



# Direito à Saúde e Proteção de Dados Pessoais: desafios e potencialidades contemporâneas





# **Direito à Saúde e Proteção de Dados Pessoais:**

## desafios e potencialidades contemporâneas

## EXPEDIENTE

---

### ELABORAÇÃO

**Idec - Instituto Brasileiro de Defesa do Consumidor**

### INSTITUCIONAL

**Carlota Aquino Costa** - Diretora Executiva

**Igor Rodrigues Britto** - Diretor de Relações Institucionais

**Georgia Carapetkov** - Gerente de Programas e Projetos

### ORGANIZAÇÃO

**Ana Navarrete** - Coordenadora do Programa de Saúde

**Camila Leite Contri** - Advogada do Programa de Telecomunicações e Direitos Digitais

**Matheus Zuliane Falcão** - Analista do Programa de Saúde

**Marina Paullelli** - Advogada

**Marina Fernandes de Siqueira** - Estagiária do Programa de Telecomunicações e Direitos Digitais

### REDAÇÃO E TRADUÇÃO

**Ludmilla Duarte** - Jornalista

### REVISÃO DE COMUNICAÇÃO

**Fernando Gentil** - Analista de Comunicação

### JORNALISTA RESPONSÁVEL

**Daniel Torres** - Coordenador de Comunicação - [imprensa@idec.org.br](mailto:imprensa@idec.org.br)

Agosto de 2022

Somos uma organização da sociedade civil sem fins lucrativos que atua para proteger e ampliar os direitos dos/as consumidores/as, de forma independente de governos, partidos políticos e empresas. Nossa trabalho é mantido com recursos de projetos de fundações filantrópicas e por doações de pessoas físicas que acreditam na importância do que fazemos. Desde 1987 representamos consumidores/as de todo o país na luta por relações de consumo mais justas, especialmente nas áreas de telecomunicações e direitos digitais, serviços financeiros, saúde, alimentação adequada e saudável, mobilidade, energia e consumo sustentável.

Esta obra teve apoio e financiamento da Open Society Institute,  
em cooperação com a Open Society Foundations

Supported by a grant from the Foundation Open Society Institute  
in cooperation with the Open Society Foundations

# SUMÁRIO



<b>PREFÁCIO</b>	<b>4</b>
<b>ACESSO A MEDICAMENTOS, INDÚSTRIA FARMACÊUTICA E PROTEÇÃO DE DADOS PESSOAIS</b>	<b>6</b>
INTRODUÇÃO: 1º DIA DE EVENTO	7
PROTEGENDO OS DADOS DE SAÚDE COMO UM BEM PÚBLICO GLOBAL: CONSIDERAÇÕES CRUCIAIS PARA A EQUIDADE (Artigo Anita Gurumurthy e Nandini Chami)	10
INDÚSTRIA FARMACÊUTICA E PROTEÇÃO DE DADOS PESSOAIS: A EXPERIÊNCIA BRASILEIRA (Entrevista Joyce Souza)	13
<b>SERVIÇOS DE SAÚDE E PROTEÇÃO DE DADOS PESSOAIS</b>	<b>19</b>
INTRODUÇÃO: 2º DIA DE EVENTO	20
PERSPECTIVA SUL COREANA DE DIGITALIZAÇÃO NOS SISTEMAS DE SAÚDE	
Uso secundário de dados públicos de saúde na Coreia: pesquisa comercial e interesse público (Artigo Junho Jung)	22
“O desafio é usar a propriedade pública para gerar bem público” (Entrevista Junho Jung)	26
PERSPECTIVA BRASILEIRA DE DIGITALIZAÇÃO NOS SISTEMAS DE SAÚDE	
Direito à saúde, transformação digital e proteção de dados (Artigo de Héider Aurélio Pinto, José Santos Souza Santana e Arthur Chioro)	32
O acesso e o uso de dados na saúde têm que respeitar os princípios de equidade e privacidade (Entrevista Héider Pinto)	41
Open Health na Saúde Suplementar: regulação pró ou anti competitiva? Reflexões sobre o mercado brasileiro (Artigo Flávia Harumi Ramos Tanaka; Tainá Leandro; Fabrícia Goltara Vasconcellos Faedrich; Paulo Roberto Vanderlei Rebello Filho)	44
<b>INTELIGÊNCIA ARTIFICIAL E SAÚDE</b>	<b>54</b>
INTRODUÇÃO: 3º DIA DE EVENTO	55
DIREITO À SAÚDE E PROTEÇÃO DE DADOS PESSOAIS: DESAFIOS E POTENCIALIDADES (Artigo de Nicoletta Dentico)	57
A IA VAI REVOLUCIONAR A SOCIEDADE E A MEDICINA (Entrevista Daniel Dourado)	59
EXPERIÊNCIA LATINO-AMERICANA: NECESSIDADE DE MECANISMOS DE PARTICIPAÇÃO E MONITORAMENTO	
Implantar Tecnologias Sem Debate Público Foi Naturalizado Na América Latina (Entrevista Jamila Venturini)	64
<b>ENCERRAMENTO</b>	<b>70</b>

# PREFÁCIO



**O** Instituto Brasileiro de Defesa do Consumidor atua desde 1987 na luta pelos direitos de todos os brasileiros e brasileiras em diferentes temas e programas. Nesses 35 anos, a sociedade brasileira passou por várias mudanças em diferentes setores, inclusive no de tecnologia e saúde.

Ao seguir os caminhos e mudanças trazidas pela adoção de tecnologias, o Idec passou a atuar junto a projetos que envolvem a análise, fiscalização e reivindicação de políticas que envolvem a área de proteção de dados pessoais, com atenção especial ao tratamento de dados de saúde.

Vários dos casos que aconteceram no país em todos esses anos tiveram o Idec como protagonista na luta pelos direitos dos consumidores, inclusive perante o Ministério da Saúde (MS), a Agência Nacional de Vigilância Sanitária (Anvisa) e a Agência Nacional de Saúde Suplementar (ANS). Esse é o principal dever do Instituto: lutar pelo direito das pessoas.

Um desses casos foi o de **perfilização de planos de saúde**, ou seja, uma espécie de pontuação para cada um dos usuários dos planos, de acordo com a probabilidade de risco que eles tinham de ter problemas de saúde e eventualmente utilizar os serviços do plano. O Idec atuou fortemente contra as empresas e associações patronais que tentaram incluir esse tipo de sistema no sistema de saúde suplementar do Brasil.

Desde 2019, o Idec notificou as empresas, entidades e até o Conselho Federal de Medicina (CFM) com o intuito de impedir esse absurdo que infrigia não apenas o Código de Defesa do Consumidor (CDC) como também a própria Lei Geral de Proteção de Dados (LGPD) que havia sido recém aprovada.

Ainda sobre o mesmo tema, em 2020 o Idec notificou empresa que tentava fazer **venda de dados de saúde** dos usuários em um *marketplace* (plataforma digital). O que também ia de encontro às regras do CFM e da LGPD.

O Instituto teve atuação direta nos casos de **vazamentos de dados** dos usuários que ocorreram na Anvisa e no Ministério da Saúde. Foram vários, mesmo após a aprovação da LGPD, mas dois merecem destaque: o vazamento de dados da Anvisa de pacientes autorizados a usarem Canabidiol e o vazamento de dados do MS, em 2020. Ambos, embora bastante diferentes, foram relevantes devido à publicização de dados

médicos, considerados dados pessoais sensíveis e perigosos de serem expostos.

No caso da Anvisa, que ocorreu em fevereiro de 2020, o Idec cobrou a elaboração de um plano de ação por parte da agência reguladora. Já nos casos que envolvem os vazamentos do Ministério da Saúde, o Instituto acionou o Ministério Público Federal para investigar a situação. No documento, o Idec destacou o potencial prejuízo aos afetados e a necessidade de investimentos do setor público na proteção dos consumidores e na adequação à LGPD, que já havia entrado em vigor. O caso segue em análise do MPF e foi objeto de uma importante audiência pública.

Outra atuação importante do Instituto foi sobre o **tratamento de dados pessoais em farmácias**. Muito comum no Brasil. É só ir comprar um medicamento que o atendente pede o seu CPF.

Em junho de 2021, um episódio exacerbou as preocupações com a prática: uma imposição de fornecimento de impressão digital em farmácias. A preocupação foi suscitada por relatos de clientes de drogarias. As impressões digitais são dados biométricos (biológicos) que, como os dados de saúde, possuem exigências ainda maiores para seu tratamento, caracterizando-se como dados pessoais sensíveis.

O Idec enviou uma notificação extrajudicial à empresa, contendo pedido de esclarecimentos e enfatizando que o tratamento de dados deve ser norteado pela transparência, legalidade e segurança dos titulares de dados. Um pedido de informações também foi enviado à Abrafarma (Associação Brasileira de Redes de Farmácias e Drogarias). Em seguida, a rede de farmácias deixou de pedir biometria para a concessão de descontos em sua rede.

Esses são apenas alguns dos casos que mostram o quanto a proteção de dados pessoais na saúde é importante para os brasileiros e brasileiras e é uma das grandes lutas do Idec.

Por isso, o Instituto possui uma frente de atuação própria para a interface de temas de Dados e Saúde. Esse esforço culminou com a consolidação dos aprendizados por meio desta publicação, feita a partir de um longo e complexo processo de trabalho, junto ao bem sucedido evento de “Direito à Saúde e Proteção de Dados Pessoais: desafios e potencialidades contemporâneas” realizado entre os dias 17 e 19 de maio de 2022, que teve também a participação do South Centre e do ICICT.

O texto a seguir mostra um bom resumo do que foi esse trabalho em conjunto com a sociedade civil, autoridades e os principais pesquisadores e pesquisadoras da área de saúde e proteção de dados pessoais.



A proteção de dados pessoais na saúde é importante para os brasileiros e brasileiras e é uma das grandes lutas do Idec.





# 1 ACESSO A MEDICAMENTOS, INDÚSTRIA FARMACÊUTICA E PROTEÇÃO DE DADOS PESSOAIS

CLIQUE E ASSISTA  
O PAINEL



# INTRODUÇÃO: 1º DIA DE EVENTO



**A** fragilidade causada pela falta de regulação permite acesso a dados pessoais sensíveis de saúde em ambientes digitais. Este foi o foco das contribuições de especialistas durante a primeira rodada de debates, que foram unânimes em concordar que a administração de medicamentos por profissionais de saúde não pode levar à apropriação indevida dos dados dos pacientes pelo comércio de farmácias, planos de saúde e outras fontes secundárias ou terciárias.

A pandemia da Covid-19 acelerou o fenômeno de “plataformização” da sociedade - nas palavras da pesquisadora indiana Anita Gurumurthy, co-fundadora da ONG [IT for Change](#) -, ou de “dataficação” das economias capitalistas, como cunhou a jornalista e cientista social Joyce Souza, pesquisadora da Universidade Federal do ABC. Ou seja, há um aumento exagerado no uso de plataformas de uso de dados em diferentes áreas da sociedade e, apesar disso gerar facilidades, também traz diversas preocupações.

Na abertura, a gerente de programas e projetos do Idec, Georgia Carapetkov falou sobre a importância desse tipo de evento. “As tecnologias incorporadas à rotina das pessoas trazem como consequência negativa usos econômicos potencialmente perigosos que advêm da apropriação privada de dados pessoais. É vital que os países alinhem seu funcionamento informatizado à plena realização do direito à saúde dos cidadãos e ao cumprimento dos deveres constitucionais do Estado, e que as sociedades reflitam para onde querem caminhar”, enfatizou.

Isso porque dados pessoais têm valor de mercado, concordaram as três painelistas. Cada uma delas abordou os riscos de sua apropriação sob diferentes perspectivas.

A pesquisadora Angela Acosta, da Universidade de Cali (Colômbia), usou como exemplo o aplicativo australiano para celulares que se propõe a monitorar a saúde mental (níveis de ansiedade e estresse) de seus usuários. O app é da empresa privada de telecomunicações Telstra, que oferece velocidade 5G e reúne o maior número de clientes daquele país. “Como essas informações estão sendo manejadas e mantidas em segurança? A preocupação quanto à ética é um debate que ocorre agora na Austrália. Temos novos ambientes de um lado, escassez de regulação e vigi-



Há um aumento exagerado no uso de plataformas de uso de dados em diferentes áreas da sociedade

lância do outro", afirmou a pesquisadora, que é doutora em Ciências Farmacêuticas e Farmacoepidemiologia.

No Brasil, a [LGPD](#), construída à semelhança da lei europeia ([GDPR](#)), trouxe balizas importantes para o tratamento de dados pessoais e a garantia de direitos dos titulares de dados, mas ainda há muitas fragilidades, apontou a jornalista e pesquisadora Joyce Souza, da Universidade Federal do ABC Paulista. Um deles é o setor varejista farmacêutico. "A coleta dos dados biométricos do cidadão ou cidadã no momento da compra de um medicamento, por exemplo, é assunto muito pouco discutido dentro da Agência Nacional de Saúde", frisou.

Outro grave problema envolvendo proteção de dados e saúde foi objeto de trabalho acadêmico da jornalista. Em uma pesquisa de campo feita em drogarias de São Caetano (SP), Souza constatou que, em troca de altos descontos em remédios, as farmácias vinham coletando dados pessoais, clínicos e até financeiros dos clientes (como o valor gasto e a forma de pagamento) e repassando para convênios, seguradoras e planos privados de saúde. "Uma terceira questão envolvendo as farmácias é o fato de que muitas recebem pedidos via aplicativos, plataformas digitais ou [websites](#). São soluções desenvolvidas por empresas terceirizadas e que acabam também tendo acesso aos dados dos pacientes", ressaltou.

De acordo com Anita Gurumurthy, a principal motivação para que os países regulem o acesso, uso e tratamento de dados pessoais vem da necessidade de que o mercado esteja preparado para resolver a tensão entre a cautela necessária no tratamento de dados pessoais sensíveis, como de saúde dos cidadãos, e o enorme valor comercial que possuem.

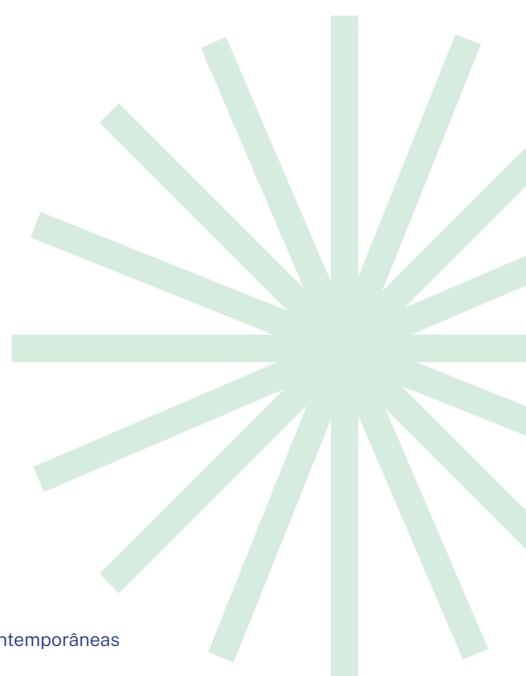
Na China, citou a pesquisadora, lei estabelecida em 2021 combina a proteção de dados com a cibersegurança de modo a afastar a possibilidade de coleta de dados dos chineses por entidades estrangeiras. "No contexto de alguns acordos bilaterais e multilaterais sobre serviços digitais, países em desenvolvimento 'perdem' os dados pessoais de saúde de seus cidadãos, porque não possuem esse tipo de proteção. Regulações diferenciadas são necessárias para os diferentes tipos de dados. Usuários públicos e privados de dados devem estar submetidos a governanças distintas", acredita.

Mediadora do painel e coordenadora do Programa de Desenvolvimento, Inovação e Propriedade Intelectual do [South Centre](#)

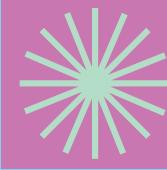


O acesso a medicamentos é um elemento essencial do direito à saúde e sua regulamentação precisa melhorar. Ela também precisa avançar no sentido de gerar melhor e mais ampla assistência de saúde, colaborar com a pesquisa para o desenvolvimento de novos medicamentos e tratamentos, além de reduzir as desigualdades no acesso à saúde

(organização intergovernamental sediada em Genebra, Suíça), Viviana Muñoz destacou: “o que está claro é que os governos precisam criar políticas e regulações, e precisam ser muito cuidadosos com as escolhas que fazem. O acesso a medicamentos é um elemento essencial do direito à saúde e sua regulamentação precisa melhorar. Ela também precisa avançar no sentido de gerar melhor e mais ampla assistência de saúde, colaborar com a pesquisa para o desenvolvimento de novos medicamentos e tratamentos, além de reduzir as desigualdades no acesso à saúde”.



# PROTEGENDO OS DADOS DE SAÚDE COMO UM BEM PÚBLICO GLOBAL: CONSIDERAÇÕES CRUCIAIS PARA A EQUIDADE



**ANITA GURUMURTHY**

Fundadora e diretora-executiva do IT for Change (ITfC).



**NANDINI CHAMI**

Diretora adjunta da IT for Change (ITfC). Mestre em Desenvolvimento Comunitário Urbano e Rural pelo Tata Institute of Social Sciences (Mumbai, Índia).

O imperativo de “proteger dados de saúde para e como um bem público global” por meio de uma abordagem que possa maximizar os benefícios e minimizar os danos foi enfatizado pela OMS durante o enfrentamento da pandemia.

Na era do *big data* e da Inteligência Artificial, a inovação em saúde para benefício público envolve uma multiplicidade de dados – registros clínicos de pacientes, dados de pesquisa clínica, registros de atividades de profissionais de saúde, informações ambientais, dados genômicos sobre humanos e patógenos e, cada vez mais, dados de *wearables* [dispositivos “vestíveis”, como relógios digitais], aplicativos e dispositivos de *IoT* (Internet das coisas).

A abordagem de Bens Públicos Globais (*Global Public Goods*, ou GPG) da OMS fornece um ponto de partida para tornar os dados de saúde acessíveis para mudanças sistêmicas. Mas sua eficácia na inovação pública, na resiliência institucional e na equidade de acesso à saúde depende de um regime global de dados de saúde que possa efetivamente endereçar os riscos de captura do bem público e de perfilização sem limites de pessoas e do planeta. Uma economia de dados desregulada e prosperando com impulsos neocoloniais somente fará com que a universalização da saúde seja um sonho distante.

## CAPTURA PRIVADA DE DADOS PÚBLICOS

Arquiteturas públicas para compartilhamento de dados de saúde no Reino Unido, Dinamarca, Suécia e Índia refletem um alto risco de captura privada de tais conjuntos de dados abertos por empresas multinacionais. Por

serem dependentes de empresas estrangeiras para desenvolver pesquisas baseadas em *big data*, os países em desenvolvimento são ainda mais vulneráveis ao extrativismo de dados.

O caso [GenBank](#) mostra como sequências de genes de países do Sul Global, compartilhadas em repositórios de livre acesso (*open access*) online, são usadas por empresas farmacêuticas do Norte Global para construir linhas de tratamento patenteadas, sob regras de direito internacional [incapazes](#) de garantir a repartição justa e equitativa dos benefícios com as comunidades de origem.

O cenário gritante de fluxo de dados unidirecionais do Sul para os cofres da *Big Tech/Big Pharma* do Norte levanta questões críticas sobre o poder geoeconômico na “economia da inteligência” e o consequente esvaziamento do conhecimento e das capacidades de dados institucionais do Sul.



Uma economia de dados desregulada e prosperando com impulsos neocoloniais somente fará com que a universalização da saúde seja um sonho distante.

## EROSÃO DA AUTONOMIA SOCIAL

Na era dos fluxos de dados de saúde transnacionais onipresentes, as [abordagens tradicionais](#) em privacidade das informações de saúde – atreladas à sensibilidade das categorias de dados com patamares mínimos de informação e consentimento – não antecipam os riscos desconhecidos de reutilização e tratamento de dados. Algumas tipologias de dados consideradas menos sensíveis [podem não ter](#) grandes garantias de privacidade. No entanto, dados aparentemente inócuos – como os de *wearables* – podem ser facilmente recombinados e analisados para perfilização e direcionamentos antiéticos/ilegais.

Leis como a GDPR tentam proteger os direitos individuais à privacidade dos cidadãos europeus. Entretanto, direitos de indivíduos e grupos (por exemplo, [mulheres mens-truadas, povos indígenas](#)), particularmente em países em desenvolvimento que não possuem tais leis, correm um grande risco de abuso, já que esses dados viajam para fora do alcance de suas jurisdições.

## UMA ABORDAGEM GPG PARA OS DADOS DE SAÚDE CENTRADA NA EQUIDADE

---

A era da Inteligência Artificial anuncia um momento que exige amplos debates globais e locais sobre as inúmeras questões éticas intrínsecas à coleta e uso de dados de saúde. Marcos regulatórios globais são necessários para proteger os *commons* de dados de saúde de serem implantados para satisfazer a ganância neoliberal e a engenharia social e para promover o valor social e público dos dados de saúde com vistas à equidade global.

Uma abordagem GPG dos dados de saúde não conseguirá endereçar essas considerações, a menos que esteja fundamentada em um regime de governança de dados transversal que inclua conjuntos de dados pessoais e não pessoais, incluindo aqueles não gerados originalmente no contexto de ambientes clínicos de saúde.

As negociações em curso na OMS para alterar o Regulamento Sanitário Internacional (“RSI”, de 2005) [apresentam uma oportunidade](#) para lançar as bases para tal regime com foco na equidade global em saúde. O RSI pode obrigar os países a compartilhar dados de saúde de suas bases nacionais para respostas coordenadas em nível global, com medidas proporcionais de compartilhamento de benefícios para que comunidades e países do Sul não sejam ludibriados.

A OMS deve assumir a liderança para estimular uma nova estrutura multilateral vinculante, visando uma regulação de dados pessoais de saúde que seja integrada e baseada em direitos humanos. Essa estrutura legal deve abranger direitos individuais e coletivos, garantir a autonomia do sistema de saúde para todos os países e articular as normas de interesse público para inovações, construídas a partir de infraestruturas de dados comuns.

No nível nacional, os governos – como guardiões dos conjuntos de dados de saúde – devem criar novas estruturas jurídico-institucionais que incentivem uma abordagem de gestão da infraestrutura de dados de saúde por meio de parcerias público-comunitárias que respeitem a soberania individual e coletiva dos dados, e se comprometam com a saúde e o bem-estar de todos, sem deixar ninguém para trás.



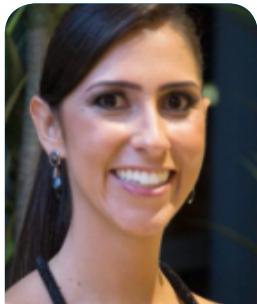
# INDÚSTRIA FARMACÊUTICA E PROTEÇÃO DE DADOS PESSOAIS:



## A EXPERIÊNCIA BRASILEIRA

***“Proteger os dados pessoais da população brasileira perpassa a questão de classe”***

*Pesquisadora alerta para os riscos que a “dataficação” do capitalismo traz para o acirramento das desigualdades dentro das sociedades e entre os países*



**JOYCE SOUZA**

Doutoranda e Mestre em Ciências Humanas e Sociais pela Universidade Federal do ABC. Pesquisadora do Laboratório de Tecnologias Livres da Universidade Federal do ABC (LabLivre/UFABC). Membro do Movimento das Tecnologias Não Alinhadas (NATM).

**U**m novo viés da exploração capitalista, o “colonialismo de dados” traz a perspectiva de que há uma tentativa sistemática do capitalismo de tornar todas as experiências humanas alvo de extração lucrativa. “Nesse contexto, quem está conectado está de alguma forma sendo colonizado pelos dados gerados, rastreados e processados”, aponta a jornalista, cientista social e doutoranda na Universidade Federal do ABC Paulista, Joyce Souza.

Painelista do evento *Direito à Saúde e proteção de dados pessoais: desafios e potencialidades contemporâneas*, do [Idec](#), Joyce Souza abordou a proteção dos dados pessoais de Saúde no Brasil a partir dos achados de seu trabalho de mestrado *A saúde dos dados pessoais e o município de São Caetano do Sul* e do seu artigo [\*Os riscos das tecnologias digitais: do campo ao garfo\*](#), produzido como parte de uma pesquisa da Fundação Heinrich Böll Brasil.

Para ela, para estruturar um sistema de proteção dos dados pessoais do cidadão brasileiro contra a ganância dos empresários da saúde deve-se ter em mente a questão de classe. “Em um país como o Brasil, em que o salário mínimo está em torno de R\$ 1.200,00 e a cesta básica atingiu o valor do salário mínimo, não é uma opção entregar ou não os dados pessoais em troca de descontos em farmácias”, exemplifica a cientista social.

Joyce Souza também é pesquisadora do Laboratório de Tecnologias Livres ([LabLivre](#)), coprodutora do podcast [Tecnopolítica](#), integrante do Movimento das Tecnologias Não-Alinhadas e organizadora do livro *Sociedade de Controle: Manipulação e Modulação nas Redes Digitais*.

## CONFIRA A ENTREVISTA CONCEDIDA POR ELA AO IDEC.

---

**Idec:** Para sua tese de mestrado, você desenvolveu uma reveladora pesquisa de campo sobre como as farmácias de São Caetano do Sul, no ABC Paulista, manejam os dados pessoais dos consumidores. Quais foram os achados mais preocupantes, em sua opinião, resultantes de seu estudo?

**Joyce Souza:** A minha pesquisa de mestrado foi sobre a compra e venda de dados pessoais no setor da saúde pública e privada no município. Organizando um organograma desse setor, a partir da pesquisa de campo, que foi composta por entrevistas, observei que as farmácias ocupavam um espaço importante no contexto, em especial as grandes redes. Dentre os principais elementos observados, destaco que as farmácias, por meio de programas de descontos e parcerias com seguradoras e operadoras de planos de saúde e também empresas - via benefícios como o vale-farmácia destinado aos funcionários -, se tornaram grandes coletoras de dados pessoais. Os dados coletados, naquela ocasião, eram repassados aos parceiros por meio de planilhas com informações pessoais do consumidor: o que ele havia adquirido na ida à farmácia, qual havia sido o desconto aplicado e a forma de pagamento. Há algumas questões importantes a serem avaliadas nessa prática. Entre elas, a questão da transparência e da privacidade em relação ao modelo de negócios adotado, visto que o consumidor não era alertado sobre como seus dados estavam sendo coletados, armazenados e compartilhados com parceiros. Outra questão é a segurança em relação aos dados - por exemplo, onde e como são armazenados, quem seriam os atores com acesso a eles, quais sistemas de segurança da informação são aplicados para que não haja vazamentos dos dados, entre outras questões que são fundamentais quando analisamos esse contexto.

**Idec:** Sua pesquisa foi feita antes da promulgação da Lei Geral de Proteção de Dados. Você acha que a lei trouxe proteção adicional contra essa prática?

**Joyce Souza:** A minha pesquisa foi realizada de fevereiro de 2016 a janeiro de 2018, ou seja, antes da promulgação da LGPD. Boa parte da pesquisa ocorreu no momento em que o debate sobre o Brasil ter uma Lei Geral de Proteção de Dados era incipiente. Os olhares no Brasil estavam voltados a compreender a preocupação da Europa com a privacidade de seus cidadãos e como o continente estava avançando em um regulamento para o tema. O Brasil analisava este cenário a partir do viés econômico, buscando possíveis adequações, caso necessário, para manter boas relações com os países da União Europeia. Apesar da preocupação com a privacidade e a proteção dos dados pessoais e sensíveis não ser a tônica, nesses anos da minha pesquisa, em especial em 2016 e início de 2017, é sempre importante destacar que o setor da saúde, independente da LGPD, já tem normas bastante específicas no que tange

aos cuidados com dados e informações de pacientes. Um exemplo é o Código de Ética Médica -em vigor desde 11 de janeiro de 1965 e com diversas atualizações nas últimas décadas - que determina a confidencialidade de informações médicas relacionadas ao paciente. Esse é só um dos exemplos que podemos encontrar em relação à preocupação dos dados na área da saúde. Porém a LGPD trouxe entraves para além de atuações específicas, como no exemplo da relação médico-paciente. O fato de a lei trazer definições específicas e deveres no que tange a dados pessoais, dados pessoais sensíveis, responsabilizações no âmbito de controladores e operadores de dados, consentimento de usuários enquanto uma das bases legais para a utilização de seus dados, entre diversos outros, ela tem feito com que empresas, inclusive as farmácias, busquem adequações em relação à lei. Que elas tenham, portanto, que dar transparência ao que tem sido realizado no âmbito da coleta, armazenamento e processamento de dados dos consumidores. Esse processo ainda tem caminhado lentamente e tenho visto que o consentimento é um tema complexo nesse contexto, mas já é um passo importante para compreendermos o que tem ocorrido no âmbito da privacidade e proteção de dados e o que pode ser feito para que garantias, como o princípio da não-discriminação, sejam realmente aplicadas.

**Idec:** *No aspecto do uso de dados de saúde de cidadãos pelas farmácias para fins comerciais, inclusive em associação explícita ou velada com seguradoras de saúde, você acredita que ainda há fragilidades na legislação e/ou em sua implementação pelo Poder Público? Quais são essas fragilidades?*

**Joyce Souza:** Acredito que seja fundamental conhecer toda a cadeia que envolve coleta, guarda e tratamento de dados nesse setor. Ao conhecer essa cadeia, será possível verificar todos os atores que têm acesso às informações, como são feitos esses acessos, quais garantias de segurança existem, por qual razão determinados acessos ou trocas de informações e dados ocorrem, entre outras questões fundamentais para então analisarmos as fragilidades da legislação. A Autoridade Nacional de Proteção de Dados (ANPD) tem se apresentado pouco em situações complexas envolvendo, por exemplo, vazamento de dados pessoais e dados pessoais sensíveis no setor da saúde. Recentemente ocorreu um mega vazamento de dados por uma grande rede de laboratórios privados de análises clínicas e não houve pronunciamento sobre o caso pela ANPD. Também não me recordo de ter visto nenhum parecer da Autoridade no que tange à coleta de biometrias que estava ocorrendo em uma grande rede de farmácias. O posicionamento oficial da ANPD é fundamental para o avanço da LGPD no país e, consequentemente, no setor da saúde.



A Autoridade Nacional de Proteção de Dados (ANPD) tem se apresentado pouco em situações complexas envolvendo, por exemplo, vazamento de dados pessoais e dados pessoais sensíveis no setor da saúde.

**Idec:** Quando olhamos para o comportamento do consumidor, quais são os erros em que, de um modo geral, ele incorre na sua relação com o mercado de farmácias e que colocam sua privacidade em risco?

**Joyce Souza:** Não acredito em erros dos consumidores nas suas relações com as farmácias. Em um país como o Brasil, em que o salário mínimo está em torno de R\$ 1.200,00 e a cesta básica atingiu em junho deste ano o valor do salário mínimo, não é uma opção entregar ou não seus dados pessoais em troca de descontos em farmácias. No Brasil, pensar a privacidade e a quem ela é garantida perpassa pensar a questão de classe. Por isso, é fundamental que órgãos e instituições que atuam em favor dos direitos dos cidadãos estejam atentos ao que tem ocorrido e questionem com veemência o mercado que se constitui em torno dos dados e dos descontos nas farmácias.

**Idec:** Durante sua participação no evento do Idec você falou sobre o novo fenômeno de “dataficação das economias capitalistas”. Pode explicar, em linhas gerais, o que é esse fenômeno?

**Joyce Souza:** Na última década, com o avanço da capacidade de processamento computacional e a consolidação de modelos de negócios baseados em tecnologias digitais, como a das plataformas capazes de coletar dados de usuários a partir de suas interações em redes sociais, ampliou-se a crença de que os dados são elementos fundamentais para a compreensão da sociedade e do comportamento social. Desta forma, se antes os metadados eram considerados subprodutos, sem valor, agora são considerados recursos valiosos por empresas e governos, pois a partir deles é possível extrair informações preciosas para criação de novos produtos, serviços e monitoramento social. A dataficação tem crescido, se tornado um paradigma aceito nas sociedades e também visto como uma forma importante de governabilidade neoliberal. O neoliberalismo, que é composto por um conjunto de discursos, práticas e dispositivos, tem se utilizado desse processo para reforçar grandes assimetrias e desigualdades, seja entre países desenvolvidos e periféricos, seja entre sociedades e suas classes sociais.

**Idec:** Seu trabalho Os riscos das tecnologias digitais: do campo ao garfo chama atenção para diversos riscos embutidos no primeiro edital do programa Agro 4.0, do Governo Federal, que visa investir R\$4,8 milhões em 14 projetos pilotos de adoção e de difusão de tecnologia 4.0 no agronegócio. Quais são os principais riscos e que interseção isso tem com a saúde?



A dataficação tem crescido, se tornado um paradigma aceito nas sociedades e também visto como uma forma importante de governabilidade neoliberal.

**Joyce Souza:** A tônica do Governo Federal no que tange à implementação de tecnologias digitais no Brasil está no investimento em startups como solução para o desenvolvimento tecnológico do país. A primazia das startups segue as orientações das consultorias e das organizações internacionais que muito influenciaram os formuladores de editais e documentos oficiais do Governo Federal. Não é só na questão do agro que esta realidade está presente, ela figura também em documentos como na Estratégia Brasileira de Inteligência Artificial ([EBIA](#)), na Estratégia de Transformação Digital ([E-Digital](#)) e no [Saúde Digital](#). Dados de diferentes setores podem ser correlacionados e apresentarem resultados entre si. A intersecção que o contexto do Agro 4.0 pode ter com o setor da saúde é a conexão que a coleta, o processamento e a classificação de dados de um setor podem trazer ao outro. Por exemplo, dados atrelados ao consumo de agrotóxico por determinadas populações, se analisados por meio de algoritmos preditivos, podem apresentar resultantes na classificação de riscos de doenças. Além disso, vale destacar que big techs (grandes empresas de tecnologia digital), como Amazon e Microsoft, apresentam soluções tanto para o agronegócio quanto para a saúde. Também apresentam soluções para a guarda de dados em nuvem, que tem sido bastante utilizada pelas startups que atuam tanto em um setor quanto em outro. Não desenvolvi um mapeamento sobre toda essa cadeia para afirmar com precisão as correlações entre os setores, mas acredito que se desenharmos bem o organograma de toda a cadeia de empresas de tecnologias digitais atuantes do “campo ao garfo”, em hospitais e indústrias farmacêuticas, provavelmente notaremos gargalos importantes sobre a coleta, o processamento e a utilização de dados sendo feitos em setores diferentes, mas por meio das mesmas empresas para a ampliação de seus lucros.

**Idec:** Você afirma que o jargão amplamente midiatizado “o Agro é tech, o Agro é pop, o Agro é tudo” traz incutida a ideia de que as tecnologias digitais são a única e melhor alternativa para que o agronegócio cresça e mantenha sua vantagem competitiva em escala global. Quais riscos, em sua opinião, isso traz para a população no que se refere à privacidade de dados pessoais?

**Joyce Souza:** Há uma ideologia - e até de certa forma também uma ilusão - no que tange às tecnologias digitais. Atualmente, elas são vistas com um potencial muito além de suas reais capacidades. São colocadas como as grandes salvadoras dos problemas das sociedades, sejam eles políticos, econômicos ou sociais. Em alguns casos, mais extremos, são apresentadas como capazes de superar o próprio ser humano que a criou e, desta forma, resolver os grandes problemas que permeiam as sociedades. Sustentados também pela crença do “dataísmo”,



Há uma ideologia - e até de certa forma também uma ilusão - no que tange às tecnologias digitais.

Atualmente, elas são vistas com um potencial muito além de suas reais capacidades.

os processos de dataficação têm se normalizado e se popularizado rapidamente, e auxiliado na consolidação e na ampliação de formas de vigilância, controle e monitoramento social. A dataficação também tem sido utilizada para modulação comportamental, aplicada a partir do processamento de dados do cidadão, que permite uma análise mais minuciosa de suas características. Isso é usado na criação de estratégias de *microtargeting*, novos produtos e serviços, acelerando, assim, o processo de circulação da mercadoria.

**Idec:** Você afirma também que o colonialismo de dados implica em novas formas de exploração e apropriação que resultam em dinâmicas de discriminação e de desigualdade. Pode desenvolver essa afirmação?

**Joyce Souza:** A ideia do colonialismo de dados, como é apresentada por Nick Couldry e Ulises Mejias no livro *The costs of connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (2019) traz a perspectiva de que há uma tentativa sistemática do capitalismo em tornar todas as experiências humanas alvo de extração lucrativa. Neste contexto, quem está conectado de alguma forma está sendo colonizado pelos dados gerados, rastreados e processados. Apesar dos autores não apontarem a elevação da desigualdade que esse processo engendra, o que vejo é que há profundas assimetrias existentes entre as nações desenvolvidas e as nações periféricas. Por exemplo, dados coletados em território brasileiro estão sendo utilizados para extração de lucro e geração de valor às empresas oriundas dos países desenvolvidos, como é o caso da Amazon, Google, Microsoft, Apple, entre outras, localizadas nos Estados Unidos. Também ocorrem desigualdades entre os grupos econômicos dominantes e os grupos sociais marginalizados, na maioria das vezes, sem seus direitos básicos, incluindo a proteção de dados e a privacidade, como foi o caso do exemplo que dei sobre a “escolha” entre a privacidade e a disponibilização de dados pessoais em troca de descontos em medicamentos nas farmácias.





## 2 SERVIÇOS DE SAÚDE E PROTEÇÃO DE DADOS PESSOAIS

CLIQUE E ASSISTA  
O PAINEL



# INTRODUÇÃO: 2º DIA DE EVENTO



A proteção de dados pessoais deve levar em conta as especificidades do tratamento de dados no campo da saúde. Em especial, uma preocupação é o uso comercial das informações. Esta foi a pauta que moveu os debates dos participantes do painel durante o segundo dia do evento.

A pesquisadora-líder de um projeto de ação participativa sobre saúde digital e direitos humanos que envolve múltiplos países, Sara Margaret Davis, do [Graduate Institute](#) (baseado na Suíça), focou sua abordagem na proteção de dados pessoais de saúde de grupos vulneráveis da sociedade, como jovens, mulheres, comunidades em situação de exclusão digital ou que não possuem proficiência para usar as ferramentas virtuais.

Um estudo qualitativo feito entre jovens de Bangladesh, Colômbia, Gana, Quênia e Vietnã, e divulgado pela pesquisadora durante o evento, trouxe alguns resultados tão curiosos quanto surpreendentes.

Grande parte dos jovens entrevistados, por exemplo, apesar de ter confessado vício e mesmo dependência de seus celulares, também externou preocupação com a necessidade de privacidade e de anonimato *online*. Além disso, admitem precisar de treinamento sobre segurança de dados e direitos digitais e expressam desejo de que seus dados clínicos pessoais sejam anonimizados pelas autoridades públicas de saúde. “Eles também demonstraram estar conscientes sobre os riscos da má informação, dos diagnósticos virtuais incorretos, das imagens compartilhadas sem consentimento, da exposição, do *bullying* cibernético, do assédio sexual ou moral pela internet”, descreveu Margaret Davis.

Já na Coreia do Sul, cerca de 65% da população concorda que seus dados pessoais de saúde devam ser tratados somente por agências do Poder Público e 58,2% discordam de qualquer uso comercial dos dados por empresas privadas, de acordo com o estudo divulgado no evento pelo segundo painelista, o pesquisador Junho Jung, da Universidade de Seul.

Feita junto a 1.370 participantes entre 19 e 64 anos, a pesquisa revelou que os sul-coreanos, de um modo geral, rejeitam a apropriação de seus dados pessoais de saúde para fins comerciais. “Aqueles que passaram por uma experiência de hospitalização tendem a concordar em maior número com o uso de dados públicos. As pessoas mostram estar interessadas em um melhor e mais facilitado acesso aos seus

próprios dados de saúde, mas desconfiam dos mecanismos de proteção e de eventual mal uso desses dados. E há um entendimento geral de que deve haver necessariamente interesse público envolvido no tratamento das informações”, apontou Jung.

Mediado pela advogada do programa de Telecomunicações e Direitos Digitais do Idec, Camila Leite, o painel contou ainda com as exposições do médico sanitário Héider Pinto - pesquisador em Saúde Coletiva, Política Pública e Transformação Digital em Saúde nas universidades federais da Bahia (UFBA) e do Recôncavo Baiano (UFRB) -, e de Tainá Leandro, assessora da [ANS](#) (Agência Nacional de Saúde Suplementar).

Héider Pinto, que esteve à frente da criação do [e-SUS](#) no Brasil, destacou a importância da interoperabilidade dos prontuários de saúde dos pacientes na rede pública. Ou seja, a importância de um sistema uniformizado e interconectado em que médicos de hospitais e clínicas podem garantir a assistência de cada paciente, usando a mesma base de dados catalogados sobre cada um, de modo a garantir a continuidade e a eficiência do cuidado e evitar a demanda por exames desnecessários.

Outro avanço na área da saúde digital com ganhos para os usuários do SUS, segundo o médico sanitário, é o [Telessaúde Brasil Redes](#), criado em 2004, sobretudo por sua capacidade de oferecer atenção primária a moradores de localidades afastadas sem a presença de determinadas especialidades de atendimento clínico. “A Covid-19 tornou inevitável a expansão desse tipo de serviço virtual”, observou. Ressaltou, no entanto, que a aceleração do uso de ferramentas digitais na saúde pela pandemia trouxe junto a necessidade de se regular e monitorar a forma de tratamento dos dados pessoais, “porque eles podem ser usados também para a construção de novos modelos de negócios”.

No âmbito das operadoras de planos privados de saúde, Tainá Leandro destacou a recente iniciativa da ANS de disponibilizar dados pessoais anonimizados e agregados que estão em sua base. “Isso torna possível conhecer o mercado sem identificar os beneficiários dos serviços de saúde”, explicou a assessora, acrescentando que um dos avanços trazidos pela LGPD nesta seara foi a de vedar as operadoras de plano privado de saúde o acesso prévio aos dados pessoais dos clientes.



# PERSPECTIVA SUL COREANA DE DIGITALIZAÇÃO NOS SISTEMAS DE SAÚDE



## *Uso secundário de dados públicos de saúde na Coreia: pesquisa comercial e interesse público*



**JUNHO JUNG**

Pesquisador do Center for Health and Social Change (Coreia do Sul).

**O** advento da medicina de alta precisão, do *big data*<sup>[1]</sup> e da inteligência artificial na medicina fez aumentar a demanda por dados de saúde individuais e coletivos. Entidades públicas e privadas estão ativamente engajadas na acumulação e utilização de dados de saúde. O governo coreano selecionou a biomedicina, especialmente os dados de saúde, como uma das três áreas que irão impulsionar o crescimento econômico futuro do país. Uma pesquisa revelou que o governo alocou 66 milhões de dólares em seu orçamento para ações de coleta e uso dos dados de saúde pública em 2021. O orçamento nacional total alocado para o sistema de saúde em 2021 foi de 250 milhões de dólares.

Junto com o orçamento, houve uma grande mudança na estrutura legal para o uso de dados de saúde pública desde agosto de 2020. A alteração na lei de proteção da privacidade permitiu que, para fins de compilação de estatísticas e pesquisa científica, os dados *pseudonimizados*<sup>[2]</sup> possam ser usados sem o consentimento do titular. Essa mudança na estrutura legal está de acordo com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR). No considerando 53, a GDPR dispensa o consentimento individual para tratamento de dados pseudonimizados para “fins de arquivamento de interesse público, fins de pesquisa científica ou histórica, ou fins estatísticos”. Esta dispensa de consentimento individual rapidamente atraiu muitas empresas privadas interessadas em acessar os dados de saúde pública.

Um requerimento notável para acessar os dados de saúde pública veio de operadoras de saúde. Elas alegaram que a atual estrutura de taxas é derivada de dados desatualizados ou de fontes estrangeiras, criando um ônus injusto para seus clientes. Seu principal argumento é que, uma vez liberado o acesso gratuito aos dados de saúde pública coletados pelo governo, os seguros privados podem aumentar a cobertura com preços razoáveis e baseados em dados.

Em julho de 2021, seis seguradoras de saúde privadas ganharam direito de acesso ao Health Insurance Review & Assessment Service (HIRA) <sup>[3]</sup>. Agora, elas têm acesso a amostras de dados *pseudonimizados* do HIRA, incluindo informações sobre diagnóstico, código CID-10, instituição médica, data e duração de admissão hospitalar, prescrições, despesas, etc.

Existem duas grandes organizações na Coreia que coletam a maioria dos dados de saúde pública. Uma é o National Health Insurance Services (NHIS); a outra é um braço do NHIS chamado HIRA.

O sistema de saúde da Coreia é baseado no seguro de saúde nacional, que cobre 60% das despesas médicas de todo cidadão. Além disso, o seguro nacional é obrigatório para empresas e pessoas; portanto, todos os dados relacionados à saúde são colecionados no NHIS. O que também atrai as seguradoras privadas é que os dados de saúde pública do NHIS incluem a situação financeira das famílias, pois o seguro nacional de saúde é cobrado levando-se em consideração a renda.

Há uma preocupação, tanto da comunidade médica quanto da sociedade civil, de que um mais amplo acesso aos dados de saúde pública pelas companhias de seguro privadas na verdade terá o resultado oposto ao que foi prometido: com base na situação médica e financeira dos coreanos, os produtos de seguros privados serão mais estratificados, com taxas mais altas, e eliminarão os grupos de alto risco de serem segurados. Também há preocupação para com o uso secundário inadequado dos dados *pseudonimizados* adquiridos por seguradoras, que frequentemente são subsidiárias de conglomerados financeiros.

Com isso em mente, a decisão final do Conselho de Monitoramento de Segurança de Dados no NHIS sobre acesso a dados foi diretamente oposta à do HIRA. O regulamento interno do NHIS afirma que os dados de saúde pública de sua base só podem ser fornecidos “se a pesquisa for de interesse público”. Após uma análise cuidadosa da proposta de pesquisa das seguradoras privadas, o Conselho concluiu que elas foram direcionadas para o interesse comercial e não para o interesse público, além de também violarem o princípio do uso mínimo. As empresas rapidamente se opuseram à decisão, pois a atual “Diretriz de Utilização de Dados de Saúde” do Ministério da Saúde coreano não separa a pesquisa comercial da pesquisa científica.



O que também atrai as seguradoras privadas é que os dados de saúde pública do NHIS incluem a situação financeira das famílias, pois o seguro nacional de saúde é cobrado levando-se em consideração a renda.

A atual estrutura legal para uso secundário de dados pseudonimizados de saúde pública não define claramente o que constitui pesquisa “científica”, deixando uma área cinzenta para interpretação. No caso da GDPR, a pesquisa científica dispensa consentimento, porque ela a ciência serviria ao interesse público. Assim, os relatórios do European Data Protection Supervisor (EDPB) separam a pesquisa comercial da científica. O princípio da GDPR é que o livre fluxo de dados deve ser protegido, enquanto a pesquisa comercial impede esse princípio por meio de segredos comerciais. Além disso, a sensibilidade e a vulnerabilidade dos dados de saúde são bem observadas na GDPR, que determina a tomada de cuidados e provisões especiais antes do tratamento de dados.

Durante anos, as seguradoras privadas tiveram acesso a dados de saúde pública anonimizados amostrados, em redes fechadas, tanto no NHIS quanto no HIRA. Agora elas têm acesso a amostras de dados pseudonimizados pelo HIRA, incluindo dados de diagnóstico, código CID-10, instituição médica, data e duração da internação, prescrições, despesas. Todos os dados são fornecidos em uma rede fechada; apenas os dados tratados podem ser exportados, e todos os identificadores pessoais são removidos. Desta maneira, o risco de vazamento de dados é relativamente baixo.

No entanto, o que as entidades privadas fazem com os dados finais tratados não pode ser controlado. A HIRA diz que exige um consentimento dos pesquisadores, no sentido que os dados não serão usados para fins comerciais e serão descartados após um mês. Entretanto, não há, na prática, nenhum mecanismo de monitoramento ativo para rastrear esse compromisso, nem há como sancioná-los em caso de uso indevido. Por isso é necessária a construção de um mecanismo para salvaguardar o interesse público inerente ao uso de dados de saúde pública.

Há vozes mistas na sociedade. A sociedade civil expressou a preocupação sobre este ser um grande passo para a comercialização de dados pessoais de saúde. Alguns grupos de consumidores saudaram a decisão da HIRA argumentando que o fornecimento de dados pessoais para as companhias de seguros privadas pode diversificar as opções de produtos de seguro com taxas reduzidas. Enquanto isso, a Associação de Médicos se opôs fortemente, pois o acesso ao conjunto de dados de saúde pública era exclusivo dos profissionais de saúde, mas eles foram largamente deixados de fora durante os debates. E o governo está pressionando por um mais amplo uso de dados de saúde pública pseudonimizados, esperando que isso dinamize a economia. Essas interações complexas entre as partes interessadas dificultam chegarmos a um equilíbrio entre garantir o interesse público e proteger a privacidade.



É necessária a construção de um mecanismo para salvaguardar o interesse público inerente ao uso de dados de saúde pública.

O uso adequado de dados de saúde pública pode gerar interesse público. No entanto, para garantir o bem público deve haver regras e regulamentos bastante claros. Os dados de saúde pública têm, de fato, algumas características de bem público, pois podem melhorar a saúde coletivamente. Ao mesmo tempo, os dados de saúde individuais são uma das informações pessoais mais sensíveis. Para uso secundário de dados de saúde pública, os agentes de tratamento de dados devem fornecer evidências convincentes de que suas pesquisas podem criar um bem público maior que o risco evidente. Além disso, conforme previsto nos princípios do GDPR, os resultados extraídos do uso de dados públicos devem ser abertos ao público de modo a assegurar o interesse público.



[1] Conjunto de tecnologias criadas para armazenar, analisar e gerenciar volumes massivos de dados digitalizados.

[2] A pseudonimização é uma técnica que substitui informações contidas num conjunto de dados que identifica um indivíduo por um identificador artificial, um pseudônimo.

[3] Agência governamental coreana da área de Saúde.

## **“O desafio é usar a propriedade pública para gerar bem público”**

*Líder do projeto que está fazendo uma análise crítica da digitalização da Saúde no país da Ásia Oriental, Junho Jung fala sobre a percepção da sociedade e as lacunas no marco regulatório*



**JUNHO JUNG**

Pesquisador do Center for Health and Social Change (Coreia do Sul).

**N**a Coreia do Sul, uma alta porcentagem da população (72,5%) têm consciência de que corporações privadas acessam e tratam seus dados pessoais; ao mesmo tempo, somente 39,2% estão de acordo com seu uso comercial e 65,3% desejam que o país adote penalidades mais altas para quem usá-los indevidamente ou sem consentimento.

Esses são alguns dos resultados da pesquisa feita pelo *Center for Health and Social Change*, uma organização sem fins lucrativos especializada em estudos transdisciplinares de saúde.

Ocorre que a legislação coreana destinada a proteger os dados pessoais de saúde da população ainda está longe de refletir esse anseio, indica o biólogo e médico-pesquisador Junho

Jung, da Jeonbuk National University of Korea e um dos líderes da pesquisa. Sem diferenciar pesquisa científica de comercial ou estabelecer mecanismos de monitoramentos ativos sobre os entes privados que acessam os dados pessoais de saúde dos cidadãos, o sistema regulatório da Coreia possui lacunas e áreas cinzentas. “A maior preocupação deve ser a de como gerar bem público com propriedade pública, ao invés de beneficiar certas entidades privadas”, afirma Jung, que foi um dos palestrantes do evento *Direito à Saúde e proteção de dados pessoais: desafios e potencialidades contemporâneas* e concedeu a seguinte entrevista ao Idec, em complemento ao seu artigo.



**“A maior preocupação deve ser a de como gerar bem público com propriedade pública, ao invés de beneficiar certas entidades privadas”**

**Idec:** O Center for Health and Social Change da Coreia do Sul, onde o senhor é pesquisador, conduziu uma interessante pesquisa de percepção da população sul-coreana sobre uso secundário dos dados pessoais de saúde. Os resultados da pesquisa chegaram a surpreendê-lo?

**Junho Jung:** O resultado geral da pesquisa foi conforme esperado, com desaprovação generalizada do uso comercial dos dados públicos de saúde, baixa confiança na proteção de dados e suporte ao uso de dados para tópicos de interesse público. O que nos surpreendeu foi a discrepância sobre a aprovação do uso dos dados por diferentes entidades. Não esperávamos que as pessoas estivessem mais favoráveis ao uso de dados por empresas de TI do que pelas seguradoras de saúde, pois as empresas de TI são conhecidas por serem mais propensas à violação de dados, ao uso indevido e são menos reguladas.

**Idec:** Esse resultado foi linear em todas as faixas etárias?

**Junho Jung:** A influência da idade foi outro achado interessante. Esperávamos que os idosos fossem mais relutantes ao uso secundário do uso de dados públicos. No entanto, foi o grupo etário masculino dos 20-30 anos que apresentou forte oposição e desconfiança na utilização de dados pessoais por parte de quaisquer entidades. Talvez essas faixas etárias sejam mais ativas no uso de dados *online*, portanto têm maior conhecimento de ocorrências que envolvem seu uso indevido, o que leva a um maior grau de desconfiança.

**Idec:** Na Coréia do Sul, uma taxa relativamente alta da população revelou conhecer a lei da privacidade (61,4%) e estar ciente do uso de seus dados pessoais pela indústria (72,5%). A que você atribui esse nível alto de conscientização?

**Junho Jung:** Desde 2019, a lei Data 3 (uma alteração da Lei de Privacidade) foi muito debatida no Parlamento e teve uma cobertura de mídia relativamente ampla. Isso pode explicar a conscientização sobre as mudanças na lei de privacidade. Além disso, recentemente o projeto *MyData* do setor financeiro, iniciado pelo governo, permitiu que as pessoas administrassem todos os seus dados financeiros (saldo, transações, etc) de qualquer aplicativo de banco, independentemente do banco do qual a pessoa é cliente. Convencionalmente, você precisava instalar os aplicativos de cada banco para verificar o saldo ou fazer a transferência. Essas mudanças radicais podem alertar as pessoas.

**Idec:** E quanto ao alto grau de conhecimento geral sobre uso de dados pela indústria?

**Junho Jung:** Em relação ao uso dos dados pela indústria, acho que há dois fatores. Primeiro: casos de vazamento de dados pessoais. Em 2012, 2014 e 2016, a KT (maior empresa sul-coreana de telecomunicações) foi atacada e foram vazados respec-

tivamente 8 milhões, 14 milhões e 30 milhões de dados pessoais. Existem muitos outros casos de vazamentos de dados na Coreia. O povo coreano diz sarcasticamente que nosso número de previdência social é de propriedade pública, pois foi vazado por inúmeras empresas em várias ocasiões. Segundo: provavelmente a Covid-19 e o rastreamento de contatos (*contact tracing*). Durante a pandemia, o governo sul-coreano implementou check-in eletrônico para locais públicos (restaurantes, shoppings, museus, teatros). Esse sistema QR foi amplamente terceirizado para empresas privadas de TI, como a Naver e a Kakao. Durante a fase inicial da vacinação, as pessoas também fizeram reservas através dessa plataforma SNS privada. Isso permitiu que todos percebessem o quanto de dados essas empresas realmente acumulam e utilizam.

**Idec:** *A pesquisa revelou que somente 39,2% concordam com o uso comercial dos dados pessoais de saúde; menos da metade (41,5%) concordam que eles sejam usados por seguradoras para o desenvolvimento de novos produtos; cerca de metade (53,3%) concordam com o uso em TI para saúde digital, proporções maiores de pessoas concordam com uso pela indústria farmacêutica (61%) e pelo Poder Público (65,6%). Em sua opinião, o enquadramento legal atual do país acompanha esse sentimento da população?*

**Junho Jung:** No momento, a lei de dados na Coreia afirma que “quando as informações pessoais são necessárias para a compilação de estatísticas, ou para fins de pesquisa científica, as informações pessoais são fornecidas de uma forma pela qual um indivíduo específico não possa ser identificado.” (Artigo 18º 2.4, [Lei de Proteção de Informações Pessoais](#)). O que permite efetivamente o uso secundário de dados pseudonimizados sem consentimento individual em pesquisas científicas. Essa mudança na regulamentação está alinhada com a Lei Geral de Proteção de Dados da União Europeia (GDPR, [Artigo 89](#)), que libera o processamento de dados do consentimento individual se for para “fins de armazenamento por interesse público, fins de pesquisa científica ou histórica ou fins estatísticos”. No entanto, a GDPR explica que pesquisa científica é aquela voltada para o bem público, e é diferente da pesquisa comercial.

**Idec:** *Então essa diferenciação não existe na legislação coreana?*

**Junho Jung:** Não. Esse entendimento não foi refletido na regulamentação coreana e a diretriz de processamento de dados de saúde publicada pelo Ministério da Saúde da Coreia explica que “pesquisa científica” pode ser considerada como qualquer pesquisa que adote “metodologia científica”, permitindo que a



É seguro dizer que a estrutura legal atual na Coreia tem muitas áreas cinzentas, deixando um número de lacunas para interpretações variadas e desalinhadas com a percepção do público.

pesquisa comercial também possa ser considerada como pesquisa científica. Essa interpretação oficial do Ministério sobre a lei foi suficiente para incentivar as seguradoras privadas a solicitarem o uso de dados de saúde pública para “pesquisa científica” comercial. Portanto, é seguro dizer que a estrutura legal atual na Coreia tem muitas áreas cinzentas, deixando um número de lacunas para interpretações variadas e desalinhadas com a percepção do público.

**Idec:** Quando se trata de “quanto podemos usar”, 64,2% concordam com uso por agências públicas apenas e 42% disseram não concordar com uso comercial em situação alguma. Além disso, cerca de metade (50,8%) têm impressão negativa sobre uso dos dados pessoais por seguradoras privadas. Quais pontos da legislação atual da Coreia do Sul teriam que ser ajustados para refletir o desejo da população por privacidade?

**Junho Jung:** Como mencionei anteriormente, a estrutura legal atual tem uma grande área cinzenta, deixando a decisão final para as instituições individuais. Existem duas grandes organizações na Coreia que coletam a maioria dos dados de saúde pública. Uma é o National Health Insurance Services (NHIS), outra é o braço do NHIS chamado Health Insurance Review & Assessment Service (HIRA). A NHIS supervisiona todos os dados nacionais de saúde e seguro, incluindo finanças (já que o seguro nacional de saúde é cobrado de acordo com seu status de renda). A HIRA lida com dados de solicitação de seguro da instituição médica. Durante o ano de 2021, a HIRA forneceu alguns dos seus dados públicos a seguradoras privadas, uma vez que ela não tinha regulamentação interna que a impedissem de fornecer dados a entidades privadas, o que também é permitido por lei superior (artigo 18 do PIP). Por outro lado, a NHIS possui um regulamento interno determinando que os dados de saúde pública só podem ser fornecidos se a pesquisa proposta visa melhorar o “bem público”. O debate ainda está em andamento e a decisão final sobre se a NHIS fornecerá dados públicos a entidades privadas não foi tomada. Essas confusões surgiram da ambiguidade na legislação que define o alcance e os limites da “pesquisa científica”. Assim, esclarecimentos sobre **quem, como e o quê** constitui pesquisa científica ainda precisam ser claramente disciplinados.

**Idec:** Qual é a margem de liberdade que as seguradoras privadas possuem atualmente no que se refere ao acesso aos dados dos cidadãos?

Junho Jung: Durante anos, as seguradoras privadas tiveram acesso a amostras de dados de saúde pública anonimizados, em rede fechada, tanto na NHIS quanto na HIRA. Agora elas têm acesso a amostras de dados pseudonimizados da HIRA, incluindo dados de diagnóstico, código CID-10, instituição médica, data de admissão e duração da internação, prescrição, despesas, etc. Todos os dados são transacionados em rede fechada e somente os dados processados podem ser exportados, com todos os identificadores pessoais removidos - então presumo que a violação de

dados não seja muito preocupante. No entanto, o que as entidades privadas fazem com os dados finais processados não pode ser controlado, embora a HIRA tenha dito que obteve o consentimento de pesquisadores informando que os dados não serão usados para fins comerciais e serão descartados após um mês. Mas não encontrei nenhum mecanismo de monitoramento ativo para rastrear tal compromisso, nem há como sancioná-los em caso de uso indevido.

**Idec:** *Os sul-coreanos revelaram querer condições mais rígidas para o uso de dados públicos, como o estabelecimento de penas mais rígidas para eventuais transgredões durante seu tratamento (65,3%), anonimização completa (55%), proibição de uso por terceiros (53,6%) e até mesmo banimento completo do uso comercial (46,8%). O senhor acredita que existe um movimento do governo no sentido de incorporar esse desejo à regulação?*

**Junho Jung:** Como o governo coreano vê os dados como o principal motor econômico para a próxima geração, no nível administrativo não há muito movimento no sentido de proteger e limitar o uso de dados públicos. Em vez disso, o governo está na vanguarda do incentivo ao uso de dados públicos por todas as entidades. Também não há movimento ativo no Parlamento para alterar a legislação atual.

**Idec:** *Em termos de comportamento da população, o senhor acha que os sul-coreanos, apesar da evidente preocupação com a privacidade, habitualmente compartilham os dados pessoais de saúde em aplicativos, websites, plataformas comerciais?*

**Junho Jung:** Em termos de seguradoras privadas [de saúde], devo dizer que sim. O resultado de nossa pesquisa mostrou que pessoas que tiveram experiência recente de internação hospitalar foram mais favoráveis ao uso público de dados de saúde, mesmo por entidades privadas. Embora o tratamento médico seja amplamente coberto pelo seguro nacional na Coreia, ainda há um enorme mercado de seguros privados. O seguro privado cobre custos médicos que não são cobertos pelo seguro nacional, como usos médicos mais experimentais/cosméticos/estilo de vida. No entanto, a forma de cobrança do seguro privado é um pouco mais incômoda do que a nacional. Como as reivindicações de seguro nacional são feitas automaticamente da instituição médica para a HIRA, você não precisa se preocupar com elas (muitas pessoas nem sabem como as cobranças são feitas no regime nacional). No caso do regime privado, você precisa pegar um documento do seu médico, as faturas e o recibo e enviar por fax, ou mandar a fotocópia pelos aplicativos. Assim, há uma demanda do lado do consumidor para



O uso público adequado de dados de saúde pode gerar bem público. No entanto, para garantir o bem público, será preciso haver regras e regulamentos mais claros.



Percepção da população sul-coreana sobre uso de dados por seguros privados de Saúde

**Negativa**  
**50.8%**

**Não tem certeza**  
**26.3%**

**Positiva**  
**22.9%**

**Conhecem a lei sobre proteção de dados:**  
**61,4%**

**Sabem que dados pessoais de saúde são usados por empresas:**  
**72,5%**

**Concordam com o uso de dados pelas seguintes fontes secundárias:**

Agências governamentais:

**65,6%**

Indústria farmacêutica:

**61%**

Empresas de tecnologia em saúde digital:

**53,3%**

Seguradora de saúde (para desenvolver novos produtos):

**41,5%**

Empresas de marketing:

**39,3%**

**Sob quais condições os dados de saúde da população podem ser tratados?**

**65,3%**  
Penalidades mais rígidas

**55%**  
Anonimização completa

**53,6%**  
Uso por fontes terciárias deve ser proibido

**46,8%**  
Banimento completo do uso comercial

Fonte: "A Survey of Public Attitudes on the Secondary Use of Public Health Data in Korea" (2022). Autores: Junho Jung, Seung-Hwa Lee, Jungchan Park, Sungsoo Lim, Hyungjin Kim e Kwangmo Yang.

tornar esse processo mais simples, com armazenamento e transferência mais fácil dos prontuários.

**Idec: O senhor acredita que os resultados da pesquisa poderão influenciar o governo do seu país em termos de mudanças no quadro regulatório?**

**Junho Jung:** Essa é a nossa esperança. Acreditamos que o uso público adequado de dados de saúde pode gerar bem público. No entanto, para garantir o bem público, será preciso haver regras e regulamentos mais claros. Além disso, acho que nosso estudo mostra que há uma grande discrepância na compreensão dos benefícios e riscos do uso público de dados de saúde. A sociedade, de modo geral, está preocupada com vazamentos de dados, porém este risco é relativamente pequeno, pois são processados apenas em rede fechada. A maior preocupação deve ser a de como gerar bem público com propriedade pública ao invés de beneficiar certas entidades privadas. A legislação atual possui ambiguidades que requerem melhor interpretação.



# PERSPECTIVA BRASILEIRA DE DIGITALIZAÇÃO NOS SISTEMAS DE SAÚDE



## *Direito à saúde, transformação digital e proteção de dados<sup>1</sup>*



**HÉIDER AURÉLIO PINTO**

Médico sanitarista, mestre e pós-doutorando em Saúde Coletiva, doutor em Políticas Públicas. Professor da UFBA e UFRB.



**JOSÉ SANTOS SOUZA SANTANA**

Médico sanitarista, mestre e doutorando em saúde coletiva. Secretário Executivo da FESF.



**ARTHUR CHIORO**

Médico sanitarista, doutor em saúde coletiva. Professor da Unifesp.

## **INTRODUÇÃO**

O uso de tecnologias de comunicação e informação (TIC) na promoção de inovações no processo de trabalho em saúde tem sido associado a transformações importantes e positivas nos modos de produzir o cuidado, de desenvolver ações de vigilância em saúde e de gerir os serviços e sistemas de saúde. São mudanças evidenciadas na literatura científica: serviços de saúde com mais informações clínicas sobre os pacientes e maior capacidade de resolver seus problemas de saúde; redução da realização de procedimentos desnecessários (exames, encaminhamentos, etc.); maior compartilhamento de decisões entre profissionais melhorando a coordenação e qualidade do cuidado e otimização da oferta de serviços de saúde, com redução de filas e tempos de espera.

Além disso, o envelhecimento da população, o aumento da carga de doenças crônicas e a escalada dos gastos em saúde têm estimulado ainda mais processos de transformação digital na saúde, tanto no setor público quanto privado, focando quatro aspectos: (i) informatização dos serviços de saúde e processos de trabalho; (ii) integração e troca de informações entre profissionais e serviços; (iii) atendimento remoto; e (iv) uso da inteligência artificial. Ao mesmo tempo que esses processos são recomendados por organismos multilaterais, como a OMS, são objeto de interesses do mercado, como trataremos à frente.

Em função disso, é fundamental que a discussão sobre transformação digital na saúde seja articulada, e não oposta, à de

<sup>1</sup> Texto adaptado para esta publicação de ensaio submetido a periódico científico e nascido no contexto do seminário Direito à Saúde e Proteção de Dados Pessoais.



governança e proteção de dados. Não somos obrigados a escolher entre duas alternativas polares: 1) abrir mão da proteção de dados em nome da transformação digital, por mais cobertura, qualidade, efetividade e eficiência dos serviços de saúde; ou 2) abrir mão de uma necessária transformação digital no sistema de saúde brasileiro em nome da proteção de dados dos cidadãos. O debate sobre inovação, transformação digital e uso de dados deve ser amplo e envolver as políticas de ciência, tecnologia e inovação (CT&I); de saúde e as voltadas ao modelo de desenvolvimento econômico-social que se quer para o Brasil. É vital que se construam políticas e estratégias que combinem proteção e segurança dos dados, melhoria do sistema de saúde e desenvolvimento econômico-social sustentável e includente.

Apresenta-se neste ensaio uma discussão com base em estudos e pesquisas que têm sido desenvolvidos pelos autores no campo de inovação e tecnologias em saúde. Serão analisados quatro focos dos processos de transformação digital, buscando apontar suas justificativas, avanços e promessas, bem como os riscos que podem trazer à privacidade dos dados e usos comerciais inadequados e lesivos às pessoas na condição de cidadãos e de consumidores.

É vital que se construam políticas e estratégias que combinem proteção e segurança dos dados, melhoria do sistema de saúde e desenvolvimento econômico-social sustentável e includente.

## INFORMATIZAÇÃO DO PROCESSO DE TRABALHO E DOS SERVIÇOS DE SAÚDE

O Brasil possui mais de cinquenta sistemas de informação no setor público de saúde, fundamentais para as análises epidemiológicas, estatísticas e para o planejamento das políticas públicas. Esses sistemas registram informações dos pacientes, seus problemas de saúde, procedimentos realizados, mas não substituem o prontuário do paciente e nem organizam a agenda e processo de trabalho dos serviços de saúde. Em outras palavras, reúnem informações sanitárias e administrativas importantes para o sistema de saúde, mas não informatizam o processo de trabalho, tal como ocorre quando se usa prontuários eletrônicos e sistemas de gestão de serviços de saúde.

Há dez anos apenas 10% das equipes de saúde da família, por exemplo, contavam com prontuário eletrônico. Com a criação e implementação do prontuário eletrônico público, eSUS-AB, em 2013, hoje 50% das equipes usam esse sistema e 20% utilizam outros prontuários eletrônicos, mas 100% são obrigadas a alimentar o Sistema de Informação em Saúde da Atenção Básica - SISAB. Dentre as melhorias promovidas por essa implantação destacam-se a melhoria da tomada de decisões clínicas com a

preservação da memória dos atendimentos anteriores, a produção de cuidado mais singular e personalizado e as condições para garantir a continuidade do cuidado e evitar procedimentos desnecessários ou não recomendados com base em evidências científicas.

Mas esse processo não é isento de conflitos e riscos. Por exemplo, a oferta de prontuários públicos gratuitos restringe o mercado privado de prontuários. Por isso, não há interesse dos agentes econômicos que soluções públicas e gratuitas tenham ampla implementação e/ou que sejam desenvolvidas e atualizadas, de modo que fiquem em um patamar similar ou acima das ofertas do setor privado. Além disso, muitas vezes são as empresas privadas que, na prática, fazem a gestão dos dados, com baixa interferência e governança do contratante público, podendo ainda dar ensejo a práticas inadequadas, como a comercialização de dados sem consentimento e conhecimento do órgão público e do cidadão.

## **INTEGRAÇÃO E TROCA DE INFORMAÇÕES ENTRE PROFISSIONAIS E SERVIÇOS**

Há um paradoxo no SUS quando se considera a quantidade de informações existentes sobre cada pessoa e as possibilidades de seu uso clínico para o cuidado dos pacientes. Como não há interoperabilidade entre sistemas, não se consegue, de forma unívoca, associar as informações de uma mesma pessoa contidas em diferentes sistemas. Com isso, os dados clínicos gerados em uma consulta não podem ser acessados para atendimentos posteriores, principalmente quando realizados em outros pontos da rede de atenção à saúde, o que seria essencial a um atendimento mais adequado, efetivo e com menos realização de procedimentos repetidos e desnecessários.

Diversos países vêm investindo na interoperabilidade entre os sistemas de informação usados em seus sistemas nacionais de saúde. A OPAS/OMS aponta esse investimento como central para avançar na qualidade e resolutividade dos sistemas de saúde, recomendando fortemente a criação e disponibilização de Registros Eletrônicos de Saúde (RES) com dados clínicos alimentados e consultados por serviços da rede de atenção. No Brasil, esforços vêm sendo desenvolvidos há mais de 15 anos.

Um marco importante na definição dos padrões de interoperabilidade do SUS foi a Portaria MS nº 2.073, de 2011. De lá pra cá, manteve-se no MS o objetivo de interoperar os dados, chegando em 2022 na Rede Nacional de Dados em Saúde – RNDS.

Contudo, isso vem acontecendo em um ritmo muito lento. Em meio às turbulências

políticas que fragilizaram a ação do MS, trocas constantes de ministros e interposição de interesses na condução desse processo, observa-se em 2022 resultados frágeis, muito aquém do desejado.

Atualmente, a interoperabilidade reduz-se aos dados da Covid-19. Além disto, cenário é preocupante. Ataque hacker promoveu perda de dados do MS, gerando problemas aos usuários que precisavam comprovar a vacinação com o ConecteSUS. Conflitos de interesses entre dirigentes desse processo, que, depois de contratarem empresas como agentes públicos passaram a trabalhar nas mesmas, foram fartamente noticiados. O fato é que ainda não há interoperabilidade entre os sistemas de informação da rede de atenção para apoiar a tomada de decisões clínicas nos serviços de saúde, nem para decisões de gestão relacionadas à análise da saúde populacional e ao planejamento de ações sanitárias de impacto coletivo.

Ante a lentidão e desorganização do âmbito federal, estados e municípios têm investido nessa perspectiva digital, resultando em experiências que buscam permitir interoperabilidade entre dados de alguns sistemas de cuidado, até experiências mais robustas, como a Plataforma Eletrônica da Saúde (iPeS), que visa interoperabilidade ampla, customizável e colaborativa e que envolve governos estaduais, municipais e também uma instituição interfederativa, e o Consórcio Interestadual de Desenvolvimento Sustentável do Nordeste.

## ATENDIMENTO REMOTO

O Brasil vem investindo no Programa Telessaúde Brasil desde 2007, com o objetivo de oferecer educação continuada a profissionais de saúde do SUS e apoiá-los a tomar decisões clínicas com o apoio de especialistas, em serviços tão diversos quanto urgências cardiológicas, ambulâncias do SAMU e unidades de saúde ribeirinhas na Amazônia, por exemplo. A partir do princípio de que a informação e o conhecimento é que devem circular (e não a pessoa), mostrou-se que era possível oferecer um atendimento de qualidade, com redução de gastos em infraestrutura e diminuindo em até 50% o deslocamento de pacientes e profissionais de saúde. Além de otimizar recursos, essas alternativas permitem enfrentar a grande escassez de médicos especialistas, especialmente nas cidades mais distantes de centros urbanos.

Porém, o Programa tinha como um de seus condicionantes uma regulação infralegal muito restritiva em termos de possibilidades de atenção à saúde remota, não presencial. Em grande parte, isso ocorreu por resistência dos conselhos profissionais, que buscavam, sobretudo, reserva de mercado. Tais resistências, no Brasil e em outros países, em termos de teleatendimento, sofreram mudanças durante o enfrentamento

da pandemia da Covid-19, o que abriu espaço para a utilização intensiva de tecnologias de interação à distância em muitos setores. Foi neste contexto que a teleconsulta no país foi autorizada pelo Congresso Nacional e regulamentada posteriormente, abrindo espaço para o seu desenvolvimento nos setores público e privado.

É necessário perceber também que a aceleração decorrente da pandemia, a disponibilidade internacional e nacional de tecnologias, a experiência de uso em outros países e agora também no Brasil, e o enorme potencial de mercado apontam para um intenso investimento, mas também exploração do setor privado. Sabemos que atendimentos remotos geram dados, incluindo aqueles nos quais o cidadão interage com um aplicativo. É de se imaginar que, no modelo de negócio de algumas empresas, pode estar à venda não só o uso de uma solução de tecnologias de informação e comunicação (TIC) ou do serviço de teleatenção, mas também a captação de dados do usuário para usos que lhes gerem valor.

## USO DA INTELIGÊNCIA ARTIFICIAL

A chamada nova economia pressupõe o uso massivo de dados e da inteligência artificial, que podem gerar ganhos de efetividade, produtividade e redução de custos em diversos setores e atividades. Essa aposta estende-se também ao setor saúde, onde podem ser citadas três finalidades que miram um horizonte auspicioso para o uso da inteligência artificial em serviços públicos e privados: (i) o uso da inteligência artificial na gestão de saúde populacional; (ii) a melhoria de processos de trabalho na construção e aplicação de protocolos articulando condutas e critérios de encaminhamento, contribuindo com a equidade e redução de filas de espera; e (iii) o apoio à tomada de decisões clínicas, com aplicações que, em ato, sugeram ou desestimulem condutas.

De outro lado, temos algumas preocupações. Aplicações também podem sugerir ou desestimular condutas, além de atuarem para aumentar a indicação de um procedimento, exame ou uso de medicação desnecessários, por interesse de quem realiza lucro com os mesmos. Podem, ao contrário, desestimular a realização de procedimentos necessários em benefício de um seguro de saúde, cujo modelo de negócio consista em usar o mínimo possível de recursos ante o “sinistro” de um segurado. Os dados pessoais podem ser usados para excluir ou fazer seleção adversa de usuários de planos de saúde, na medida em que projete que certas pessoas demandarão gastos acima do custo médio. Podem, também, ser usados por diversos outros setores e empresas, sugerindo a concessão ou não de seguros de vida, crédito e mesmo a contratação ou não de trabalhadores, ou sua demissão, a partir da projeção de prejuízos ou lucros menores para a empresa em questão.

## CONCLUSÃO

O uso de tecnologias de comunicação e informação na promoção de inovações no processo de trabalho em saúde, ao proporcionar ganhos de efetividade e eficiência, é cada vez mais essencial tanto para a segurança e melhoria da qualidade do cuidado, como para o planejamento, a gestão e a própria resiliência dos sistemas de saúde. Em função de sua complexidade e do amplo leque de interesses envolvidos no processo de transformação digital na saúde, torna-se fundamental dar centralidade ao tema da qualificação e fortalecimento da governança pública dos sistemas de informações em saúde. Da mesma forma, urge elevar e garantir a transparência e proteção de dados por meio da implementação e aprimoramento da LGPD, em busca de garantir privacidade dos dados dos cidadãos usuários de serviços de saúde e proteção quanto ao uso comercial inadequado e lesivo.

É necessário, portanto, acompanhar a implementação e aplicação da LGPD e, sobretudo, avançar na legislação de autorizações de acesso e uso de dados no setor privado, como também no aprofundamento do arcabouço regulatório para coibir o uso do dado em malefício do cidadão – como ações de segmentação e seleção adversa de clientela, desrespeitando critérios de igualdade e equidade, em prejuízo do cidadão. Isto pode ocorrer a exemplo do que já há, de modo análogo, em companhias de capital aberto, com a punição do uso de informação privilegiada para a manipulação de preços, ou no judiciário, no qual um processo pode ser anulado se a prova for obtida de modo indevido.



Urge elevar e garantir a transparência e proteção de dados por meio da implementação e aprimoramento da LGPD, em busca de garantir privacidade dos dados dos cidadãos usuários de serviços de saúde e proteção quanto ao uso comercial inadequado e lesivo.

## REFERÊNCIAS

- CELES, Rafaela Santana et al. A telessaúde como estratégia de resposta do Estado: revisão sistemática. **Revista Panamericana de Salud Pública**, v. 42, p. e84, 2018.
- COELHO NETO, Gillete Cardoso; CHIORO, Arthur. Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil?. **Cadernos de Saúde Pública**, v. 37, p. e00182119, 2021
- ESPANHA, Rita; FONSECA, Rui B. Plano Nacional de Saúde 2011-2016: Tecnologias de informação e comunicação. **ISLA Lisboa**, CIES-ISCTE/IULJ, p. 3, 2010.

FERNANDEZ, Michelle; PINTO, Héider. Estratégia intergovernamental de atuação dos estados brasileiros: o Consórcio Nordeste no enfrentamento à Covid-19. **Saúde em Redes**, v. 6, n. 2 Suplem, 2020.

GONÇALVES, João Paulo Pereira et al. Prontuário Eletrônico: uma ferramenta que pode contribuir para a integração das Redes de Atenção à Saúde. **Saúde em Debate**, v. 37, n. 96, p. 43-50, 2013.

MAKARY, Martin A.; DANIEL, Michael. Medical error – the third leading cause of death in the US. **Bmj**, v. 353, p. i2139, 2016

PINTO, Héider A; SANTANA, José S.S; SILVA JUNIOR, Ailton Cardozo da; CHIORO, Arthur; MASSUDA, Adriano Massuda. Uso da Lei de Inovação para qualificar a ação interfederativa em prol da saúde. **Revista de Administração Municipal - IBAM**, Rio de Janeiro, 301, 2020a: 11-19.

PINTO, Héider Aurélio; MASSUDA, Adriano; SANTANA, José; SILVA JÚNIOR, Ailton Cardozo; COUTINHO, Leila Fraga; CHIORO, Arthur. Inovações de uma encomenda tecnológica contribuindo com novos modos de enfrentar a pandemia do Coronavírus – o caso da Plataforma Eletrônica da Saúde e do Consórcio Nordeste. **Revista de Administração Municipal – IBAM**, Rio de Janeiro, 304, 1, 25-36, 2020b.

PINTO, HA; SANTANA, JSS; CHIORO, A. **Inovação, saúde, proteção de dados e controle social**. Editora Rede Unida. No Prelo. 2022.

TASCA, Renato; MASSUDA, Adriano. Estratégias para reorganização da Rede de Atenção à Saúde em resposta à Pandemia COVID-19: a experiência do Sistema de Saúde Italiano na região de Lazio. **APS EM REVISTA**, v. 2, n. 1, p. 20-27, 2020.



## **Os tratamentos de dados em saúde devem respeitar os princípios de equidade e privacidade**

*Médico sanitarista, professor e pesquisador, Hêider Pinto defende as plataformas e outros instrumentos eletrônicos no setor de saúde, mas aponta que regulação precisa ser rígida*



**HÉIDER AURÉLIO PINTO**

Médico sanitarista, mestre e pós-doutorando em Saúde Coletiva, doutor em Políticas Públicas. Professor da UFBA e UFRB.

**O**médico sanitarista Hêider Pinto, doutor em Políticas Públicas, é um entusiasta da informatização na saúde. Quando exerceu cargos de direção no Ministério da Saúde, ele liderou a criação de ferramentas hoje largamente adotadas em todo o país, como o [e-SUS APS](#) - prontuário eletrônico presente nos atendimentos em mais de quatro mil municípios - e o [SISAB](#) - um sistema de informação nacional para a atenção básica -, além de ter dirigido o Programa [Telessaúde Brasil](#), em vigor desde 2004, um instrumento que está sendo intensamente acionado desde o início da pandemia de Covid-19.

Professor nas escolas de medicina de duas universidades federais na Bahia -UFBA e UFRB-, suas pesquisas vêm contribuindo para um processo de transformação digital na saúde com presença importante em governos do Nordeste do país, como na construção da Plataforma Eletrônica da Saúde (iPeS).

Com um pós-doutorado em Inovação, Saúde e Tecnologias em curso, Hêider Pinto acredita que, embora a recém-promulgada [LGPD](#) signifique um avanço para o Brasil, ela ainda precisa ser efetivamente implementada em seus órgãos executores e também ser acompanhada por uma regulação com regras claras a serem seguidas pelo setor privado. “O Brasil precisa introduzir uma legislação que puna, por exemplo, aquelas empresas que praticarem a segmentação de clientela em função de acesso a dados pessoais, quebrando critérios como os da equidade e da privacidade em malefício do paciente”, acrescenta o médico e pesquisador. Confira a entrevista completa:

**Idec:** O senhor esteve à frente da implementação de duas ferramentas informatizadas de gestão de saúde, o e-SUS Atenção Primária, em 2011, e o Telessaúde Brasil Redes, criado em 2004. Acredita que, em termos de ampliação ou democratização do acesso, o Telessaúde tem prestado um papel relevante para a população que vive mais afastada dos centros urbanos?

**Hêider Pinto:** Com certeza,. E essa importância ficou ainda mais evidente com a pandemia de Covid-19. O Telessaúde permite que a informação circule em vez da pessoa. Seja essa pessoa o usuário que está em localidades de difícil acesso – comunidades ribeirinhas, áreas rurais, ou municípios do interior do país sem disponibilidade de médicos ou determinados especialistas - ou o próprio profissional de saúde. Por exemplo: você consegue ter um especialista da Escola Paulista de Medicina (Unifesp) atendendo uma comunidade indígena ribeirinha na Amazônia. O serviço aumenta o acesso e permite aquilo que não exige a presença física do profissional ou um exame possa ser feito à distância. Ele garante um atendimento compartilhado entre um profissional de saúde que está no local com o paciente e um especialista que está à distância.

**Idec:** O Telessaúde continua hoje funcionando com efetividade?

**Hêider Pinto:** Reduziu muito, porque teve redução de financiamento, teve redução de recursos para as universidades, que eram parceiras importantes. Existia um 0800 que garantia às enfermeiras e aos médicos da atenção primária o acesso ao Telessaúde e isso também foi descontinuado. Então houve redução da Telessaúde em comparação, por exemplo, com o que tínhamos em 2015.

**Idec:** A classe médica chegou a resistir ao Telessaúde?

**Hêider Pinto:** A categoria médica não resistiu ao Telessaúde do Ministério [da Saúde], porque o programa não previa teleconsulta, ele operava com segunda opinião formativa, teleducação, teleconsultoria e com interconsulta. O paciente era atendido por um profissional presencialmente e o médico ou o especialista de outra área, que estava à distância, dialogava com ele. A teleconsulta, que é entrar em contato à distância com um(a) paciente para atendê-lo(a), era uma coisa que o Conselho Federal de Medicina não autorizava. Mas durante a pandemia, com a aprovação de uma nova lei no contexto da emergência sanitária, passou a se permitir a teleconsulta. De certa maneira, isso desobstruiu a proibição que havia no Brasil e uma vez que foi constatado que a teleconsulta é viável e eficiente em muitos casos, com atendimento de qualidade e sem custos, acredito que não será mais possível retroceder.

**Idec:** A forma como o Telessaúde opera traz, em sua opinião, riscos de violação de dados pessoais de saúde dos pacientes?

**Héider Pinto:** Aí tem níveis. Porque hoje os médicos e outros profissionais de saúde têm trocado informações para atender as pessoas. Na pandemia, eles estavam fazendo isso via WhatsApp. Então, imagine, eu vou pegar dados do paciente e eu posso ser mais ou menos cuidadoso. Eu posso escrever no WhatsApp, eu posso botar fotos no WhatsApp, posso mandar para um colega que pode passar para outras pessoas, posso mandar num grupo e falar “gente, me ajuda aqui com essa lesão: o que é isso?”. Então, hoje as pessoas já usam para conversar, elas estão fazendo isso sem nenhuma ferramenta especial. No Telessaúde nós tínhamos um nível pré-pandemia e pré-LGPD em que havia sistemas em que o profissional ia lá, colocava as informações do usuário e recebia a teleconsultoria de outros profissionais. Com a LGPD e com o que a gente já avançou em termos de segurança de dados, precisou ter uma adaptação, ter certificação digital, um conjunto de preocupações para proteger a privacidade do usuário. Eu quero dizer com isso que os mecanismos do Telessaúde eram adequados, mas num contexto pré-LGPD. Hoje estão em adequação e, ao mesmo tempo, a gente entende que isso é melhor do que o que acontece espontaneamente, que coloca muito mais em risco a exposição de dados do usuário.

**Idec:** Por “espontaneamente” o senhor quer dizer, por exemplo, quando as pessoas usam aplicativos que monitoram sintomas de gripe e elas colocam nele voluntariamente seus próprios dados de saúde?

**Héider Pinto:** Isso também. E também quando o médico, no serviço de saúde público ou privado onde você é atendida, passa seus dados no WhatsApp para os colegas pedindo ajuda para o seu problema.

**Idec:** O e-SUS Atenção Primária (e-SUS APS) é uma estratégia para reestruturar as informações da Atenção Primária em nível nacional. O senhor pode explicar resumidamente como ele funciona e se, em sua opinião, ele vem trazendo benefícios reais para os usuários?

**Héider Pinto:** Ele traz muitos benefícios e temos várias pesquisas provando isso. O e-SUS é um prontuário eletrônico público, ele é de uso gratuito pelos municípios. Isso reduz um custo impressionante, porque prontuário eletrônico é caro, de R\$ 3 mil a R\$ 5 mil por unidade de saúde. Então, o primeiro efeito é o gestor municipal não precisar pagar por um prontuário de ótima qualidade que é oferecido pelo Ministério da Saúde. Ele está presente em mais de quatro mil municípios, o que mostra que ele tem uma aceitação muito grande. Muitas vezes no prontuário de papel o profissional de saúde não tem a informação do paciente, ou



Ter esses dados informatizados para garantir a continuidade do cuidado ao paciente é fundamental. O e-SUS veio para qualificar o cuidado e reduzir custos dos municípios. É fundamental que se informatize o sistema de Saúde.

não encontra o prontuário anterior e tem que abrir um novo prontuário do zero, sem nenhuma informação pregressa daquela pessoa. O prontuário tem todo o histórico do paciente - doenças crônicas, como hipertensão e diabetes, saúde mental, neoplasias, problemas que os profissionais de saúde precisam acompanhar. Se perde-se o prontuário, os malefícios para o usuário são muito grandes, como demora no diagnóstico ou mesmo diagnóstico errado, prescrição de um tratamento inadequado, solicitação de exames repetidos ou desnecessários. Ter esses dados informatizados para garantir a continuidade do cuidado ao paciente é fundamental. O e-SUS veio para qualificar o cuidado e reduzir custos dos municípios. É fundamental que se informe o sistema de Saúde.

**Idec:** *Existe alguma regulação que proteja os dados pessoais coletados via e-SUS para que eles não sejam acessados por entidades secundárias ou terciárias?*

**Hêider Pinto:** O dado do e-SUS só pode ser acessado por profissionais de saúde e localmente. Se o paciente sai do município, o dado fica inacessível. Mas alguns desses dados são enviados para a Rede Nacional de Dados em Saúde, a [RNDS](#), que ainda está em construção e que pretende tornar algumas informações oriundas dos prontuários disponíveis para acesso do profissional de saúde em qualquer lugar do país em que o paciente esteja. Isso é um desafio (o compartilhamento de dados), mas, mesmo assim, o projeto da RNDS prevê esse acesso a um conjunto limitado de dados. A RNDS atualmente está compartilhando apenas os dados relacionados à Covid-19, alimentando o [ConecteSUS](#) via aplicativo e, mesmo assim, com muitos problemas, como temos visto na mídia.

**Idec:** *Em que nível de regulação da proteção de dados pessoais de saúde o senhor acha que o Brasil está? Quais são as lacunas mais preocupantes?*

**Hêider Pinto:** A gente avançou bastante com a LGPD, mas ela precisa ser implementada e a regulamentação aperfeiçoada. Elementos como os dados de vigilância à saúde, por exemplo, a gente precisa qualificar mais na LGPD, entender que a vigilância na saúde tem uma natureza diferente, que é responsabilidade do Estado garantir a proteção à saúde do conjunto das pessoas. Então dados específicos de uma pessoa que está infectada podem ser do interesse da Saúde Pública, como estamos vendo acontecer no mundo com a pandemia. Precisamos da estruturação, com efetividade e eficiência, da Autoridade Nacional de Proteção de Dados. Ou seja, implementar a LGPD do ponto de vista de seus órgãos executores. E ficar atentos sobre como o setor privado vem captando os dados. Então, quando estes são usados, não como dados de saúde - para se ter mais flexibilidade no uso dos mesmos -, mas são informações relacionadas à saúde da pessoa e interessam a decisões econômicas relacionadas aos seguros de saúde, de vida, etc. Nessa área a gente precisa avançar. Tanto para ter clareza quanto à possibilidade de compartilhamento dos dados como

quanto a ter uma legislação que puna o uso inadequado desses dados. Que puna, por exemplo, aquelas empresas que praticarem a segmentação de clientela em função de acesso a dados pessoais, quebrando critérios como os da equidade e da privacidade em malefício do paciente.

**Idec:** *O brasileiro é um usuário ativo das redes sociais e, no que se refere à saúde, a pandemia fez surgir uma enxurrada de aplicativos que monitoram tudo, dos sintomas de gripe ao peso, passando por aferição do nível individual de estresse. Quais riscos esse compartilhamento indiscriminado de dados pessoais traz para o cidadão?*

**Héider Pinto:** Nós podemos ter vários tipos de risco. Desde a coleta, via aplicativos, dos dados de perfil pessoal (gênero, idade, peso, localização geográfica), a dados relacionados a sintomas e doenças prévias. De posse desses dados, o controlador do aplicativo pode fazer várias coisas. Pode vender os dados para uma empresa tentando mostrar quais são as pessoas com determinadas doenças crônicas que são mais rentáveis do ponto de vista do plano de saúde. Pode vender algumas informações sobre determinados sintomas para segmentos da indústria farmacêutica e estabelecimentos que comercializam medicamentos, etc. Por isso, precisamos avançar na regulamentação para o setor privado, com definições claras dos termos de uso com os quais os usuários precisariam concordar. Isso não pode ficar como é hoje apenas a cargo do *compliance* das empresas de tecnologia. Segundo: precisamos de campanhas educativas, orientando a população de modo a que a sociedade tenha um comportamento proativo de fiscalização. E terceiro: uma legislação que puna tanto o uso inadequado por quem captou os dados como de quem comprou a informação para tirar vantagem econômica disso e, nesse processo, prejudicou o usuário. Por exemplo: impedindo-o de adquirir um determinado serviço ou aumentando os preços especificamente para ele em função de dados que a empresa sequer deveria ter acessado.



Precisamos avançar na regulamentação para o setor privado, com definições claras dos termos de uso com os quais os usuários precisariam concordar. Isso não pode ficar como é hoje apenas a cargo do *compliance* das empresas de tecnologia.



## **Open Health na Saúde Suplementar: regulação pró ou anti competitiva? Reflexões sobre o mercado brasileiro**

**Flávia Harumi Ramos Tanaka ; Tainá Leandro ; Fabrícia Goltara Vasconcellos Faedrich;  
Paulo Roberto Vanderlei Rebello Filho**



**FLÁVIA HARUMI  
RAMOS TANAKA**

Gerente de Monitoramento Assistencial na Agência Nacional de Saúde Suplementar (ANS). Pós-graduada em Administração Pública na Fundação Getúlio Vargas (FGV Rio).

### **INTRODUÇÃO**

Diante dos avanços tecnológicos, muito tem se discutido sobre o compartilhamento de informações entre instituições privadas para fomentar a concorrência e oferecer um serviço com mais qualidade e que melhor se adeque às necessidades dos consumidores. Alguns argumentam que seria vantajoso replicar as experiências do setor de seguros e financeiro para o setor de saúde, com o compartilhamento de dados pessoais de saúde, entre os diferentes agentes do mercado. Afirmam que o *Open Health* pode ampliar a competição nos diversos elos da cadeia de saúde.



**TAINÁ LEANDRO**

Assessora do Diretor de Normas e Habilitação da Agência Nacional de Saúde Suplementar (ANS). Doutora e mestre em economia pela Universidade de Brasília (UnB).

O compartilhamento de informações de saúde de pacientes entre prestadores de serviços médico-hospitalares tem o potencial de melhorar a saúde populacional e reduzir desperdícios. Contudo, o efeito de permitir que operadoras de planos de saúde tenham acesso a informações de utilização e diagnóstico dos beneficiários gera a possibilidade de seleção de risco, prática que afeta a estrutura mutualista com solidariedade intergeracional no qual o sistema de saúde suplementar brasileiro se ancora, o que pode resultar em aumento de preços para os que demandam maiores cuidados em saúde, como idosos e doentes crônicos.

Grande parte dos benefícios divulgados nas iniciativas do *Open Banking* e *Open Insurance*, quando traduzidos para o setor de saúde suplementar, podem ser alcançados com desenhos regulatórios que garantam segurança aos consumidores mas que não resultem em seleção de risco. Nesse contexto, é importante observar algumas das iniciativas já desenvolvidas pela Agência Nacional de Saúde Suplementar (ANS), como a portabilidade de carências, regulamentada em 2009, e que trouxe diversos benefícios concorrenenciais sem a necessidade de compartilhamento de dados individuais de utilização como foi desenhado para o setor de seguros e previdência complementar<sup>2</sup>.

<sup>2</sup> <https://openinsurance.susep.gov.br/>



**FABRÍCIA GOLTARA  
VASCONCELLOS  
FAEDRICH**

Gerente-geral de Regulação e Estrutura dos Produtos na Agência Nacional de Saúde Suplementar (ANS). Pós-graduada pela Fundação Getúlio Vargas (FGV Rio).



**PAULO ROBERTO  
VANDERLEI  
REBELLO FILHO**

Diretor-Presidente da Agência Nacional de Saúde Suplementar (ANS). Graduado em Direito pelo Centro Universitário de João Pessoa (Unipê/ PB).

O presente artigo tem como objetivo apresentar uma análise sobre *Open Health* na saúde suplementar no Brasil, sob diferentes aspectos. Na seção 2 são discutidas as premissas que baseiam o *Open Insurance* e o *Open Banking* e sua relação com o *Open Health*. Na seção 3 é apresentado o arcabouço legal que rege a matéria, enquanto a seção 4 aborda a relação entre o *Open Health* e a Rede Nacional de Dados em Saúde (RNDS). A seção 5 contextualiza as falhas de mercado na saúde suplementar e seu impacto na definição de políticas voltadas para o *Open Health*. Na seção 6 é apresentada uma discussão sobre a evolução da portabilidade de carências nos planos de saúde e os atributos do *Open Health* já alcançados pela política implementada pelo órgão regulador. Por fim, nas considerações finais, argumenta-se sobre o aprimoramento das regras do Guia ANS de Planos de Saúde como desenho para o *Open Health*.

## **DIFERENÇAS NAS PREMISSAS DO OPEN INSURANCE E OPEN BANKING VERSUS OPEN HEALTH**

Diante dos avanços tecnológicos e novos serviços e funcionalidades existentes a partir do *big data*, tornou-se uma vantagem competitiva relevante possuir volumes substanciais de dados pessoais, aumentando o valor econômico dessas informações<sup>3</sup>. Nesse contexto, o compartilhamento de dados pode fomentar a concorrência entre instituições privadas, ao ampliar a escolha do consumidor, reduzir os custos de troca e oferecer ao destinatário final um serviço com mais qualidade, adequado às suas necessidades<sup>4</sup>.

<sup>3</sup>PONCE, Paula Pedigoni. Direito à portabilidade de dados: entre a proteção de dados e a concorrência. RDC, v. 8, n.1, p138, 2020. Disponível em: <https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/view/521>

<sup>4</sup>The Right to Data Portability under the LGPD: Possible Regulatory Scenarios and Relevant Antitrust Implications. BAXAULI, Nuria D.; CRISTOFARO, Giovanna. IN ATHAYDE, Amanda; MURTA, Giulia; MAIOLINO, Isabela; LIRA, Mydyá do Nascimento; ALMEIDA, Paloma Caetano. (Coord.). Mulheres no Antitruste. Volume IV. São Paulo: Singular, 2021. Disponível em: <https://www.womeninantitrust.org>

O primeiro grande serviço de interoperabilidade no Brasil ocorreu com o *Open Banking* com normas estabelecidas pelo Banco Central em 2020, permitindo que um cliente transite entre instituições financeiras através do compartilhamento de seus dados. Em seguida, a Superintendência de Seguros Privados (SUSEP) estabeleceu uma estrutura de governança para implementação do *Open Insurance* para os consumidores de serviços de seguros e previdência complementar.

Em ambos os casos, informações pessoais de grande relevância são fornecidas pelas próprias entidades reguladas – dados de crédito, utilização de seguros, etc. Na saúde suplementar, no entanto, dados em saúde – como resultados de exames e diagnósticos de doenças – são de posse dos prestadores de serviços de saúde, atores sobre os quais o braço regulatório da ANS é limitado. Além disso, dados em saúde são considerados sensíveis de acordo com a LGPD e as regras de proteção de dados instituídas pelo Governo Federal, sendo importante avaliar de que forma o compartilhamento de dados pessoais de saúde afeta cada um dos stakeholders: consumidores, prestadores e operadoras de plano de saúde.

## ARCABOUÇO LEGAL BRASILEIRO

A Constituição Federal assegura, em seu artigo 6º, o direito à saúde como um direito social fundamental, tendo como escopo o bem-estar e a justiça social. O artigo 196 da Carta Magna consagra o direito à saúde como um direito de todos e um dever do Estado garantido mediante políticas sociais e econômicas que visem à redução do risco de doenças e agravos além de acesso igualitário e universal às ações e serviços para sua promoção, prevenção e recuperação. O artigo 197 reconhece a relevância pública das ações e serviços de saúde, permitindo que sejam executadas diretamente pelo Estado ou por particulares, desde que, sob o controle, fiscalização e regulamentação estatal.

Dessa forma, a despeito dos serviços de saúde serem facultados aos entes privados, essa permissão não desnatura seu caráter público, devendo quem os executa perseguir o atingimento do interesse público alinhado com as políticas públicas estabelecidas e não apenas buscar atingir seus interesses negociais.

A CRFB/88 prestigia, ainda, o direito ao sigilo, mesmo que não expressamente relacionado aos dados pessoais, tendo sido recentemente promulgada a Proposta de Emenda Constitucional PEC 17/2019. Inspirada na regulamentação europeia (Regulamento Geral de Proteção de Dados, o GDPR), foi aprovada em 2018 a Lei Geral de Proteção de Dados (LGPD), que estabelece regras sobre a coleta, tratamento, armazenamento e compartilhamento de dados pessoais administrados por organizações.

A Lei determina que os brasileiros são proprietários legais de seus dados e podem exigir das empresas contratadas os seus dados e informações pessoais, inclusive para compartilhar com empresas concorrentes.

Visando preservar a privacidade dos cidadãos, além de impedir práticas comerciais, sociais e políticas indesejáveis resultantes do uso de dados pessoais de forma obscura ou abusiva, a LGPD permite o uso e compartilhamento de dados pessoais apenas mediante consentimento expresso do titular do dado e a comunicação da finalidade do seu uso da informação<sup>5</sup>. Com a previsão legislativa, logo surgiram iniciativas no exterior e posteriormente no Brasil, para que empresas atrelassem um incentivo e fizessem busca ativa a esse tipo de autorização de compartilhamento de dados junto aos seus titulares.

Nos diversos elos da cadeia de saúde, a regulamentação do uso das informações pessoais, especialmente dados sobre saúde e utilização de serviços médicos e hospitalares, apresenta um desafio adicional: respeitar os limites definidos no marco regulatório brasileiro para estratégias de seleção de risco e discriminação de preço.

Os legisladores buscaram impedir que os dados de saúde de determinado indivíduo fossem utilizados como forma de restringir o seu acesso à cobertura ou aquisição de planos de saúde, ou como barreira em processos seletivos para empregos.

Não à toa, a LGPD determinou, no seu art. 11, §§ 4º e 5º, a proibição da seleção de risco no tratamento de dados pessoais relativos à saúde.

Nesse contexto, é importante destacar que a LGPD está em linha com a legislação dos planos de saúde. O art. 14 da [Lei nº 9.656, de 1998](#), limitou a possibilidade de operadoras desse setor praticarem seleção de risco. A vedação da prática de seleção de riscos na contratação de qualquer tipo de plano de saúde é reforçado pela [ANS na Súmula Normativa nº 27, de 2015](#). Já o art. 7º da [Resolução Normativa-RN nº 438, de 2018](#), proíbe a discriminação de preços no momento da portabilidade de carências.

Logo, observa-se que todo o arcabouço legal brasileiro, de forma certeira, busca assegurar o direito do consumidor à saúde garantido pela Constituição Federal Brasileira, vedando práticas de discriminação que vão de encontro ao estado de bem-estar social.

<sup>5</sup> Art. 7º, inc. I, c/c art. 8º, § 4º.



Nos diversos elos da cadeia de saúde, a regulamentação do uso das informações pessoais, especialmente dados sobre saúde e utilização de serviços médicos e hospitalares, apresenta um desafio adicional: respeitar os limites definidos no marco regulatório brasileiro para estratégias de seleção de risco e discriminação de preço.

## **OPEN HEALTH E A REDE NACIONAL DE DADOS EM SAÚDE (RNDS)**

O compartilhamento do histórico de saúde dos pacientes entre prestadores de saúde – cujas atividades estão voltadas para realização de diagnóstico e decisão sobre protocolos de tratamento – e o compartilhamento dessas informações entre operadoras de planos de saúde – empresas com fins lucrativos que especificam o acesso aos serviços de saúde para os consumidores – merecem tratamentos distintos.

Na primeira situação, o compartilhamento do histórico de saúde de pacientes entre prestadores representa um grande avanço para a efetiva implementação do Registro Eletrônico em Saúde (RES) no país. Nesse sentido, a RNDS, instituída pela [Portaria GM/MS nº 1.434, de 2020](#), propõe ser a plataforma digital de inovação, informação e serviços de saúde para todo o Brasil, em benefício dos usuários, cidadãos, pacientes, comunidades, gestores, profissionais e organizações de saúde. A RNDS é um projeto estruturante do Programa Conecte SUS do Governo Federal e tem o objetivo de permitir que os estabelecimentos assistenciais de saúde, os profissionais de saúde e os cidadãos compartilhem informações de saúde, promovendo a prevenção e o atendimento de saúde no país com maior qualidade. Além disso, visa promover a continuidade do cuidado em diferentes níveis de atenção, fundamental para a eficácia dos processos de gestão em saúde e coordenação do cuidado e é considerado essencial para o acompanhamento do processo saúde-doença dos pacientes.

Nesse sentido, uma proposta de Open Health que vise ao compartilhamento de dados em saúde é fator indispensável para a eficiência e eficácia do cuidado. Eliminar o desperdício é benéfico e fundamental para a sustentabilidade dos sistemas de saúde, porém a economia de custos deve advir de reais ganhos de eficiência, em resultados em saúde e qualidade de vida, gerando valor em saúde aos pacientes e não da transferência de custos e restrições nos tratamentos, ou, menos ainda, da redução da qualidade da assistência.

Atualmente, não se sabe ao certo em que medida os diferentes tipos de prestadores de saúde registram os dados clínicos dos pacientes, e pouco se ouve sobre registro de indicadores de resultados em saúde e desfechos clínicos, sendo necessária uma padronização desses registros, conforme previsto na [Estratégia de Saúde Digital para o Brasil 2020-2028](#) (ESD28). Atualmente, os sistemas de compartilhamento de dados estão voltados para permitir de forma mais eficiente a realização do pagamento das redes de prestadores de saúde, seja no SUS, seja no sistema de saúde

suplementar – como a Troca de Informações na Saúde Suplementar – TISS<sup>6</sup>.

É incontestável, portanto, que a informatização e integração dos sistemas de informação em saúde têm o potencial de produzir um salto de qualidade no gerenciamento do sistema como um todo e na atenção à saúde prestada à população.

Por outro lado, o compartilhamento de dados em saúde dos pacientes com e entre operadoras de planos de saúde requer uma análise específica. O uso indevido dos dados pelas operadoras pode gerar prejuízos, e não benefícios, à principal parte interessada: o paciente, usuário do sistema.

Uma proposta de *Open Health* que permita a venda de planos customizados (prática vedada atualmente) e precificados com base no histórico de utilização de cada usuário desconsidera a equação de entrega de valor em um modelo de atenção à saúde baseado no cuidado integrado durante todo o ciclo de vida, com foco na atenção primária e na prevenção, o que reduz a necessidade de utilização de serviços mais dispendiosos de alta complexidade. Precificar com base na baixa utilização estimula exatamente o contrário: que os usuários, para evitar o aumento da mensalidade do seu plano de saúde, passem a realizar menos procedimentos preventivos e busquem atendimento apenas quando estiverem em situações de maior gravidade.

Além disso, a precificação com base no perfil de utilização dos serviços de saúde despreza toda a lógica do mutualismo em que se fundamenta o sistema de saúde suplementar, como veremos na seção seguinte.



O compartilhamento de dados em saúde dos pacientes com e entre operadoras de planos de saúde requer uma análise específica. O uso indevido dos dados pelas operadoras pode gerar prejuízos, e não benefícios, à principal parte interessada: o paciente, usuário do sistema.

## ***OPEN HEALTH NA SAÚDE SUPLEMENTAR, EM UM CONTEXTO DE FALHAS DE MERCADO***

Uma das principais preocupações associadas ao compartilhamento do histórico de utilização em saúde é a ameaça à lógica de divisão de riscos na saúde suplementar

<sup>6</sup> O TISS é um padrão obrigatório para as trocas eletrônicas de dados de utilização de serviços médicos dos beneficiários de planos, entre os agentes da Saúde Suplementar.

brasileira conhecida como *mutualismo com solidariedade intergeracional*. Por “mutualismo” entende-se que, dentro de cada faixa etária, o prêmio é igual para todos os usuários e é determinado pelo risco médio daquele grupo. Ou seja, os indivíduos mais saudáveis (de menor risco) subsidiam aqueles menos saudáveis (de maior risco), dentro da mesma faixa etária. E por “solidariedade intergeracional”, entende-se que os beneficiários das faixas etárias mais jovens (de menor risco) subsidiam os indivíduos mais idosos (de maior risco)<sup>7</sup>.

Isso significa que, nos planos de saúde, os custos de consultas, cirurgias, internações e demais atendimentos são repartidos entre os beneficiários, o que possibilita a diluição das despesas, tornando-as viáveis para todos. Essa é uma característica fundamental do modelo de negócio adotado pelas operadoras de planos de saúde. Desse modo, o acesso aos dados de saúde dos beneficiários pelas operadoras e a possibilidade de que estas façam ofertas de acordo com o perfil de risco dos usuários é uma ameaça direta à estrutura no qual o sistema se anora.

Parte das vantagens competitivas comumente associadas ao *Open Banking* e *Open Insurance* está associada a ampliar a prática conhecida como *cream-skimming*, ou “seleção do bom risco”. No *Open Insurance*, por exemplo, ao compartilhar informações sobre sua apólice de seguro com uma empresa concorrente, o consumidor compartilha o seu perfil de risco e poderá ter acesso a melhores ofertas caso seja percebido como um cliente de baixo risco.

Na saúde suplementar, que se baseia no mutualismo, como explicado, é marcado por falhas de mercado como assimetria de informação, seleção adversa e risco moral<sup>8</sup> - <sup>9</sup>, tais estratégias representariam resultados regulatórios indesejáveis, ao permitir a discriminação em razão de idade e condição de saúde no ato da contratação de planos de saúde, podendo gerar danos para determinados segmentos populacionais, como os idosos e doentes crônicos. Uma proposta de *Open Health* que permita tais práticas pode representar um aumento da demanda de serviços de saúde no Sistema

<sup>7</sup> Fonte: <https://rebep.emnuvens.com.br/revista/article/view/1271>

<sup>8</sup> GAYNOR, M., Is vertical integration anticompetitive? Definitely maybe (but that's not final). [Editorial]. *Journal of Health Economics* 25 (2006) 175-180. 2006.

<sup>9</sup> ARROW, K.J. Uncertainty and the welfare economics of medical care. *American Economic Review*, December, 53: 941-973. 1963



Uma das principais preocupações associadas ao compartilhamento do histórico de utilização em saúde é a ameaça à lógica de divisão de riscos na saúde suplementar brasileira conhecida como *mutualismo com solidariedade intergeracional*.

Único de Saúde (SUS), pois os segmentos populacionais excluídos do sistema suplementar terão que recorrer ao SUS para atendimento.

Caso a regulamentação do *Open Health* desconsidere a necessidade de atenuar a seleção de risco, o resultado será uma concorrência entre as operadoras menos efetiva para atingir o bem-estar social, com efeitos limitados quanto à garantia da oferta e a melhoria da qualidade dos serviços de saúde<sup>10</sup>.

Conforme já apontado na seção 2, o arcabouço regulatório brasileiro foi claro em proibir a seleção de risco e impedir a possibilidade de discriminação de preço e limitação de acesso, enquanto a LGPD foi clara na intenção de proteger os cidadãos ao vedar às operadoras o tratamento de dados de saúde para fins de contratação e exclusão de beneficiários.

Assim, cabe aos órgãos com competência regulatória sobre os agentes do setor o papel de implementar uma política de compartilhamento de dados pessoais de saúde que amplie os benefícios para os consumidores e fomente a concorrência entre as operadoras, mas que busque diminuir a possibilidade de seleção de risco e garantir a melhoria da saúde da população e a sustentabilidade do sistema de saúde brasileiro.



Caso a regulamentação do *Open Health* desconsidere a necessidade de atenuar a seleção de risco, o resultado será uma concorrência entre as operadoras menos efetiva para atingir o bem-estar social, com efeitos limitados quanto à garantia da oferta e a melhoria da qualidade dos serviços de saúde

## OPEN HEALTH E A PORTABILIDADE DE CARÊNCIAS NA SAÚDE SUPLEMENTAR

Nos últimos 10 a 15 anos, a ANS apresentou grandes avanços em temas que começaram a ser delineados nas iniciativas do Open Insurance e Open Banking pela SUSEP e pelo BCB apenas recentemente. No setor de saúde suplementar, muitos dos benefícios divulgados nessas iniciativas não demandam compartilhamento de dados de utilização individualizados, tendo sido desenhados a partir da utilização de dados cadastrais e análises de microdados não identificados, já disponibilizados no Portal de Dados Abertos da ANS.

<sup>10</sup> GAYNOR, M., VOGT, W. B., Antitrust and Competition in Health Care Markets. in *Handbook of Health Economics*. Anthony J. Curley and Joseph P. Newhouse, Editors, Amsterdam: North-Holland. pp. 1405-1487 (Capítulo 27) 2000.

A portabilidade de carências, que foi incluída apenas na fase 3 do projeto de *Open Insurance*, foi regulamentada pela ANS em 2009. A regra passou a permitir que o consumidor que já tivesse cumprido as carências previstas em Lei pudesse mudar de plano de saúde sem o ônus de cumpri-las novamente no plano de destino, desde que atendesse alguns requisitos como: prazo mínimo de permanência, compatibilidade de preço entre os planos, adimplência etc.

Para viabilizar a portabilidade, a Agência desenvolveu o [Guia ANS de Planos de Saúde](#), que amplia a capacidade de escolha do consumidor diante da diversificada oferta de planos de saúde comercializados no país, de forma gratuita, fornecendo dados de toda a base de planos de saúde em comercialização no país. O Guia ANS possui inteligência de dados com uma interface direta com os demais sistemas de informação da ANS, contendo dados dos beneficiários, dos planos e das operadoras e conta com a aplicação das regras de portabilidade de carências na própria ferramenta. Assim, simplifica o exercício do direito, desburocratizando o processo, e confere maior segurança jurídica e legitimidade ao ato da portabilidade. O usuário precisa somente informar seu CPF e data de nascimento para ter acesso às informações do seu plano de saúde, facilitando a sua consulta. Importante destacar que os dados utilizados na ferramenta são de envio obrigatório pelas próprias operadoras de planos de saúde à ANS, periodicamente.

O Guia, além de apresentar toda a oferta de planos de saúde de determinada região, permite identificar a composição da rede hospitalar de cada plano, um dos principais elementos para a tomada de decisão para os consumidores na hora da contratação. Além disso, apresenta em um único lugar outras características relevantes do produto, como tipo de cobertura, abrangência geográfica e área de cobertura, tipo de acomodação, entre outros.

A transparência de informações que o Guia ANS promove traz um importante ganho ao setor, reduzindo a assimetria de informação e atuação de intermediários, como corretores de planos de saúde e administradoras de benefícios, ou das próprias operadoras, entes que invariavelmente ofertam os produtos de seu maior interesse comercial e permite a comparabilidade entre planos de diferentes operadoras, estimulando a concorrência no setor.

Importante esclarecer que a ANS auxilia o consumidor fornecendo informações, mas não participa diretamente de eventual aquisição ou troca de planos de saúde. A efetivação da transação em si ainda depende de contato direto do consumidor com as operadoras envolvidas.

A portabilidade de carências, apesar de representar grande avanço para o mercado, pode contar com aperfeiçoamentos a serem incluídos dentro do escopo do *Open*

*Health* na Saúde Suplementar. Alguns exemplos de melhorias são a possibilidade de simplificar o fluxo de informações entre beneficiários, operadora de origem e de destino, permitir pesquisa também por rede hospitalar, incluir informações sobre qualificação de operadoras, prestadores e indicadores de atenção à saúde, ou, ainda, informações sobre reajuste praticado por cada operadora.

## CONCLUSÃO

O bem-estar social e a sustentabilidade do setor devem ser as premissas por trás de qualquer proposta de implementação de *Open Health* no Brasil. Apesar de ser desejável que haja o compartilhamento de dados de saúde dos pacientes entre profissionais e estabelecimentos de saúde, para fins de gestão de saúde, conforme previsto na RNDS, não há benefícios claros para os consumidores se as operadoras de planos de saúde puderem acessar tais informações sensíveis.

Isso porque um eventual cenário em que as operadoras possam comercializar planos de saúde mais baratos para pessoas que tenham menor risco, resultará em planos de saúde mais caros para determinados grupos etários – como crianças e idosos – e, ainda, para indivíduos com doenças crônicas, possibilitando a exclusão desses grupos dos planos de saúde e a consequente sobrecarga do SUS. Não à toa, a legislação e a regulação do setor estabelecem limites para estratégias de seleção de risco e discriminação de preço.

Diante do exposto, conclui-se que uma proposta de *Open Health* que tenha como fundamentação precisar os planos de saúde de acordo com o perfil de utilização dos consumidores vai contra os preceitos que regem o setor e garantem sua viabilidade.

Vislumbra-se que o aprimoramento das regras de Portabilidade de Carências pode oferecer um *Open Health* que efetivamente fomente, ainda mais, a concorrência no setor, zelando pelo bem-estar social, desde que instruído de robusta análise de impacto sobre o mercado de saúde suplementar, sem a necessidade do compartilhamento de dados de saúde com as Operadoras de Planos de Saúde. Quem sabe, num futuro próximo, a portabilidade poderá ser exercida diretamente pelo Guia de Planos da ANS.



Uma proposta de *Open Health* que tenha como fundamentação precisar os planos de saúde de acordo com o perfil de utilização dos consumidores vai contra os preceitos que regem o setor e garantem sua viabilidade.





### 3 INTELIGÊNCIA ARTIFICIAL E SAÚDE

CLIQUE E ASSISTA  
O PAINEL



# INTRODUÇÃO: 3º DIA DE EVENTO



A Inteligência Artificial (IA) se desenvolveu rapidamente nos últimos 40 anos, especialmente o *deep learning* (aprendizagem profunda), uma categoria do *machine learning* (aprendizagem de máquina). Ao mesmo tempo, a capacidade institucional de regulamentação desse novo paradigma pelas sociedades de todo o planeta não acompanha o ritmo, o que coloca em risco a ética, especialmente quando se trata da interseção entre mercado e o direito humano de acesso à saúde.

Essa complexa, sensível e multifacetada convergência que envolve uma tecnologia em constante evolução e que está na base dos negócios das *big techs* - referenciadas pelo acrônimo GAFAM: Google, Apple, Facebook, Amazon e Microsoft - foi o alvo das discussões do painel *Inteligência Artificial e Saúde* no terceiro dia do evento. “Os dados são o petróleo das novas tecnologias de Inteligência Artificial”, explicou o palestrante Daniel Dourado, médico e advogado, professor de Medicina da Escola de Ciências da Saúde da Universidade Anhembi Morumbi e pesquisador do [Cepedisa](#). “A medicina de alta precisão se alimenta do processamento dos dados de saúde, que vai inferir ações de diagnóstico e tratamento, por exemplo”, explicou.

O processo de *deep learning* se dá por meio de algoritmos autodidatas que aprendem com a experiência e identificam padrões e parâmetros de comportamento das populações. Eles “rodam” em computadores que têm grande capacidade de processamento de *big data* (gigantescas quantidades de dados, analisadas simultaneamente).

Histórico familiar, sistema imunológico, uso de medicações, uso de álcool e drogas; ambiente social e padrão comportamental são exemplos de tipos de dados pessoais que podem render *inputs* via uso de Inteligência Artificial e gerar avanços na assistência de saúde em todo o mundo, destacou Dourado.

Mas em um contexto sem regulamentação e no qual a ética e a transparência sejam fracas ou ausentes, apontou o pesquisador, pode haver da violação de privacidade e o uso de dados pessoais de saúde das populações poderá culminar em mais discriminação, estigma, desigualdade e encarecimento do acesso. “Uma abordagem da IA voltada para a equidade não pode permitir que os algoritmos reproduzam a lógica da discriminação e do preconceito”, enfatizou.



Uma abordagem da IA voltada para a equidade não pode permitir que os algoritmos reproduzam a lógica da discriminação e do preconceito

Além disso, a ferramenta nascida de uma nova tecnologia não necessariamente significa um avanço, conforme constatou um estudo da organização independente [Derechos Digitales](#) ao analisar 16 iniciativas latinoamericanas com uso de aplicativos criados para enfrentar a pandemia da Covid-19. Os resultados da pesquisa foram divulgados pela painelista Jamila Venturini, jornalista, cientista social e co-diretora executiva da entidade.

A análise dos pesquisadores da Derechos Digitales sobre aplicativos desenhados para fazer *contact-tracing* (rastreamento de contatos) e alerta de exposição à Covid-19, entre outras funções, constatou que, de um modo geral, a gestão pública foi precária e não baseada em evidências. Sob a ausência de marcos normativos, regras específicas, transparência e análise de impactos aos direitos humanos não incluiu a implementação de mecanismos de monitoramento, supervisão e nem de espaços de participação. “Ainda assim, em países como Argentina, Colômbia e Uruguai esses aplicativos tiveram uma penetração que chegou a alcançar 20% da população. A gratuidade de acesso a essas ferramentas pode vir acompanhada de transações opacas dos dados de seus usuários. Isso demonstra que não basta termos uma [LGPD](#), se não tivermos um marco institucional capaz de fazer sua implementação”, frisou Venturini.

Mediadora do painel do terceiro dia do evento, a advogada Analluza Dallari, doutora e mestre em Direito Internacional e Comparado pela USP e co-coordenadora da obra coletiva [LGPD na Saúde](#), chamou atenção para o fato de que a IA, além de ainda carecer de um conceito universal e específico, é uma tecnologia em constante transformação e que é aplicada em uma gama de segmentos entrelaçados com a saúde, “do agro às cirurgias robóticas”, concluiu.



# DIREITO À SAÚDE E PROTEÇÃO DE DADOS PESSOAIS: DESAFIOS E POTENCIALIDADES



NICOLETTA DENTICO

Jornalista e analista sênior de políticas em saúde global e desenvolvimento. Diretora do Médico Sem Fronteiras (MSF) e líder do programa de saúde global da Sociedade para o Desenvolvimento Internacional (SID).

A Covid-19 inaugurou uma transformação sem precedentes na assistência à saúde em todo o mundo, tanto no que se refere aos efeitos diretos da pandemia sobre as infraestruturas de assistência à saúde quanto aos seus efeitos indiretos, aqueles decorrentes dos esforços dos governos para mitigar a proliferação do contágio.

Esta guinada levou o setor de saúde a acelerar a implantação de [ferramentas que antes da pandemia enfrentavam resistência](#), ampliando o poder de fogo analítico dos *players do Big Tech*. O [Global Pandemic App Watch](#) mostra que, até dezembro de 2020, pelo menos 74 países lançaram aplicativos para automatizar e dar suporte aos seus já existentes sistemas manuais de rastreamento de contatos (*contact tracing*).

Os aplicativos de smartphone foram interconectados a uma ampla gama de tecnologias digitais, incluindo vigilância sindrômica, aprendizado de máquina e processamento de linguagem natural, [diagnóstico digital e genômica](#). Essa “[pandemia de smartphones](#)” expandiu consideravelmente a capacidade dos governos de monitorar o comportamento individual, e os cidadãos se tornaram “cada vez mais visíveis para seus governos, mas não o contrário”, conforme sinalizado por [Philip Alston em 2019](#).

Enquanto a indústria tecnológica global “permanece virtualmente uma [zona livre de direitos humanos](#)”, um novo foco surgiu nas desvantagens dessa nova dimensão da digitalização e seu potencial para [exacerbar as desigualdades sociais pré-existentes](#). A questão é: a corrida tecnológica pode lesar o futuro do direito à saúde?

O enigma olha obviamente para futuras pandemias. A escolha entre segurança de saúde pública e privacidade e proteção de dados desencadeou muitos dilemas éticos, sociais e de direitos humanos situados na fronteira entre o valor privado e o [valor público da saúde e dos dados pessoais](#). As diferenças nas estratégias regulatórias para coleta e gerenciamento de dados foram reveladas pela forma como os governos escolheram organizar o rastreamento digital (*digital tracing*) do SARS-CoV-2. Muitas

vezes, os dados de saúde ou relacionados à saúde armazenados em aplicativos móveis e interações online não são usados para rastrear contatos [contaminados por Covid-19], mas para limitar os movimentos das pessoas e monitorar a conformidade da sociedade com as regras de emergência, apenas para citar um exemplo.

Oscritérios usados para anunciar uma situação de saúde nacional e a implementação de normas para o período de crise estão associados às experiências anteriores dos países com emergências nacionais. A abertura asiática ao compartilhamento obrigatório de dados para combater o Covid-19, por exemplo, certamente deriva de experiências anteriores com a SARS.

Na Europa, as sociedades ignoravam as mortes em massa por doenças infecciosas antes da pandemia. Enquanto isso, a experiência do regime totalitário fascista, por meio de decretos de emergência e controle governamental de vidas privadas, levou à convicção de que os cidadãos não deveriam permitir o acesso do governo a dados pessoais, mesmo sob uma emergência sanitária. Essa relutância foi ainda mais estimulada pelas revelações de vigilância do [caso Snowden](#) e pelo escândalo [Facebook-Cambridge Analytica](#), que também corroeu a confiança do público americano em um Estado que coleta e trata dados de seus cidadãos.

As *Big Techs* ganharam espaço nos sistemas de saúde dos países após a Covid-19, por isso será mais difícil afastá-las da nova arquitetura dos serviços de saúde. Seus *players* aproveitaram a pandemia para aumentar participação de mercado e os lucros, mas sua permanência na zona de conforto pode ter chegado ao fim, pois a Covid-19 colocou um microscópio mais sensível no poder da tecnologia.

Sob governança adequada, a maior disponibilidade de dados de saúde deve facilitar decisões e comunicações oportunas e transparentes aos sistemas de saúde e aos pacientes. As tensões entre a saúde e as transformações digitais devem ser resolvidas em favor dos valores centrais da saúde e da [estratégia Saúde para Todos da OMS](#), o fundamento normativo que melhor pode promover a solidariedade dos dados de saúde para um novo contrato social.



Sob governança adequada, a maior disponibilidade de dados de saúde deve facilitar decisões e comunicações oportunas e transparentes aos sistemas de saúde e aos pacientes.





**Pesquisador do Cepedisa/USP e do Institut Droit et Santé da Universidade de Paris, Daniel Dourado acredita no potencial da Inteligência Artificial, mas rejeita que ela viole privacidade**



**DANIEL DOURADO**

Médico e Advogado Sanitarista. Pesquisador Associado do Centro de Pesquisa em Direito Sanitário da Universidade de São Paulo (Cepedisa/USP); Pesquisador do Institut Droit et Santé da Université de Paris (França). Doutorando e Mestre (MSc) em Saúde Coletiva pela Faculdade de Medicina da Universidade de São Paulo (FMUSP).

**E**nquanto os debates sobre a ética aplicada à Inteligência Artificial apenas engatinham no Brasil, o crescimento do uso dessa ferramenta – inclusive na medicina - é exponencial, afirma o médico e advogado sanitarista Daniel Dourado. “Os algoritmos vão ter capacidade de entrar na assistência à saúde muito antes de a gente ter se organizado para que eles entrem”, afirma Dourado, que foi um dos participantes do painel *Inteligência Artificial e Saúde* no terceiro dia do evento do Idec.

Pesquisador do Centro de Estudos e Pesquisas de Direito Sanitário ([Cepedisa](#)), uma associação sem fins lucrativos vinculada à Universidade de São Paulo (USP), e do [Institut Droit et Santé](#) da Universidade de Paris, Daniel Dourado está neste momento estudando o modelo europeu de regulação ética da Inteligência Artificial em Saúde com a finalidade de ajudar a construir um formato para o Brasil.

Nesta entrevista concedida ao Idec, o pesquisador enfatizou que é defensor de um modelo que ajude a universalizar o acesso à saúde e traga ganhos para os pacientes sem violar a privacidade ou perpetuar as desigualdades na assistência.

**Idec:** Em sua fala no evento, o senhor observou que o deep learning, uma categoria do machine learning na Inteligência Artificial, se desenvolveu muito rapidamente nos últimos 10 anos e a capacidade institucional de regulamentação desse novo paradigma pelas sociedades de todo o planeta não acompanha o ritmo. Quais são os riscos principais, em sua opinião, que isso traz para a ética quando se trata do direito à Saúde?

**Daniel Dourado:** O deep learning se desenvolveu enormemente nos últimos 10 anos, 5 anos, porque os programadores começaram a usar o *big data*, um volume massivo de dados heterogêneos processados em alta velocidade, com a possibilidade de transportar e usar muitos dados. A capacidade institucional não tem a menor condição de acompanhar isso. O que vai acontecer é que os algoritmos vão ter capacidade de entrar na assistência à saúde muito antes de a gente ter se organizado para que eles entrem. Porque, pense bem, não é uma coisa trivial, a gente ter uma máquina intermediando ou fazendo uma atividade que é feita há séculos pelo ser humano, como dar um diagnóstico, um prognóstico, definir um tratamento – e eu não tenho dúvida de que isso vai acontecer em brevíssimo tempo. Já há computadores com capacidade para isso. Então o que a gente vai ter que fazer é organizar a sociedade para receber isso, não só na saúde como em todas as áreas, porque a Inteligência Artificial será como a eletricidade: uma ferramenta que servirá para tudo e as implicações são inúmeras.

**Idec:** O senhor também colocou em sua palestra que é por meio da Inteligência Artificial que é possível desenvolver uma medicina de alta performance. Poderia explicar o que significa essa medicina de alta performance?

**Daniel Dourado:** Os algoritmos serão usados na prática clínica, na assistência à saúde. E eles vão permitir, primeiro, que os próprios pacientes processem os seus dados. Uma coisa que hoje não é fácil e nem é comum de se fazer. Porque o que a gente tem hoje é as pessoas usando os algoritmos não do *machine learning*, mas do Google, quando estão com sintomas, e elas vão achar algo que alguém escreveu. Quando o paciente estiver usando a Inteligência Artificial, ele vai ter, em um aplicativo, os dados dele próprio: onde está geograficamente, quanto caminha por dia, quantas horas de sono, histórico clínico, etc; que vão gerar uma resposta a partir de sintomas, por exemplo, com muito mais precisão, mais próxima do que ele espera de um aconselhamento clínico.



Os algoritmos vão ter capacidade de entrar na assistência à saúde muito antes de a gente ter se organizado para que eles entrem.

**Idec: Isso do lado do paciente. E do lado do profissional de Saúde?**

**Daniel Dourado:** Pensando da perspectiva do profissional, os algoritmos vão aumentar muito a eficiência da atividade clínica: diagnósticos muito mais rápidos e mais precisos, tratamentos mais eficazes porque serão melhor direcionados, e até desenvolver drogas e tratamentos específicos para pessoas com distintas características. Hoje já há algoritmos de Inteligência Artificial que têm auxiliado na descoberta de novos tratamentos, de novas drogas, porque eles conseguem olhar variáveis e formular perguntas de pesquisa clínica, organizar grupos de uma maneira muito mais eficaz. Então são vários elementos, várias camadas de uso de algoritmos e, é claro, haverá um tipo de Inteligência Artificial para cada um desses momentos. Isso vai revolucionar nossa sociedade e a medicina está progredindo muito rápido. O crescimento é exponencial.

**Idec: Quais são, de uma forma geral, os inputs que a IA traz para essa medicina?**

**Daniel Dourado:** Além dos que eu já mencionei, da área da medicina clínica e assistencial, posso acrescentar os *inputs* para a medicina preventiva, para a tomada de decisão em política pública, porque a IA nesse caso vai trabalhar com os dados populacionais. Por exemplo: indicando as comunidades mais vulneráveis a determinada endemia, ou relações ecológicas entre animais e seres humanos que são de risco para a transmissão de agentes infecciosos. Isso ganhou relevo com a Covid-19, com a descoberta da mudança de padrão na varíola transmitida por macacos, só para citar alguns exemplos recentes. A IA vai trazer para a Saúde Pública, para a relação da ecologia com saúde, elementos que vão aportar substratos que hoje não temos e de maneira muito rápida e muitíssimo eficiente, porque o computador tem uma capacidade de “pensamento dirigido” muito maior que o cérebro humano.

**Idec: Falando agora dos riscos de violação da privacidade, o senhor mencionou que eles podem ser de ordem deontológica ou consequencialista. Pode explicar isso de forma sintética?**

**Daniel Dourado:** Vou começar pelos riscos consequencialistas. Quando os dados de alguém são usados para fazer algoritmos e esses dados vazam, caindo nas mãos de uma outra empresa ou outras pessoas, eles podem trazer prejuízos para a pessoa cujos dados foram vazados. Por exemplo: a pessoa pode perder o emprego, porque seu patrão descobriu que ela tinha um histórico de um determinado problema de saúde, ou o plano de



A IA vai trazer para a Saúde Pública, para a relação da ecologia com saúde, elementos que vão aportar substratos que hoje não temos e de maneira muito rápida e muitíssimo eficiente, porque o computador tem uma capacidade de “pensamento dirigido” muito maior que o cérebro humano.

saúde descobre que ela tem uma tendência a uma determinada doença e aumenta a mensalidade [os custos de saúde] daquela pessoa. Ou seja, a pessoa sofre uma consequência negativa em razão de um dado que foi vazado sem autorização. Isso tem a ver com a ideia da privacidade dos dados. Na perspectiva deontológica (que no direito significa “aquilo que deve ser”), se trata de que, ainda que não cause prejuízo, deve-se criar mecanismos de proteção da pessoa, pois é um dever moral da sociedade. Ou seja, a privacidade de dados é, em si mesma, um valor moral que a sociedade deve perseguir.

**Idec:** A Organização Mundial de Saúde estabelece algumas diretrizes éticas para o tópico da Inteligência Artificial em Saúde. Poderia explicar um pouco quais são elas?

**Daniel Dourado:** A OMS juntou um comitê de especialistas e construiu um “[Guia de ética para a Inteligência Artificial na Saúde](#)” baseado em seis princípios. Um deles é a autonomia, a ideia de que deve ser reservada à pessoa, ao ser humano, a *autonomia* de tomar as decisões que forem da sua esfera de direito e não delegá-la à Inteligência Artificial. O segundo é a *não-maleficência/beneficência*. Um princípio oriundo da bioética que, no caso, aponta que os algoritmos não podem fazer mal às pessoas. Ao contrário, devem fazer o bem. O terceiro é o da *transparência/expli-cabilidade*, a ideia de que o algoritmo tem que ser compreensível, pelo menos em suas linhas gerais. De que tem que haver um mecanismo de transparência que seja compreendido pelo ser humano ao menos em sua lógica geral. O quarto princípio está conectado a este terceiro. É o princípio da *responsabilização jurídica* de quem está manipulando o algoritmo no caso de usá-lo para prejudicar alguém. O princípio da *equidade*, ou inclusão, é a ideia de que os algoritmos têm que incorporar meios de não fazerem discriminação – eles não podem discriminar pessoas por condição social, por raça, por país onde mora, por idade, por gênero, etc. O último é o princípio da *responsividade/sustentabilidade*, que é um pouco mais abrangente, indicando que os algoritmos têm que responder a uma necessidade da sociedade como um todo e serem sustentáveis do ponto de vista da estrutura social. Só para dar uma ideia: não dá, por exemplo, para criar um algoritmo voltado para desempregar pessoas.

**Idec:** Em que estágio o senhor acha que o Brasil está hoje? Onde é preciso avançar?

**Daniel Dourado:** O Brasil está em uma fase muito inicial. Em junho deste ano a Comissão do Congresso Nacional que está fazendo a discussão sobre Inteligência Artificial ([CJUSBIA](#)) pediu prorrogação dos trabalhos por 120 dias. Eles estão ouvindo especialistas de outros países para entender, por exemplo, os elementos éticos necessários. Mas ainda não há no Brasil o desenho de um projeto de lei para regulamentar a IA na Saúde. A discussão é em cima de uma lei geral de uso da IA, e a comissão do Senado está formulando um projeto de lei que vai detalhar e talvez especificar elementos específicos da IA por setor. Eu acho que o Brasil avançou bastante

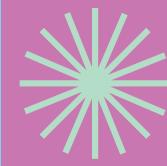
do ponto de vista da privacidade. A LGPD é uma lei boa, inspirada no regulamento europeu. Mas na prática estamos atrasados porque demoramos para implantar a lei. A [Autoridade Nacional de Proteção de Dados](#) somente em 2021 começou a funcionar efetivamente. Então, é nos próximos anos que a coisa vai acontecer, o Brasil tem muito que avançar nessa discussão. Por exemplo: as empresas desenvolvedoras, como elas vão entrar no mercado? O que vai precisar para um algoritmo, de fato, valer?

**Idec:** *O senhor acredita que a Inteligência Artificial pode ajudar as sociedades a atingirem uma cobertura universal de assistência de saúde de suas populações? De que forma?*

**Daniel Dourado:** Veja, os sistemas de saúde são uma coisa recente, eles existem de 1948 para cá. Então, é a primeira vez nessas décadas que há a possibilidade de os sistemas de saúde visualizarem uma oportunidade de redução de custo. Porque os sistemas de saúde sempre incorporaram a tecnologia acompanhada de um encarecimento. Além disso, as populações começaram a viver mais e, com isso, a usar mais os sistemas de saúde, que consequentemente têm que gastar mais. E isso é um grande obstáculo ao alcance da cobertura universal, mesmo nos países ricos. Com a Inteligência Artificial há a possibilidade de que essa tecnologia seja incorporada com um custo baixo, muito menor, por exemplo, do que o custo de se construir uma indústria para produzir uma vacina. O algoritmo tem custo de implantação barato, a aplicação é imediata e isso pode acelerar a possibilidade de acelerar a cobertura, inclusive beneficiando populações onde há escassez de recurso humano de saúde.



# EXPERIÊNCIA LATINO-AMERICANA: NECESSIDADE DE MECANISMOS DE PARTICIPAÇÃO E MONITORAMENTO



## *Implantar tecnologias sem debate público foi naturalizado na América Latina*

*Análise de 16 aplicações digitais criadas na região durante pandemia revelou que ausência de mecanismos de participação e monitoramento colocou direitos humanos e privacidade em risco*



**JAMILA VENTURINI**

Jornalista e mestra em Ciências Sociais com foco em Educação pela FLACSO (Argentina). Atualmente é co-diretora executiva na Derechos Digitales

**A**s ferramentas digitais de *contact-tracing* implantadas em 14 países da América Latina com o objetivo de desacelerar a transmissão do coronavírus nasceram com vícios de origem, alerta o [informe](#) “Uma análise crítica das tecnologias implantadas na América Latina contra a pandemia”, produzido pelo Observatório Covid-19 do [Consórcio Al Sur](#).

“A implantação de aplicações no conjunto das medidas de emergência sanitária reproduziu a cultura que permeia, tradicionalmente, a formulação de políticas públicas na região: ocorreu sem se basear em evidências científicas, sem análise prévia de impactos aos direitos humanos e desconectada da introdução de mecanismos de participação popular, monitoramento e análise de eficácia”, resume a brasileira Jamila Venturini, jornalista, cientista social e co-diretora executiva da [Derechos Digitales](#), uma das onze organizações responsáveis pelo levantamento feito em 2020 e também uma das autoras do informe.

Essa tendência, advertiu o estudo, explica uma atitude geralmente passiva do Estado em relação à adoção de tecnologias que podem afetar diretamente o exercício dos direitos fundamentais da população<sup>11</sup>, e uma ausência sistemática de consulta a vários interessados. “Foram decisões puramente administrativas, apesar de se tratar

<sup>11</sup> Sobre o tema, sugere-se também a leitura: CRUZ, Luã; CONTRI, Camila Leite; ROSA, Larissa. Privacidade, dados e pandemia: balanceamento entre contenção do contágio e LGPD. In: CGI.BR. TIC Domicílios 2020. São Paulo: CGI.br, 2021, p. 145-157. Disponível em: [https://cetic.br/media/docs/publicacoes/2/20211124201233/tic\\_domiciliros\\_2020\\_livro\\_eletronico.pdf](https://cetic.br/media/docs/publicacoes/2/20211124201233/tic_domiciliros_2020_livro_eletronico.pdf).

de implementações que podiam ter consequências importantes para a privacidade", observa Jamila.

Nesta entrevista ao Idec, a pesquisadora afirma que é preocupante o fato de que, quando se trata de uso de tecnologias pelo Estado, há uma naturalização sobre a desnecessidade de um debate amplo junto à sociedade e ao Poder Legislativo que fundamente, embase e legitime sua implementação.

**Idec: O que foi que motivou o Consórcio Al Sur a conduzir a pesquisa sobre as ferramentas digitais criadas no período da pandemia de Covid-19?**

**Jamila Venturini:** A pesquisa nasceu de uma preocupação grande que a gente tinha na América Latina sobre abusos relacionados aos direitos digitais durante a pandemia. Fazia pouco tempo que a pandemia havia começado na região e já se via uma tendência da aprovação de decretos de emergência com conteúdos ambíguos. Além disso, se multiplicavam acordos entre estados e empresas de telecomunicações para monitoramento das medidas de isolamento sem qualquer informação sobre quais os limites do compartilhamento de dados, tanto por parte do governo com as empresas, quanto por parte das empresas com o governo, assim como sobre como estavam sendo interpretados esses dados de conexão à rede celular. Cabe lembrar, que a América Latina vinha de um contexto conturbado desde 2019, quando foram registrados diversos tipos de abusos durante protestos populares que se replicavam na região. Por isso, a gente decidiu fazer essa análise de quais aplicações estavam sendo utilizadas e quais os limites para essa utilização, inclusive no que tange à reutilização de dados obtidos a partir delas.

**Idec: A pesquisa foi baseada em entrevistas ou no estudo dos aplicativos criados? Como foi o processo desse estudo dos apps?**

**Jamila Venturini:** O primeiro passo foi identificar os países que estavam implementando essas aplicações. Em todos os casos, a gente analisou as aplicações implementadas em nível nacional; uma aplicação por país, apesar de que alguns países tiveram mais do que uma-a única exceção foi a Bolívia, de onde a gente analisou três aplicações. Fizemos a análise documental e de matérias da mídia sobre essas aplicações, e o principal mecanismo de obtenção de informações foram os pedidos de acesso. Na maioria dos casos, foi possível obter certa informação dessa maneira; em alguns casos, e para certas informações, a gente encontrou limites, e isso também está refletido nos resultados da nossa pesquisa. Essas informações são de interesse público, e deveriam estar acessíveis para análise independente e revisão da cidadania. Em alguns casos, foram realizados testes técnicos para identificar indícios de compartilhamento de dados - isso foi feito pelo [InternetLab](#), por exemplo, que identificou tráfego de dados com algumas empresas que não estavam identificadas na polí-

tica de privacidade da aplicação brasileira. No caso do Equador, cujo levantamento foi liderado pela Derechos Digitales, a gente realizou entrevistas com participantes do processo de desenvolvimento ou de implementação das aplicações.

**Idec:** *Uma das conclusões do estudo, no que tange à legalidade, foi a ausência de marcos normativos ou regras específicas na implantação de soluções por meio das quais os dados pessoais de saúde de cidadãos seriam coletados, armazenados e tratados. Essa constatação foi geral para todos os países pesquisados? Nenhum deles está um pouco mais avançado que os demais no aspecto da regulação?*

**Jamila Venturini:** Alguns países estão um pouco mais avançados em relação à regulação de proteção de dados e à regulação relacionada à Telemedicina. Um desses países é o Uruguai, país que conta com uma equivalência em relação ao padrão europeu. Eles tinham uma resolução da sua Autoridade de Proteção de Dados relacionada ao tratamento de dados durante o período de pandemia. Nos demais países o contexto é desigual. Alguns não têm uma lei geral de proteção de dados ou regras específicas se aplicarem à matéria – que é o caso da Bolívia, por exemplo, e era o caso do Equador no momento da pesquisa, já que a norma equatoriana foi aprovada depois da pesquisa ter sido realizada. Também havia países que, embora tivessem uma lei de proteção de dados, ela não estava suficientemente atualizada para os desafios no mundo digital, como é o caso do Chile – que tem uma das primeiras leis de proteção de dados da região, mas que está bastante desatualizada em relação ao desenvolvimento tecnológico e aos desenvolvimentos normativos desde a sua aprovação. O Chile, por exemplo, não conta com uma autoridade de proteção de dados independente capaz de supervisionar a implementação desse tipo de aplicação para transações de dados.

**Idec:** *E qual era a situação do Brasil nesse aspecto?*

**Jamila Venturini:** O Brasil tinha uma lei de proteção de dados ainda em fase de implementação e a aplicação que nós analisamos é anterior a essa data. O que muitos países fizeram foi, durante o período de emergência, estabelecer exceções ao consentimento para o processamento de dados de saúde. Isso é compreensível e justificável numa emergência sanitária: os dados precisavam ser tratados, acessados, compartilhados, inclusive para fosse desenvolvida uma resposta adequada de contenção e de impedimento do avanço da pandemia. E a gente viu e sentiu os desafios e consequências de não se ter uma política desse tipo aqui no Brasil. Mas a grande questão é quais são os limites para o compartilhamento com o setor



Uma vez que os dados são de acesso do setor privado, eles podem ser incorporados a outros bancos de dados e eventualmente se perde controle sobre essa cadeia de tratamento.

privado. Porque muitas dessas aplicações eram desenvolvidas pelo setor privado e aí você não tinha tanta transparência em relação às condições de acesso e uso e da reutilização desses dados para outros fins. Uma vez que os dados são de acesso do setor privado, eles podem ser incorporados a outros bancos de dados e eventualmente se perde controle sobre essa cadeia de tratamento. Um outro ponto que a gente chama atenção quando falamos de legalidade na implementação de tecnologias pelo setor público é relativo a quais são as partes que discutem aquela implementação específica, e nesse caso foram decisões puramente administrativas, apesar de se tratar de implementações que podiam ter consequências importantes para a privacidade. Houve outras medidas emergenciais, como o caso do auxílio emergencial no Brasil, que passaram por discussões no Legislativo. E quando a gente pensa em uso de tecnologias pelo Estado parece que existe quase uma naturalização de que um debate mais amplo com outros setores do governo e da sociedade não é necessário.

**Idec:** *Quando o relatório de conclusão da pesquisa aponta que inexistiu análise de impacto aos direitos humanos, a que exatamente está se referindo?*

**Jamila Venturini:** A nossa pesquisa aponta que o tipo de consequência, o tipo de impacto ao exercício de direitos dessas tecnologias vai muito além da privacidade. Você tem o risco de utilização discriminatória desses dados por parte do setor privado, você tem o risco de vazamento desses dados, o que pode ter até consequências econômicas para as pessoas, a depender de como esses dados serão utilizados. Além disso, em alguns casos o uso dessas aplicações era obrigatório para pessoas que precisavam circular pelas cidades. Quando havia períodos de isolamento estrito e era necessária uma autorização para circulação - como foi o caso na Argentina, por exemplo - essas aplicações mediavam esse acesso. Essa circulação e qualquer falha nesses sistemas que foram implementados poderia afetar direitos como à livre circulação, de acesso ao trabalho e uma série de outros direitos e serviços. Então a gente defende, junto com especialistas de Direitos Humanos e organismos internacionais como a Comissão Interamericana de Direitos Humanos, que é necessário o desenvolvimento de um estudo prévio que antecipe os tipos de impactos que esses sistemas podem ter, uma análise ampla em relação aos direitos humanos. Já está estabelecido em alguns países, inclusive no Brasil, uma análise prévia de impactos à privacidade e o que a gente está propondo é uma análise de impactos em direitos humanos que inclua uma análise mais holística da tecnologia a ser implementada para identificar justamente que tipo de consequências ela pode trazer quando aplicada, quais riscos que ela representa e como mitigar esses riscos.

**Idec:** Na parte relativa à proporcionalidade e necessidade, a constatação foi de que faltou basear o desenvolvimento das políticas públicas em evidências e também que não houve espaço para monitoramento e participação. Você acha que isso foi intencional ou poderia ter sido o açodamento da emergência sanitária?

**Jamila Venturini:** Isso faz parte de uma cultura de formulação de políticas públicas sem base em evidências e sem participação pública. Por mais que a nossa região tenha um histórico amplo e muito valioso de criação de mecanismos de consulta pública e de participação – como as grandes conferências no Brasil, por exemplo, de Saúde, de Direitos Humanos, de Educação –, essa prática parece estar se perdendo nos últimos anos, e ela é praticamente inexistente quando se trata da implementação de sistemas tecnológicos pelo Estado. A gente analisou, como Derechos Digitales, uma série de outros casos de uso de tecnologias que extrapolam o contexto da emergência sanitária, em que observamos as mesmas práticas da ausência de evidências. Isso indica que há uma espécie de confiança cega no valor da tecnologia para responder a um determinado problema. Tão cega que não inclui nem uma análise prévia sobre aquela ser a solução realmente adequada para o problema, ou sequer uma avaliação posterior sobre sua eficácia. Não há mecanismo de análise – nem no âmbito do setor público, nem disponível para a população – sobre se o uso daquela tecnologia foi ou não efetivo, se aquele gasto financeiro, de recursos humanos, ou outro, foi realmente justificado e merece ser continuado, o que é problemático.

**Idec:** A pesquisa apontou que os apps tiveram grande penetração na Argentina, Colômbia e Uruguai alcançando (20% da população). Quais foram as implicações e riscos dessa penetração?

**Jamila Venturini:** A penetração foi maior nesses países, porque havia certo grau de obrigatoriedade no uso das aplicações. Na maior parte dos países a adoção era voluntária e ficou entre 0,5% e 3% da população. Muito incipiente, em razão de vários fatores, inclusive das desigualdades digitais, que ficaram muito evidentes durante a pandemia. Além da falta de uma divulgação coordenada das aplicações como estratégia de prevenção e combate ao coronavírus e da falta de legitimidade das iniciativas uma vez que não há um monitoramento de como são implementadas. A própria retórica que justifica essas aplicações em alguns países foi tão otimista que uma eventual frustração com seu uso poderia contribuir com um cenário de descrédito das instituições públicas e das soluções científicas para o combate à Covid-19. Mas na Argentina, Colômbia e Uruguai a aplicação estava associada a outros serviços relacionados a autorização de circulação, tanto para quem vinha do exterior como para quem circulava dentro do país. Então houve uma adesão maior. Tivemos também setores da população que foram obrigados a fazer o monitoramento de sintomas com essas aplicações nos momentos de flexibilização – no caso do Uruguai, o setor

esportivo, por exemplo. A preocupação aí é o impacto do mal funcionamento dessas aplicações, ou de eventuais resultados equivocados, ao direito à livre circulação, ao direito ao trabalho, entre outros.

**Idec: O estudo encontrou alguma boa prática?**

**Jamila Venturini:** Sim, no Uruguai, onde a política não assumiu, por padrão, que todos os indivíduos tinham um aparelho celular, individualmente disponível para utilizar a aplicação. Por desenho, a aplicação previa o uso por múltiplos usuários, o que me parece uma prática interessante – além de outras práticas relacionadas a acessibilidade, por exemplo -, porque ela não assume um acesso à tecnologia que não necessariamente representa o contexto de um país ou de uma família na América Latina. E isso no Uruguai que é o país com maior acesso proporcional à Internet na América Latina, que possui políticas de inclusão digital direcionadas à população jovem, à população idosa e políticas de governo eletrônico muito extensas. No Brasil, a assunção prévia de que todas as pessoas dentro de uma mesma família, teriam acesso a um dispositivo próprio criou uma série de problemas e dificuldades no caso do auxílio emergencial, inclusive com a exclusão de pessoas de benefícios emergenciais para enfrentamento da pandemia.



# ENCERRAMENTO



**A**saúde enquanto direito, os princípios que orientam o SUS - universalidade, integralidade e participação comunitária - e a própria ideia ampliada de saúde, que inspirou a criação do sistema no contexto da Reforma Sanitária, oferecem caminhos para lidar com os novos desafios deste tempo.

O Idec, com este trabalho, mostra que as discussões sobre o uso de dados em saúde ainda estão em construção tanto no Brasil quanto no mundo. Nesta publicação, abordamos as interligações do uso de dados em questões de acesso a medicamentos, acesso e utilização de serviços de saúde e de inteligência artificial no campo da saúde a partir de contribuições de grandes nomes nacionais e internacionais no campo, desde autoridades, a acadêmicos(as), a médicos e a entidades da sociedade civil.

Entretanto, apesar de ser um campo ainda em construção, temos grandes preocupações centrais que visam ao equilíbrio entre a proteção de dados e o acesso à saúde dos cidadãos. Com isso, aponta-se para um possível e necessário caminho de fornecer uma saúde pública, gratuita e de qualidade para todos os brasileiros e brasileiras e que isso deva ser feito sempre com respeito à privacidade, proteção de dados, à liberdade e demais direitos e garantias fundamentais.



