessoas, organizações e processos que compõem o sistema de proteção à saúde, a generalização da interoperabilidade das informações de saúde e a promoção da análise de dados relacionados à saúde e ao sistema de saúde¹⁰.

Estudo realizado pela Saúde Digital Brasil - SDB (Associação Brasileira de Empresas de Telemedicina e Saúde Digital), analisando os recentes marcos regulatórios pós-pandemia em vários países do mundo, aponta que:

(...) a regulamentação da Telemedicina no Brasil é bastante peculiar. Enquanto, em países como Portugal e Colômbia, cabe ao Ministério da Saúde regular a telemedicina, por

¹⁰ (<https://elglobal.es/politica/darias-presenta-el-borrador-de-la-estrategia-de-salud-digital-en-el-primer-cisns-presencial-de-la-pandemia/> acesso em 30/06/2021)

aqui, essa responsabilidade está atribuída ao Conselho Federal de Medicina, autarquia sem comparativo em outros países. Mesmo assim, é importante olhar para os outros países e como as outras economias estão lidando com telemedicina e, desta forma, trazer inovações tecnológicas para o Brasil. Entre os apoiadores da primeira consulta a distância estão Alemanha, Espanha, Canadá, Chile, Colômbia, EUA, França, Nova Zelândia e o Reino Unido. (<https://www.fbh.com.br/associacao-brasileira-de-empresas-de-telemedicina-e-saude-digital-realiza-estudo-sobre-regulamentacao-da-telemedicina-ao-redor-do-mundo/>)

As falhas de segurança do SUS e a absoluta não interoperabilidade entre rede privada e pública de saúde tem gerado manchetes¹¹ na mídia, com prejuízos incalculáveis para a sociedade, desde vazamento de dados pessoais, uso indevido dos dados dos pacientes, crimes e corrupção no pagamento de serviços, dentre muitos outros tipos de problemas de cibersegurança.

O ecossistema blockchain pode interagir com (ou oferecer) identidade digital, sistemas de pagamento, seguros e muitas outras verticais fintech para o mercado de saúde em toda a sua complexidade. Os cidadãos são capacitados, podem auto-gerenciar seus dados, colaborar com a pesquisa científica conscientemente e serem recompensados por isso. Profissionais de saúde e hospitais, clínicas, etc. podem ter sua reputação validada no blockchain evitando golpes de graves consequências. Torna-se possível a ubiquidade completa (com acesso a todos os dados que o usuário permite) do SNS, com o usuário recebendo serviço de qualquer local em seu país e até mesmo em outros países que concordam com esse serviço recíproco.

A ruptura avança com o blockchain integrando os orçamentos do Estado à base de dados descentralizada, através das carteiras dos cidadãos, para pagar as despesas com saúde que todos têm por direito. Essa possibilidade gera uma tensão entre os atuais sistemas de gestão de dinheiro público – bancos de dados centralizados, baixa rastreabilidade até o pagamento final, com muitos intermediários e burocracias, possibilidade de desvios, com riscos à segurança, etc. Além disso, como as coisas estão hoje, a opacidade desses pagamentos é total para os cidadãos, porém a blockchain e sua transparência tende a fortalecer o sistema nacional de saúde e a democracia. Pode até mesmo levar à criação de uma

¹¹ Ver matérias com exemplos recentes de 2020 em <https://www.welivesecurity.com/la-es/2020/11/27/brasil-datos-millones-pacientes-covid-19-expuestos-internet>, <https://saludconlupa.com/series/la-segunda-ola/brasil-doce-hospitales-temporales-son-investigados-por-corrupcion>; <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> e https://www.swissinfo.ch/spa/brasil-corrupci%C3%B3n_investigacion-en-brasil-fraudes-en-compra-de-f%C3%A1rmacos-por-el-ministerio-de-salud/46966448

criptomoeda/token estatal para todas as compras e pagamentos de saúde pública, integrando o SUS e o CEIS. Contratos inteligentes podem automatizar pagamentos, recompensas, validações de exames, serviços, tratamentos, etc. Tudo o que é pactuado com a sociedade e no parlamento como direito à saúde deve ser adicionado aos algoritmos, publicados e em código aberto.

Uma outra consequência importante é sobre a forma do arranjo produtivo que, no Brasil, já opera o SUS com 3 níveis federativos e contratando serviços além das unidades públicas de saúde, isto é, com um conjunto de prestadores de serviços privados. Muitos resultados significativos e positivos tem sido alcançados através dos consórcios territoriais de saúde, que agregam formalmente municípios e estados, para pagar por serviços de saúde e compras de suprimentos de forma coletiva e mais eficiente. **O mais elevado gasto do SUS não é a atenção primária e sim os níveis de maior complexidade, e não há dúvida que o sistema como um todo se tornará mais eficiente e baixará os custos com a base de dados em pool e com chave de entrada a partir de cada cidadão - não apenas pela melhoria da prevenção de doenças como pela melhoria do serviço, evitando redundâncias médicas, de exames, de medicamentos e maior precisão diagnóstica.**

Esse complexo arranjo precisa ser interoperável na blockchain do SUS, permitindo uma identidade digital para pacientes e unidades de atendimento, um histórico médico e epidemiológico unificado, receita eletrônica, pagamentos transparentes e imediatos mediante a comprovação dos oráculos, dentre muitas outras vantagens da tecnologia. O mecanismo de consenso, algo muito importante e que necessita aprofundamento especializado, pode ser também em forma de consórcio, com os nós da rede atuando com PoS e a parte pública com algoritmos como o SNOW.

Como está o sistema de informações do SUS? Em 2020 realizou-se um primeiro trabalho¹² de reconhecimento do terreno e os resultados da pesquisa foram preocupantes. Nas conclusões desta pesquisa (Cassiolato, Falcon e Szapiro, 2020) algumas perguntas são colocadas:

Por que não se difundiu imediata e amplamente o prontuário digital ou a receita eletrônica? Por que o Programa de Telessaúde não chegou aos centros de atenção primária

¹² Ver CASSIOLATO, J.; FALCÓN, M.L.; SZAPIRO, M. A dinâmica global de produção e inovação e o papel do território e dos Estados nacionais: desafios para o desenvolvimento do CEIS no Brasil. In: GADELHA, C. A. G. (Coord.). Projeto Desafios para o Sistema Único de Saúde no contexto nacional e global de transformações sociais, econômicas e tecnológicas (CEIS 4.0). Relatório de Pesquisa. Rio de Janeiro: CEE/Fiocruz, 2021.

nem a base de dados foi integrada no DataSus para todos os níveis de atenção e controle de custos?

As respostas para tais questões estão profundamente vinculadas ao modo em que o Brasil e sua população estão se incorporando à economia digital, sem coordenação suficiente nem planejamento da infraestrutura, sem investimentos continuados e suficientes para criar segurança e resiliência nos serviços públicos. A pandemia vai desmascarar a situação real do DATASUS e mostrar sua fragilidade estrutural. Assim sendo, as soluções privadas e por iniciativa própria vão proliferando e dificultando ainda mais a construção da base de dados única e segura da saúde no Brasil. (...) Além do MS e do CFM e CFF, muitas outras organizações estão envolvidas no processo de transformação digital da saúde: a coordenação do programa Telessaúde Brasil Redes, a rede de educação UMA-SUS, a rede de universidades inovadoras em telemedicina – RUTE – que possui 100 núcleos ativos, a Associação Brasileira de Telemedicina e Telessaúde – ABTms – e outras mais. Outras deveriam ser incorporadas já ao processo, que carece de divulgação e debate amplo com a sociedade. (...) O próprio Cartão Nacional de Saúde – conhecido como Cartão SUS – que foi implantado a partir de 2001 pelos municípios brasileiros segundo a NOAS-SUS 01/2001, não alcançou a universalidade necessária para estruturar a base de dados pessoais e sociais da Atenção Básica, e da qual depende todos os demais níveis de atenção e programas. Em 2015 foi lançado o cartão digital.

Num catálogo publicado em sua página na Internet, o DATASUS possui um conjunto de 262 sistemas em diversas linguagens de programação e com diversos níveis de complexidade e capacidade, gerenciando desde programas específicos de saúde (como DST/AIDS) até a gestão de licitações, execução de obras e recursos humanos. A chamada interoperacionalidade desses sistemas, a base de dados em nuvem segura e em território nacional, a acessibilidade aos dados por parte dos usuários e tantos outros objetivos estratégicos dependem de um plano de transformação digital do SUS e de investimentos na arquitetura da rede, no desenvolvimento da plataforma e na capacitação dos profissionais da saúde que irão operar e alimentar a rede.

Em 2017 foi aprovado pelo Comitê Gestor e pelo MS o documento de planejamento “Estratégia e-Saúde para o Brasil”, a partir do qual surgiu, em 2019, o programa Conecte SUS para implementar seus objetivos estratégicos. Em 2020, com a pandemia da COVID-19, ganhou fôlego a implantação do projeto da Rede Nacional de Dados em Saúde (RNDS). Também foram publicados em 2017 o PNIIS – Plano Nacional de Informação e Informática em Saúde – e o Ministério da Saúde publicou em 2019 o PDTIC – Plano Diretor de Tecnologia de Informação e Comunicação – revisado em 2020. O site do MS também convidava para contribui na revisão e atualização do PNIIS até agosto/2020.

Um aplicativo “Meu DigiSus”¹³ nas redes sociais em telefones móveis já está sendo usado para vários serviços de saúde, em ao menos 50% das unidades básicas de saúde que já estão informatizadas e em rede em 3.700 municípios, alcançando cerca de 100 milhões de usuários, segundo notícia do MS. Aliás, um programa importante nesse caminho é o “Informatiza APS”, para apoiar a entrada dos centros de atenção básica na rede do SUS. (FALCÓN, 2020-C; pp 145-147)

O governo brasileiro publicou o Decreto 9.854 de 25/06/2019 que institui o Plano de Nacional de Internet das Coisas e a Câmara de Gestao e acompanhamento do plano. Algumas Câmaras setoriais forma já instituídas, entre elas a da Saúde, mediante Acordo de Cooperacao Técnica entre MCTIC e MS (sem data, mas o ministro era Mandetta). Nenhum documento ou ata de reunião dá prosseguimento aos trabalhos de acordo com a página do MCTIC. No entanto a Câmara de Industria 4.0 está repleta de atividades, atas e tem publicado um Plano de Ação 2019-2022, que foi atualizado em abril/2021. Nada consta no MS além dos lançamentos de Apps, ou seja, não está disponível documentação sobre planejamento de e-saúde, sua infraestrutura tecnológica, construção de interoperabilidade, cybersegurança, armazenamento e uso dos dados dos cidadãos, regulação da telemedicina, garantia de direitos digitais e gestão orçamentária.

Por fim, para comparar a velocidade de transformação digital e amplitude entre o SUS e SAMS/SP, **a pesquisa do Cetic.br/OPS** informa que houveram alguns avanços no SUS, assim como há problemas no setor privado – coisas que acontecem por falta de planejamento e coordenação do processo, onde quem perde é a sociedade, os cidadãos sem garantias de seus direitos digitais e com atendimento precário (mesmo no SAMS/SP) em relação ao que a tecnologia já permite, e o CEIS como um todo, que se posiciona como seguidor/consumidor e não inovador, no mercado mundial. As Figuras 8 e 9, bem como os resultados da pesquisa nos informam que:

a) Em relação à gestão e governança de tecnologia da informação (TI), em 65% dos estabelecimentos públicos o suporte técnico em informática foi realizado por um prestador de serviço contratado pela secretaria de saúde, enquanto 69% dos privados tinham um prestador contratado pelo próprio estabelecimento. Os estabelecimentos com internação e com mais de 50 leitos foram os únicos em que a maior proporção (67%) mantinha uma equipe interna para este serviço.

¹³ Ver portal do aplicativo em <https://conectesus-paciente.saude.gov.br/menu/home> Ministério da Saúde.

b) Quanto à segurança da informação, a ferramenta que apresentou a maior variação positiva em relação à edição anterior foi a biometria para acesso ao sistema eletrônico (de 8% para 16%). Os estabelecimentos com internação (mais de 50 leitos) e os SADT (serviços de atenção ao diagnóstico e terapia) foram os que apresentaram os melhores resultados na adoção de ferramentas de segurança. Nesta edição, foram incluídas duas novas ferramentas: data loss protection/prevention (DLP), presente em 22% dos estabelecimentos de saúde, e o duplo fator de autenticação, instalado em 7% dos estabelecimentos

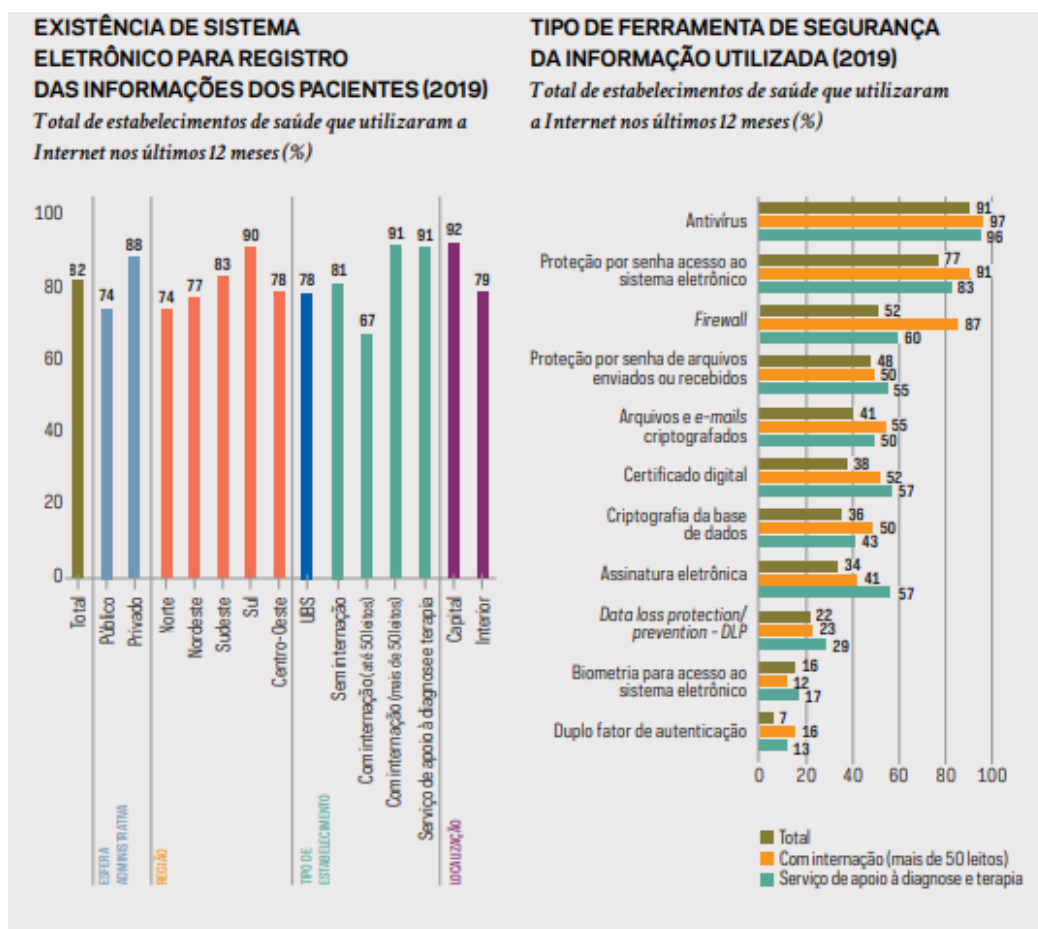
c) Em 2019, verificou-se um aumento na disponibilidade de informações do paciente em formato eletrônico. Entre os principais aumentos em relação à 2018 estão: dados cadastrais dos pacientes (89% contra 79%); principais motivos que levaram o paciente à consulta (64% contra 50%) e admissão, transferência e alta (56% contra 43%). Quanto às funcionalidades do sistema eletrônico, o destaque fica por conta do aumento de sua disponibilidade nos estabelecimentos públicos nos últimos anos, principalmente: listar todos os resultados de exames laboratoriais (de 17%, em 2016, para 41%, em 2019), listar todos os pacientes que fazem uso de uma medicação (de 18%, em 2016, para 40%, em 2019) e realizar prescrição médica (de 29% para 51%). Esses aumentos podem indicar uma evolução no nível e na complexidade dos sistemas eletrônicos adotados

d) Em 2019, os estabelecimentos privados (50%), os com internação e mais de 50 leitos (51%) e os SADT (48%) tinham tanto websites como perfis em redes sociais. No entanto, mais da metade dos estabelecimentos públicos (57%) e cerca de quatro em cada dez estabelecimentos sem internação (39%) e com internação até 50 leitos (44%) não tinham nenhum website nem perfil em rede social. Serviços on-line foram disponibilizados em menor proporção pelos estabelecimentos públicos em relação aos privados. Os SADT foram os que mais ofereceram agendamento de exames (39%) e visualização de resultados de exames (60%) via Internet. Quanto aos serviços de telessaúde, a pesquisa investigou os que estavam autorizados no período pré-pandemia e, como vem acontecendo ao longo da série histórica, são os estabelecimentos públicos que têm maior disponibilidade desses serviços. Os principais serviços oferecidos foram educação a distância em saúde, serviços de teleconsultoria e atividades de pesquisa a distância.

e) Os resultados de 2019 apontam que 91% tinham computador e 82% tinham acesso à Internet, resultado que permaneceu estável em relação a 2018. No entanto, houve uma variação positiva em relação a adoção de sistemas eletrônicos para registro de informações dos pacientes, com aumento de 69%, em 2018, para 78%, em 2019. Estas variações positivas também foram verificadas em relação ao percentual de UBS com dados dos pacientes disponíveis eletronicamente.

f) Nas UBS do sistema público, 23% dos médicos e 14% dos enfermeiros não tinham computador disponível. Entre os médicos com acesso a computador, 54% realizavam a prescrição médica em formato eletrônico e 31% realizavam tanto manual quanto eletronicamente. Apesar disso, 71% assinavam manualmente as prescrições médicas. Entre as ferramentas de telessaúde, a educação a distância foi a mais disponível para os profissionais (mais de 40% para ambos). A pesquisa a distância, teleconsultoria e segunda opinião formativa estavam disponíveis para cerca de um quarto dos profissionais. Quanto à percepção dos profissionais em relação aos impactos do uso das TIC, 83% dos médicos avaliaram que houve redução dos erros na administração de medicamentos e também melhora da qualidade do tratamento como um todo. Entre os enfermeiros, 91% acreditam que houve maior eficiência nos atendimentos e 88% que houve melhora no atendimento como um todo (BRASIL/CETIC.BR, 2021; p.4 e p.6)

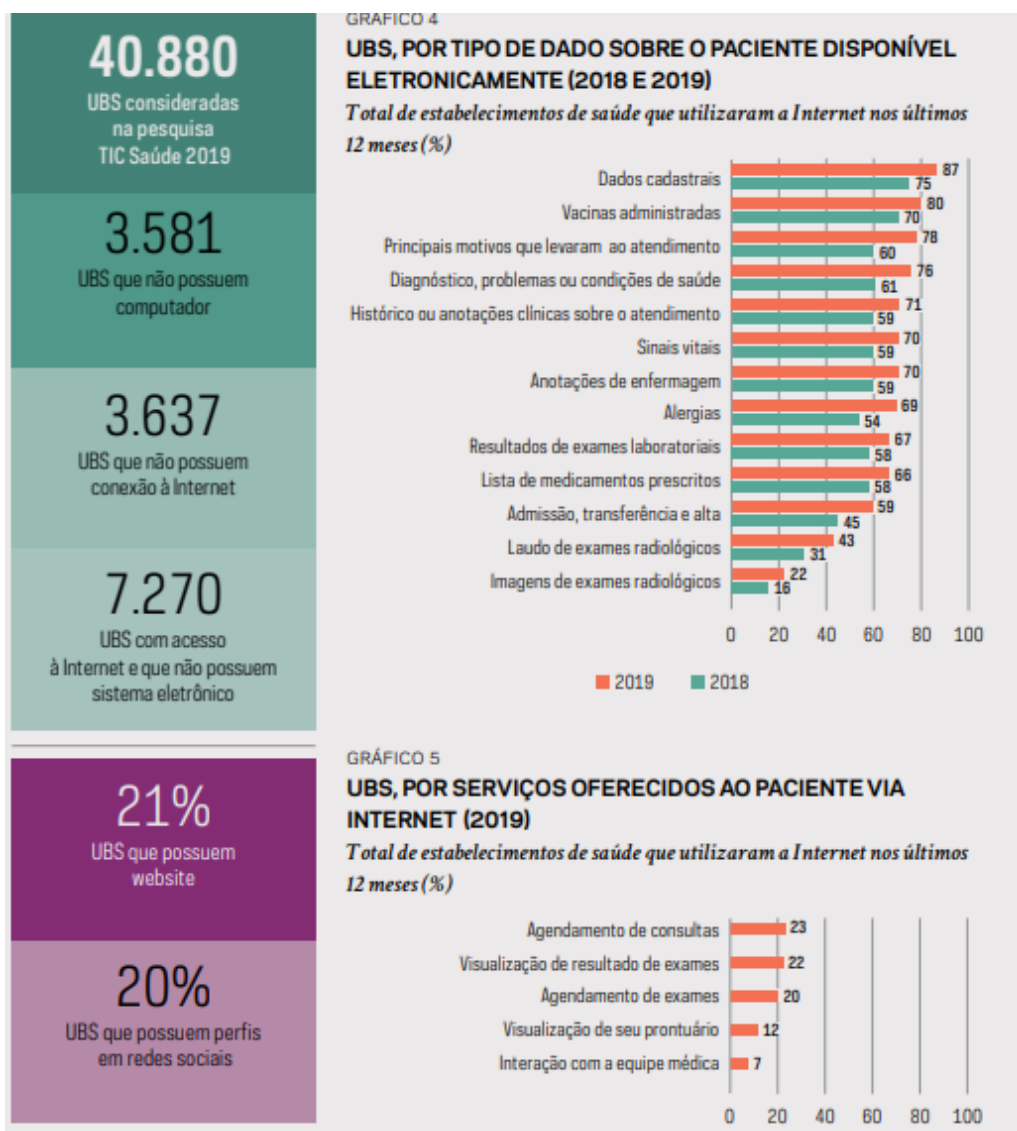
Figura 8 - Sistema nacional de saúde no Brasil e transformação digital, indicadores



Fonte: Brasil/Cetic.br/OPS, 2021, p.5.

Assim, pode-se perceber o tamanho e a complexidade do desafio que o Estado brasileiro e o SUS enfrentarão diante da premente digitalização dos serviços de saúde. Sem dúvida, os atores do setor privado já estão bastante adiantados nessa corrida tecnológica e paradigmática, da qual emergirá o arranjo produtivo e o *funding* para as próximas décadas tanto para o sistema de saúde quanto para o CEIS que lhe é integrado. Sem dúvida, a solução de tecnologia blockchain implica em uma solução consorciada, interoperável, capaz de respeitar os direitos dos cidadãos no espaço digital, mas estressará profundamente o Estado brasileiro e seu sistema orçamentário e de pagamentos. O que pode ser considerado um excelente elemento de inovação social e política.

Figura 9 - Sistema nacional de saúde no Brasil e transformação digital, indicadores das UBS sistema público



Fonte: Brasil/Cetic.br/OPS, 2021, p.7.

4 Conclusões

Diante da profunda transformação que a digitalização causa no regime de acumulação, setores produtivos novos despontam, setores produtivos tradicionais se modernizam e adotam a digitalização, muitos postos de trabalho se extinguem e surgem novas profissões em um mercado de trabalho disruptivo. A maneira de produzir, comprar, conviver e de prestar serviços se altera radicalmente, junto com a percepção da sociedade sobre suas necessidades, o que seja conforto e qualidade de vida. Na verdade, toda a regulação dos mercados – de trabalho, de consumo de massa, de acesso a serviços – e a garantia dos direitos dos cidadãos devem ser também transformadas. Em última instância, a relação Estado-Sociedade-Mercado vem sendo reelaborada com o capitalismo informacional.

Na verdade, e de maneira mais fundamentada, mais do que focar nos instrumentos tecnológicos 4.0, é necessário atualizar os meios e fins do Estado no espaço digital, suas relações com os cidadãos e empresas, pactuar políticas e instrumentos adequados. O Estado nos anos 2020 deve estar à altura das exigências de todos os números e versões das TIC – 4.0, 5.0, etc. – na defesa dos direitos das pessoas e fortalecendo as instituições do pacto democrático, sob pena de construir distopias de ficção científica, comandadas por uma elite de autocratas, “sacerdotes” dos algoritmos e oligopólios em redes informacionais ou plataformas privadas.

Se os anos 1990 foram marcados pelo surgimento de uma Internet acessível ao público, os anos 2000 estabeleceram o reinado das redes sociais e suas plataformas, a década de 2010 viu o surgimento de *softwares* de dados descentralizados criptografados (*blockchain*) resultando, nos anos 2020, na Internet das Coisas e na Internet do Valor – completando uma transformação profunda na maneira de produzir, consumir e acumular riqueza.

Tantas e tão profundas transformações estão gerando legislações inovadoras no sentido de garantir os direitos da cidadania sem impedir a evolução tecnológica. A Carta de Direitos Digitais¹⁴ da Espanha, por exemplo, é um importante guia para a regulação em um espaço digital. Na sua essência, busca atualizar e preservar os direitos constitucionais – civis, políticos, sociais e econômicos – nos espaços digitais onde passamos a trabalhar, conviver, consumir e, literalmente, existir. Está estruturada em 6 Capítulos que tratam de: Direitos de

¹⁴ Trata-se de um guia para orientar projetos, ações e legislações adotadas pelo Governo da Espanha, de acordo com o Plano de Recuperação e Resiliência 2030, com base nas leis já existentes: Lei Orgânica 1/1982 sobre proteção civil do direito à honra, à privacidade pessoal e familiar e à imagem; Lei Orgânica 2/1984, sobre direito à retificação de informações; Lei 34/2002 sobre serviços da sociedade da informação e de comércio eletrônico; Lei 34/2014 das Telecomunicações; Lei 7/2010 sobre Comunicação Audiovisual; Lei Orgânica 3/2018 sobre proteção de dados pessoais; Real Decreto-Lei 28/2020 e Real Decreto-Lei 10/2021 ambos sobre trabalho à distância (teletrabalho).

Liberdade, Direitos de Igualdade, Direitos de Participação e do Espaço Público, Direitos do Entorno Laboral, Direitos em Entornos Específicos e, por fim, de Garantias e Eficácia.

Merece destaque a clara manutenção do princípio de universalidade dos serviços de saúde, a escolha do cidadão pelo serviço presencial ou digital, para isso todos os cidadãos devem ter acesso à Internet, que em si mesmo já compõe outro capítulo de Direitos Digitais enquanto infraestrutura vital para a inclusão social e produtiva das pessoas. Também se enfatiza que, mediante o uso adequado da saúde digital ela prestará importantes serviços de prevenção e personalização ao nível individual, simultaneamente a uma epidemiologia e vigilância sanitária mais eficientes tanto pelo volume de informações em tempo real (*big data*) quanto pela IA identificando padrões e alertas de novos cenários populacionais. O uso da IA não pode prescindir da avaliação criteriosa do profissional de saúde, assim como as informações dos indivíduos e seu histórico médico devem ser armazenados com segurança, em sistemas interoperáveis e com plena portabilidade para o paciente (controle sobre seus dados).

Nenhum hospital ou seguradora pode reter os dados nem os guardar de forma inacessível ao sistema nacional de saúde. Cabe sempre ao paciente/cidadão a palavra final sobre onde guardar ou não os dados, ceder as informações para pesquisa e outros usos, e ser especialmente informado quando um algoritmo (IA) tome decisões sobre sua saúde, podendo aceitar ou não tal decisão. Por fim, os sistemas nacionais de saúde devem assegurar o direito de acesso à telemedicina e teleassistência, como também impedir que empresas de saúde privada condicionem a oferta de equipamentos e interfaces para atendimento à distância à cessão de propriedade das informações.

Em resumo, para assegurar o direito universal à saúde no estágio do capitalismo informacional, é preciso regular o mercado e estabelecer novos pactos entre Estado e Sociedade de tal maneira que fiquem assegurados os direitos constitucionais já existentes e, eventualmente, atualizar as Constituições e Leis para incluir os novos direitos digitais que interferem no espaço real-digital de vida, produção e convivência. A importância da Carta de Direitos Digitais se reveste também de oportunidade, diante da necessidade urgente de formar massa crítica na sociedade para reelaborar as normas e leis no espaço digital – um código de conduta, como formador de hábito e de consciência.

As mudanças importantes da transformação digital na saúde acontecem no âmbito dos costumes, da cultura, das regras do jogo social, enfim, das instituições sociais. Elas exigem novas normas formais para garantir os direitos de todos durante a fase de transformação. Podemos começar com o direito à Identidade Digital, para exemplificar. Para acessar os serviços de saúde digitais, públicos ou privados, é necessário identificar o beneficiário ou

cliente, tendo por base um conjunto de informações que garantem que se trata efetivamente daquela pessoa, da mesma maneira que hoje se utiliza para acessar uma conta bancária. **Ter essa identidade digital protegida** - com seus dados pessoais, histórico médico e todo o imenso conjunto de informações do seu prontuário- atendimentos, diagnósticos, resultados de exames, prescrições, medicamentos etc. – **é um direito digital. Para haver universalidade no sistema nacional de saúde é preciso ter a garantia da identidade digital e da proteção dos dados.**

Para proteger os dados e, ao mesmo tempo, garantir que os serviços possam acontecer com ubiquidade, isto é, em qualquer ponto do território e por prestador público ou privado, a base de dados deve ser dotada de características de criptografia, descentralização e interoperabilidade. Tal base de dados deve permitir minimamente os seguintes produtos: identidade digital, histórico médico, receita eletrônica, monitoramento de indicadores vitais e comportamentais de relevância (como alcoolismo, tabagismo, sedentarismo etc.) e conectar-se com aplicativos em celulares e outros sensores móveis. Por fim, destaca-se a cibersegurança, pois na maioria dos países com Leis específicas de cibersegurança os sistemas de saúde e hospitais são considerados infraestruturas críticas, que devem ser protegidas prioritariamente.

Para implementar a transformação digital das relações Estado-Sociedade-Mercado no campo da saúde é necessário: a) pactuar ao menos dois princípios como expressão de direitos digitais das pessoas – identidade digital e propriedade dos dados; b) construir uma infraestrutura segura para armazenar e processar os dados de maneira descentralizada e, ao mesmo tempo, acessível e interoperável pelos nós da rede de saúde (ubiquidade), sejam eles públicos ou privados; c) garantir o direito de acesso à Internet - como rede vital para receber serviços de saúde em telemedicina e teleassistência, prevenção e personalização dos atendimentos, elevando a esperança de vida com qualidade de vida; d) trabalhar com transparência as parcerias público-privadas no histórico médico, no atendimento à distância, no suprimento de fármacos e outros insumos, nos custos dos serviços e produtos e principalmente no uso da IA para diagnóstico, prescrição, monitoramento e gestão dos serviços de saúde.

Para atingir esses quatro objetivos para uma transformação digital do sistema nacional de saúde que seja inclusiva, universal, segura e com total transparência dos algoritmos, sem submeter os cidadãos e seus dados ao controle de plataformas privadas, a mais moderna tecnologia de dados armazenados descentralizados (DLT – *decentralized ledger technology*) está disponível: é a blockchain. Ao contrário das soluções em nuvem privada (cloud), onde as informações são armazenadas de forma centralizada e sob controle das empresas big tech e suas plataformas, a solução de descentralização das bases de dados criptografados e

organizados em cadeias de blocos impede que um ator ou poucos atores controlem o sistema, alterem informações e incluam critérios de processamento sem o conhecimento e aprovação do conjunto dos nós da rede.

Outra importante função que uma blockchain desempenha é associar “contratos inteligentes” (*smart contracts*) às transações em sua cadeia de blocos, que implica em automaticamente executar determinados comandos preestabelecidos entre os usuários através de um algoritmo que verifica as condições de atendimento. Uma vez dada a permissão (assinatura do “contrato” com sua chave privada (senha), o processo todo se automatiza. É um recurso extremamente útil para infinitas aplicações, como será visto adiante. Os *smart contracts* são majormente aplicados na blockchain Ethereum e outras que compõem seu “ecossistema”.

O modelo atual dos sistemas de saúde trata a informação de maneira opaca aos cidadãos e apresenta uma série de características que já não são aceitáveis na economia digital, resultando em serviços com menor qualidade para a sociedade e para as pessoas. É um sistema disperso, inseguro e com muitas perdas de valor ao longo do fluxo produtivo.

Considerando a estrutura do mercado brasileiro de serviços de saúde dividido entre SUS (sistema público), SAMS (sistema suplementar, privado, de seguros de saúde) e Sistema Privado (desembolso direto), muitas novas empresas estão surgindo no nicho de e-saúde

O Brasil conta atualmente com 747 healhtechs e alguns gigantes do setor de Saúde Complementar e Saúde Privada estão entrando nesse processo de digitalização acelerada. Seus serviços digitais são bem amplos e se apresentam como inovação e solução viável para uma população que hoje é atendida pela SAMS e SPrivada, com atendimento remoto integrado ao prontuário eletrônico, com tecnologia e inteligência de dados perioperatórios buscando eficiência e segurança para anestesias e centros cirúrgicos, soluções e processos para atendimento médico digital, inteligência em compras na saúde para hospitais e clínicas, serviços de telemedicina; Inteligência artificial e consultórios inteligentes, atenção dada à jornada do paciente, tornando-a cada vez mais completa e inclusiva, apoio à operadoras de saúde com soluções inovadoras para telemedicina e autoatendimento, prontuário eletrônico e prescrição eletrônica com gestão de logística integrada, robôs e atendimento à distância, telemedicina para a atenção primária e dezenas de Apps para adolescentes, prevenção, saúde mental, etc

Por um lado, durante a pandemia a maioria das unidades privadas de saúde e seus pacientes adotaram a telemedicina (57%), por outro lado a tecnologia foi utilizada de maneira pouco profissional e insegura: As falhas de segurança do SUS e a absoluta não interoperabilidade entre rede privada e pública de saúde tem gerado manchetes na mídia,

com prejuízos incalculáveis para a sociedade, desde vazamento de dados pessoais, uso indevido dos dados dos pacientes, crimes e corrupção no pagamento de serviços, dentre muitos outros tipos de problemas de cibersegurança.

O ecossistema blockchain pode interagir com (ou oferecer) identidade digital, sistemas de pagamento, seguros e muitas outras verticais fintech para o mercado de saúde em toda a sua complexidade. Os cidadãos são capacitados, podem auto-gerenciar seus dados, colaborar com a pesquisa científica conscientemente e serem recompensados por isso. Profissionais de saúde e hospitais, clínicas, etc. podem ter sua reputação validada no blockchain evitando golpes de graves consequências. Torna-se possível a ubiquidade completa (com acesso a todos os dados que o usuário permite) do SNS, com o usuário recebendo serviço de qualquer local em seu país e até mesmo em outros países que concordam com esse serviço recíproco.

A ruptura avança com o blockchain integrando os orçamentos do Estado à base de dados descentralizada, através das carteiras dos cidadãos, para pagar as despesas com saúde que todos têm por direito. Essa possibilidade gera uma tensão entre os atuais sistemas de gestão de dinheiro público – bancos de dados centralizados, baixa rastreabilidade até o pagamento final, com muitos intermediários e burocracias, possibilidade de desvios, com riscos à segurança, etc. Além disso, tal e como as coisas estão hoje, a opacidade desses pagamentos é total para os cidadãos, porém a blockchain e sua transparência tende a fortalecer o sistema nacional de saúde e a democracia. Pode até mesmo levar à criação de uma criptomoeda/token estatal para todas as compras e pagamentos de saúde pública, integrando o SUS, SAMS e SP, além do CEIS, numa visão mais ampla. Contratos inteligentes podem automatizar pagamentos, recompensas, validações de exames, serviços, tratamentos, etc. Tudo o que é pactuado com a sociedade e no parlamento como direito à saúde deve ser adicionado aos algoritmos, publicados e em código aberto.

Assim, pode-se perceber o tamanho e a complexidade do desafio que o Estado brasileiro e o SUS enfrentarão diante da premente digitalização dos serviços de saúde. Sem dúvida, os atores do setor privado já estão bastante adiantados nessa corrida tecnológica e paradigmática (embora também estejam com sérios problemas de segurança, interoperabilidade e direitos digitais), da qual emergirá o arranjo produtivo e o *funding* para as próximas décadas, tanto para o sistema de saúde quanto para o CEIS que lhe é integrado. Sem dúvida, a solução de tecnologia blockchain implica em uma solução consorciada, interoperável, capaz de respeitar os direitos dos cidadãos no espaço digital, mas estressará profundamente o Estado brasileiro e seu sistema orçamentário e de pagamentos. O que pode ser considerado um excelente elemento de inovação social e política.

5 Referências

- AGBO, C. C. Blockchain in Healthcare Opportunities, Challenges, and Possible Solutions. International Journal of Healthcare Information Systems and Informatics Volume 15, Issue 3, p. 82-97, July-September 2020.
- AGBO, C. C.; MAHMOUD, Q. H.; EKLUND, J. M. An Architecture for Cloud-Assisted Clinical Support System for Patient Monitoring and Disease Detection In Mobile Environments. In Proceedings of the 12th EAI International Conference on Pervasive Computing Technologies for Healthcare - PervasiveHealth '18 New York: ACM Press. doi:10.1145/3240925.3240944. 2018a. p. 245–250.
- AGBO, C. C.; MAHMOUD, Q. H.; EKLUND, J. M. A Scalable Patient Monitoring System Using Apache Storm. In Proceedings of the 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE) IEEE. doi:10.1109/CCECE.2018.8447696, p.1–6, 2018b.
- ANDRÈS, M. B. ¿Para qué sirve la Carta de Derechos Digitales de España? El País, 02/09/2021.
https://cincodias.elpais.com/cincodias/2021/09/01/legal/1630495751_128686.html
- BOULOS, M. N. K.; WILSON, J. T.; CLAUSON, K. A. Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. International Journal of Health Geographics, 17(1), 25. doi:10.1186/s12942-018-0144-x PMID:29973196. 2018.
- BRASIL/CETIC.BR/OPS. Resumo Executivo. Pesquisa TIC Saúde 2019. Brasília, 2021. Acesso em https://www.conasems.org.br/wp-content/uploads/2021/03/Resumo_executivo_TIC_Saude_2019-1.pdf
- DELOITTE. La aceleración de la digitalización en salud. Cinco predicciones sobre el sector salud para 2025. 2021, acesso em <https://www2.deloitte.com/es/es/pages/operations/articles/digitalizacion-sector-salud.html>
- ESPANHA. Carta de Derechos Digitales. Madrid, 2021. Acesso em https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf
- ESPANHA/ICEX. Sanidad em Brasil. 2021. Acesso em <https://www.icex.es/icex/es/navegacion-principal/todos-nuestros-servicios/informacion-de-mercados/sectores/servicios/documentos/DOC2021882782.html>

- FALCON, M. L. de O. As medidas adotadas pelos países diante da crise sanitária-econômica de 2020 e suas consequências. Nota Técnica 2. Rio: RedeSist/IE/UFRJ/Fiocruz, out 2020.
- FALCON, M. L. de O. Capitalismo Informacional, Transformação Digital da Economia e Políticas para o SUS: tendências pós-pandemia da COVID-19. Nota Técnica 1. Rio: RedeSist/IE/UFRJ/ Fiocruz, set 2020.
- FUNK, E.; RIDDELL, J.; ANKEL, F.; CABRERA, D. Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education. *Academic Medicine*, 1. doi:10.1097/ACM.0000000000002326 PMID:29901658. 2018.
- GERHARDT, H. Blockchains: building blocks of a post-capitalist future? 2020. Acesso em <https://longreads.tni.org/blockchains-post-capitalist-future>
- HASSELGREN, A. et al. Blockchain in healthcare and health sciences—A scoping review. *International Journal of Medical Informatics*, 134 104040. 2020.
- MAKRIDAKIS, S.; CHRISTODOULOU, K. Blockchain: Current Challenges and Future Prospects/Applications. *Future Internet*, 11, 258; doi:10.3390/fi11120258. 2019.
- MCKINSEY. Telehealth: a quarter trillion-dollar post Covid-19 reality. Relatório de Pesquisa. 2021 Acesso em <https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality>
- METTLER, M. Blockchain Technology in Healthcare The Revolution Starts Here. In *Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)* IEEE. doi:10.1109/HealthCom.2016.7749510agbo . 2016. p. 520–522.
- NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. <https://bitcoin.org/bitcoin.pdf>
- OECD. Health Statistics, 2019. Acesso em www.oecd.org/els/health-systems/health-data.htm
- OECD. Políticas de Banda Ancha para América Latina y el Caribe: Un Manual para la Economía Digital. 2020. Acesso em <https://www.oecd.org/digital/broadband/lac-digital-toolkit/es/toolkit-text-chapter11es.htm>
- OPS. De la evolución de los sistemas de información para la salud a la transformación digital del sector de la salud. Informe de la conferencia sobre IS4H. 2021. Acesso em <https://iris.paho.org/handle/10665.2/53801>

RADANOVIĆ, I.; LIKIĆ, R. Opportunities for Use of Blockchain Technology in Medicine. *Applied Health Economics and Health Policy*, 16(5), doi:10.1007/s40258-018-0412-8 PMID:30022440. 2018. p. 583–590.

ROMAN-BELMONTE, J. M.; DE LA CORTE-RODRIGUEZ, H.; RODRIGUEZ-MERCHAN, E. C. C.; LA CORTE-RODRIGUEZ, H.; CARLOS RODRIGUEZ-MERCHAN, E. How blockchain technology can change medicine. *Postgraduate Medicine*, 130(4), doi:10.1080/00325481.2018.1472996 PMID:29727247. 2018. p. 420–427.

SHAE, Z.; TSAI, J. Transform Blockchain into Distributed Parallel Computing Architecture for Precision Medicine. In *Proceedings of the IEEE 38th International Conference on Distributed Computing Systems IEEE*. doi:10.1109/ICDCS.2018.00129. 2018. p. 1290–1299.



cee