



Right to Health and Personal Data Protection: contemporary challenges and potentials





Right to Health and Personal Data Protection:

contemporary challenges
and potentials

CREDITS

AUTHOR

Idec – Brazilian Institute for Consumers Defense

SUPPORT

Open Society Foundations

INSTITUTIONAL

Carlota Aquino Costa - Executive-Director

Igor Rodrigues Britto - Institutional Relations Director

Georgia Carapetkov - Programs and Projects Manager

ORGANIZATION

Ana Navarrete - Health Program Coordinator

Camila Leite Contri - Telecommunications and Digital Rights Program Lawyer

Matheus Zuliane Falcão - Health Program Analyst

Marina Paullelli - Health Program Lawyer

Marina Fernandes de Siqueira - Intern at the Telecommunication and Digital Rights Program

COPYWRITER

Ludmilla Duarte - Journalist

CONTENT REVIEW

Fernando Gentil - Communications Analyst

JOURNALIST SUPERVISOR

Daniel Torres - Communications Coordinator

Press contact: imprensa@idec.org.br

August 2022

We are a non-profit civil society organization that works to protect and expand the rights of consumers, away from the influence of governments, political parties, and companies. Our work is supported by project resources from philanthropic foundations and donations from individuals who believe in the importance of what we do. Since 1987, we have represented consumers across the country in a struggle for fairer consumer relations, especially in telecommunications and digital rights, financial services, health, adequate and healthy food, mobility, energy, and sustainable consumption.

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

CONTENTS



FOREWORD	4
ACCESS TO MEDICINES, THE PHARMACEUTICAL INDUSTRY, AND PERSONAL DATA PROTECTION	6
INTRODUCTION: 1 st DAY OF EVENT	7
SECURING HEALTH DATA AS A GLOBAL PUBLIC GOOD: SOME CRUCIAL CONSIDERATIONS FOR EQUITY (Article: Anita Gurumurthy/Nandini Chami)	10
PHARMACEUTICAL INDUSTRY AND PERSONAL DATA PROTECTION: THE BRAZILIAN EXPERIENCE (Interview: Joyce Souza)	13
HEALTHCARE SERVICES AND PERSONAL DATA PROTECTION	19
INTRODUCTION: 2 nd DAY OF EVENT	20
HEALTHCARE SYSTEMS DIGITALIZATION: THE SOUTH-KOREAN EXPERIENCE: Secondary Use of Public Health Data in Korea: Commercial Research and Public Interest (Article: Junho Jung)	22
“The challenge is to have the public property generating public good,” says Korean researcher (Interview: Junho Jung)	25
HEALTHCARE SYSTEMS DIGITALIZATION: THE BRAZILIAN PERSPECTIVE Right to health, digital transformation and data protection (Article: Heider Aurélio Pinto; Jose Santos Souza Santana; Arthur Chioro)	31
Access and use of citizen Health data must respect equity and privacy e privacidade (Interview: Hêider Pinto)	38
Open health in supplementary health: pro or anti-competitive regulation? Reflections on the Brazilian market (Article: Flávia Harumi Ramos Tanaka; Tainá Leandro; Fabrícia Goltara Vasconcellos Faedrich; Paulo Roberto Vanderlei Rebello Filho)	43
ARTIFICIAL INTELLIGENCE AND HEALTH	53
INTRODUCTION: 3 rd DAY OF EVENT	54
RIGHT TO HEALTH AND PERSONAL DATA PROTECTION: CHALLENGES AND POTENTIALS (Article: Nicoletta Denticò)	56
AI WILL BE A REVOLUTION IN SOCIETY AND MEDICINE (Interview: Daniel Dourado)	58
LATIN AMERICAN EXPERIENCE: THE NEED FOR PARTICIPATION AND MONITORING MECHANISMS Public Debate Is Essential When Implementing Technologies is Naturalized in Latin America (Interview: Jamila Venturini)	63
CONCLUSION	68

FOREWORD



The Brazilian Consumer Defense Institute works since 1987 for the rights of all Brazilians through different themes and programs. Throughout these 35 years, Brazilian society has undergone several changes in various sectors, including technology and health.

In order to follow the paths and changes brought about by the adoption of technologies, Idec started working with projects that involve analysis, inspections, and claims for policies related to the protection of personal data, with special attention regarding health data.

Over these years, several cases were led by Idec in the fight for consumer rights. This protagonism also occurred in battles against government bodies, such as the Ministry of Health (MS), the National Health Surveillance Agency (Anvisa), and the National Supplementary Health Agency (ANS)¹. The Institute's primary duty is to fight for people's rights.

One of these cases was the **profiling performed by private healthcare plans**: some were scoring healthcare users according to their lower or higher risk for health problems and the likely frequency they would demand the healthcare services. Idec acted firmly against companies and employers' associations that tried to include this type of system in Brazil's supplementary healthcare system.

Since 2019, Idec has notified companies, entities, and even the Federal Council of Medicine (CFM) to prevent similar deviations that violate the Consumer Defense Code and the newly approved General Data Protection Law (LGPD).

Still on the same topic, in 2020, Idec notified a company that was trying to **sell health data** on a marketplace – which also contravenes the rules of the CFM and the LGPD.

The Institute played a direct role in cases of user **data leakage** that occurred at Anvisa and the Ministry of Health. Several breaches have come to light, even after the enactment of the LGPD. Two deserve to be highlighted: the one from Anvisa, on which patients authorized to use Cannabidiol had their data leaked; the second major incident involved data in possession of MS in 2020. Although quite different, both were relevant

¹ Supplementary health in Brazil may be understood as the economic sector of private health insurance companies working in competition and regulated under the Parliamentary Act Law n. 9656/98.

due to the leakage of medical data, considered sensitive personal data and potentially harmful if exposed.

In the event involving Anvisa, which took place in February 2020, Idec demanded through official letters that the regulatory agency submit a reaction plan. After the leaks at the Ministry of Health, the Institute requested that the Federal Public Ministry (MPF, Brazilian national prosecution body) investigate the situation. Our document highlighted the potential harm to those affected and the need for public sector efforts toward consumer protection and compliance with the LGPD, that had already come into force. The MPF is still working on that case, which was the subject of a necessary public hearing.

Another Idec significant action concerned **personal data processing in pharmacies**. It is not uncommon in Brazil that in pharmacies consumers are asked to give their document number (CPF, similar to the social security number in some countries) upon purchasing a medication.

In June 2021, an episode exacerbated concerns about the practice: the demand from a specific pharmacy chain for customers to supply their fingerprints. Reports from customers flagged the matter. Fingerprints are biometric (biological) data that, like health data, are subject to even greater processing requirements: they are considered sensitive personal data.

Idec sent the drugstore chain an extrajudicial notification requesting clarification and emphasizing that data processing must be guided by transparency, legality, and security. A demand for information was also sent to Abrafarma (Brazilian Association of Pharmacy and Drugstore Networks). As an outcome, the pharmacy network stopped asking for biometrics in exchange for discounts.

These aforementioned are just some of the cases that show that personal data protection in health is a core right for Brazilians, which is why it is one of Idec's greatest battles.

Therefore, the Institute has its specific action front for the interface of Data and Health themes. Our efforts culminate in this publication, which consolidates the lessons learned from a long and complex work process, to which the event "Right to Health and Protection of Personal Data: contemporary challenges and potentialities" was added. The international conference was held between May 17 and 19, 2022, having the South Centre and ICICT as valuable participants.

The following production summarizes this work in which civil society, authorities, and some of the world's leading researchers in health and personal data protection are our partners.



Personal data protection in health is a core right for Brazilians, which is why it is one of Idec's greatest battles.





1 ACCESS TO MEDICINES, THE PHARMACEUTICAL INDUSTRY, AND PERSONAL DATA PROTECTION

CLICK AND WATCH THE EVENT VIDEO



INTRODUCTION: 1st DAY OF EVENT



The lack of regulation jeopardizes data security and allows irregular access to the sensitive personal health information on digital platforms, as experts emphasized during the first round of debates. They unanimously agreed that medication prescriptions might not lead to the misappropriation of patient data by the pharmacy sector, health insurance companies, and other secondary or tertiary sources.

The Covid-19 pandemic has accelerated the phenomenon of “platformization” of society - in the words of Indian researcher Anita Gurumurthy, co-founder of the NGO [IT for Change](#) -, or “datafication” of capitalist economies, according to the journalist and social scientist Joyce Souza, a researcher at the Federal University of ABC (São Paulo, Brazil). In other words, there is an excessive increase in platforms of data usage across different areas of society, and, despite making many things easier, it also raises several concerns.



There is an excessive increase in platforms of data usage across different areas of society.

At the opening, Georgia Carapetkov, program and project manager at Idec, highlighted the importance of this type of event. “The technologies incorporated into people’s routine can also impose a negative consequence, such as the private appropriation of personal data. Countries must align their computerized functioning in order also to realize the citizens’ right to health and fulfill their constitutional duties. Also, societies must think about where they want to be”, she affirmed.

The three panelists agreed that personal data has a market value, and each approached the risks of its appropriation from different perspectives.

Researcher Angela Acosta, from the University of Cali (Colombia), presented as an example the Australian mobile application that aims to monitor its users’ mental health (anxiety and stress levels). The app belongs to the private telecommunications company Telstra, which offers 5G speed and brings together the most significant number of customers in that country.

“How is this information being handled and kept secure? Concern over ethics is a debate now taking place in Australia. We have new environments on the one hand and a lack of regulation and surveillance on the other,” said the researcher, who holds a Ph.D. in Pharmaceutical Sciences and Pharmacoepidemiology.

In Brazil, the [LGPD](#) (General Personal Data Protection Law), which had the European law ([GDPR](#)) as its model, imposed boundaries on the corporate world. “But there are still many loopholes,” Joyce Souza pointed out. “The collection of citizen’s biometric data upon purchasing a prescribed medication, for example, is a rarely discussed topic within the National Health Agency (ANS, its acronym in Portuguese),” she stressed.

Souza’s academic work addressed another severe problem involving privacy and health data. During field research among drugstores in São Caetano do Sul (São Paulo), she found that, in exchange for high discounts on medicines, the companies were collecting personal, clinical, and even financial data from customers (such as the amount spent and the payment method). The pharmacies subsequently passed the collected data to healthcare insurers and private healthcare plans.

“A third issue involving pharmacies is that many take orders via apps, digital platforms, or websites. These are software developed by third-party companies that also end up having access to patient data,” she stated.

According to Anita Gurumurthy, the primary motivation for countries to regulate the access, use, and processing of personal data come from the need for the market to be prepared to resolve the tension between sensitive information, such as citizens’ health data, and the enormous commercial value it possesses.

In China, she cited, the law established in 2021 combines data security with cybersecurity to rule out the possibility of Chinese data being collected by foreign entities. “In the context of some bilateral and multilateral agreements on digital services, developing countries ‘lose’ their citizens’ health data because they do not have this protection. Different regulations are required for different types of data; public and private data users must be subject to distinct governance,” she believes.

Panel moderator and coordinator of the Development, Innovation, and Intellectual Property Program at the [South Center](#) (an intergovernmental organization based in Geneva, Switzerland), Viviana Muñoz highlighted: “what is clear is that governments need to create policies and regulations, and they need to be very careful with the choices they make.



Access to medicines is an essential element of the right to health, and its regulation needs to improve,” she pointed out. “But it also needs to move forward in aspects such as generating better and broader health services, collaborating with research for the development of new drugs and treatments, in addition to reducing inequalities in access to Healthcare

Access to medicines is an essential element of the right to health, and its regulation needs to improve,” she pointed out. “But it also needs to move forward in aspects such as generating better and broader health services, collaborating with research for the development of new drugs and treatments, in addition to reducing inequalities in access to Healthcare.”



SECURING HEALTH DATA AS A GLOBAL PUBLIC GOOD: SOME CRUCIAL CONSIDERATIONS FOR EQUITY



ANITA GURUMURTHY

Founder and
Executive Director of
IT for Change (ITfC).

The [imperative](#) to “secure health data for, and as a, global public good” through an approach that can maximise benefit and minimise harms was [underscored by the WHO](#) in the wake of the pandemic,

In the age of big data and AI, health innovation for public benefit implicates a [multiplicity of data](#) – patient health records, clinical research data, health worker activity records, environmental information, genomic data about humans and pathogens, and increasingly, data footprints from wearables, apps, and IoT gadgets.



NANDINI CHAMI

Deputy Director of
IT for Change (ITfC).
Master in Urban and
Rural Community
Development from
the Tata Institute
of Social Sciences
(Mumbai, India).

The WHO’s Global Public Goods (GPG) approach provides a starting point to make health data accessible for systemic change. But its efficacy for public innovation, institutional resilience and equitable health access depends on a global health data regime that can effectively address the risks of public value capture and no-holds-barred profiling of people and the planet. An unregulated data economy thriving on neo-colonial impulses will only make health-for-all a distant dream.

PRIVATE CAPTURE OF PUBLIC DATA

Public architectures for health data sharing in the [UK](#), [Denmark](#), [Sweden](#), and India reflect a high risk of private capture of such open datasets by multinational companies. Developing countries are even more vulnerable to data extractivism, dependent as they are on foreign firms for big data-driven research. The [GenBank case](#)

shows how gene sequences from the Global South shared in open access repositories online are used by Northern pharma companies to build patented treatment lines, with current international law [unable](#) to ensure fair and equitable benefit sharing with source communities.

The stark scenario of unidirectional data flows from the South into the coffers of Northern Big Tech/Big Pharma raises critical questions about geo-economic power in the ‘intelligence economy’ and the consequent hollowing out of knowledge and institutional data capabilities from the South.



An unregulated data economy thriving on neo-colonial impulses will only make health-for-all a distant dream.

EROSION OF SOCIAL AUTONOMY

In the age of ubiquitous cross-border health data flows, [traditional approaches](#) to health information privacy – pegged on the sensitivity of data categories with differential notice and consent thresholds – do not anticipate the unknowable risks of data reuse and processing. Some typologies of data deemed to be less sensitive [may not carry](#) high safeguards for privacy. However, seemingly innocuous data – such as data from wearables – can be easily recombined and analyzed for unethical/unlawful profiling and targeting.

While laws like the GDPR attempt to protect individual rights to privacy for European citizens, the rights of individuals and groups (e.g., [menstruating women](#), [Indigenous people](#)), particularly in developing countries lacking such laws, are at huge risk of abuse as data travels out of their jurisdiction.

AN EQUITY-CENTERED GPG APPROACH FOR HEALTH DATA

The AI era heralds a moment that demands wide-ranging global-to-local debates about the innumerable ethical questions embedded in health data collection and use. Normative global benchmarks are needed to protect the health data commons from being deployed for neo-liberal greed and social engineering and to promote health data’s social and public value for global equity.

A GPG approach for health data cannot address these considerations unless grounded in a transversal data governance regime that encompasses personal and non-personal datasets, including those not originally generated in the context of clinical health settings.

Ongoing negotiations at the WHO to amend the International Health Regulations (2005) [present an opportunity](#) to lay the foundations for such a regime with a focus on global health equity. The IHRs can obligate countries to share health data from their national contexts for coordinated responses at the global level, with commensurate benefit-sharing measures so that communities and countries of the South are not shortchanged.

The WHO must take leadership to galvanize a new binding multilateral framework for an integrated human rights-based constitutionalism for health data. Such a framework must straddle individual and collective rights, ensure health system autonomy for all countries, and articulate the public interest norms for downstream innovations built from common pool data infrastructures.

At the national level, governments – as trustees of health data pools – must create new legal-institutional frameworks that encourage a stewardship approach to manage health data infrastructure through public-community partnerships that are respectful of individual and collective data sovereignty and committed to the health and wellbeing of the last person standing.





THE BRAZILIAN EXPERIENCE

“Protecting personal data of Brazilian people runs through class struggles”

Researcher Joyce Souza warns about the risks that the current capitalism “datafication” brings to the worsening of inequalities within societies and between countries



JOYCE SOUZA

Ph.D. student and Master in Human and Social Sciences at the Federal University of ABC. Researcher at the Free Technologies Laboratory at the Federal University of ABC (LabLivre/UFABC). Member of the Non-Aligned Technologies Movement (NATM).

A new facet of capitalist exploitation, “data colonialism,” brings the perspective that capitalism systematically attempts to make all human experiences a target for profitable extraction. “In this context, those who are online are somehow being colonized by the data generated, tracked, and processed,” underlines the Journalist, Social Scientist, and Ph.D. researcher at the Federal University of the ABC (São Paulo), Joyce Souza.

Speaker at the [Idec](#)’s event “Right to Health and Protection of Personal Data: Contemporary Challenges and Potentialities,” Joyce Souza addressed the protection of personal health data in Brazil from the conclusions of her master thesis *Personal health data and the municipality of São Caetano do Sul*, and her article [The risks of digital technologies: from farm to fork](#) - the latter produced as part of research funded by the Heinrich Böll Brasil Foundation.

For her, the class struggle must be considered in structuring a system to protect personal data of Brazilian citizens against the greed of health entrepreneurs. “In a country like Brazil, where the minimum wage is around R\$ 1,200.00 [in 2022], and the basic food parcel has reached the minimum wage, choosing whether to hand over personal data in exchange for discounts at pharmacies is not really an option”, exemplifies the Social Scientist.

Joyce Souza is also a researcher at the Free Technologies Laboratory ([LabLivre](#)), co-producer of the [Tecnopolítica](#) podcast, a member of the Non-Aligned Technologies Movement, and organizer of the book *Society of Control: Manipulation and Modulation in Digital Networks*.

CHECK OUT THE INTERVIEW SHE GAVE TO IDEC.

Idec: *For your master's thesis, you conducted field research on how pharmacies in São Caetano do Sul, in the metropolitan region of São Paulo, handle consumers' data. What were the most worrisome findings, in your opinion, that came out of your study?*

Joyce Souza: My master's research was about the purchase and sale of personal data in the [São Caetano] municipality's public and private health sectors. I ran interviews to build an organizational chart for this sector, and I realized that drugstores have a relevant part in the context, especially the large chains. Among the main elements, I highlight that pharmacies have become great personal data collectors through partnerships with insurance companies and health plan operators. To this end, they create benefits such as employee pharmacy vouchers and product discounts for customers. The data collected is passed on to partners through spreadsheets with personal information about consumers - such as the items purchased at the pharmacy, discounts granted, and payment method.

Idec: *What are the consequences of this practice?*

Joyce Souza: Some essential issues need a closer look. Among them is the topic of transparency and privacy in this business model, as the clients were unaware of how their data would be collected, stored, and shared with third parties. The issue of data security, for example - where and how data is stored, who would be the actors with access to them, and what security systems are in place to prevent data leaks, among other crucial considerations.

Idec: *You conducted your research before the enactment of the General Personal Data Protection Law (LGPD). Do you think the law provided additional protection against this practice?*

Joyce Souza: My research was carried out from February 2016 to January 2018, before the enactment of the LGPD. Much of the study took place when the debate about Brazil's General Data Protection Law began. At that time, Brazilian legislators sought to understand Europe's concern with the privacy of its citizens and how they advanced in their regulation. Brazil assessed the scenario from the economic point of view, seeking possible adjustments, if necessary, to maintain good trade relations with the European Union countries. Despite the concern with the privacy of personal and sensitive data not being the keynote in these years of my research, it is always important to underline that the health sector, regardless the LGPD, already had particular rules concerning the safety of data and information about patients. An example is the Code of Medical Ethics, which establishes the confidentiality of medical information related to the patient. That is just one of the examples of data

processing in the health field. However, the LGPD brought [principles and] restrictions beyond specific actions. The law introduces clear definitions and duties on personal data, sensitive personal data, liability within the scope of controllers and data processors, and the requirement of user consent for using their data, among many others - which pushes companies, including pharmacies, to seek adjustments to the law. Therefore, they must give transparency to what they have been doing when collecting, storing, and processing consumer data. This process is still moving slowly, and I have seen that consent is a complex issue in the context. However, it is already an essential step for us to understand what has happened in the field of data privacy and what can be done to ensure that guarantees, such as the principle of non-discrimination, are enforced.

Idec: *Regarding the use of citizens' health data by pharmacies for commercial purposes, in open or disguised association with health insurers, do you believe there are still gaps in its regulation and/or in government implementation? What are these gaps?*

Joyce Souza: I think it is essential to unveil the entire chain that comprises collecting, storing, and processing data in this sector. Knowing this chain, it will be possible to identify all the actors having access to information, how these accesses are made, what security guarantees are in place, and why specific accesses or exchanges of information and data occur, among other fundamental issues. From there, we would be able to look into the loopholes in the legislation. The National Data Protection Authority (ANPD) has been little engaged in complex situations such as leakage of personal data and sensitive personal data in the health sector. Recently, a mega data leak occurred in an extensive network of private clinical analysis laboratories, and there was no official note on the case by the ANPD. I also do not remember hearing any opinion from the ANPD regarding the collection of biometrics that a large chain of pharmacies was doing. The ANPD official stance is fundamental for advancing the LGPD in the country and, subsequently, in the health sector.

Idec: *When we look at consumer behavior, what are the mistakes that, in general, they make in their relationship with the pharmacy market and put their privacy at risk?*

Joyce Souza: I do not believe in consumers making mistakes in their pharmacy dealings. In Brazil, where the minimum wage is around R\$ 1,200.00 [US\$ 225.04, in July 2022], and the basic food basket reached the minimum wage in June of this year, choosing whether to hand over their data in exchange for phar-



The National Data Protection Authority (ANPD) has been little engaged in complex situations such as leakage of personal data and sensitive personal data in the health sector.

macy discounts is not an option. In Brazil, thinking about privacy and to whom it is guaranteed requires thinking about class relations. Therefore, it is essential that public bodies and institutions that stand for citizens' rights oversee and vehemently question the market constituted around data and discounts at pharmacies.

Idec: *During your participation in the Idec event, you spoke about the new phenomenon of “datafication of capitalist economies.” Can you explain, in general terms, what that phenomenon is?*

Joyce Souza: In the last decade, with the evolution of computational processing capacity and the consolidation of business models based on digital technologies—such as platforms capable of collecting user data from their interactions on social media—, the belief that data are key elements for understanding society and social behavior increased. In the past, metadata was considered valueless by-products; now, they are regarded as a valuable resource by companies and governments. One can extract precious information from data, thus shaping the introduction of new products, services, and social monitoring. Datafication has become an accepted paradigm in societies and is also seen as a vital form of neoliberal governance. Neoliberalism, composed of discourses, practices, and devices, has used this process to reinforce significant asymmetries and inequalities between developed and peripheral countries or between social groups within societies.

Idec: *Your work [The risks of digital technologies: from farm to fork](#) draws attention to several risks embedded in the first public notice of the Federal Government Agro 4.0 program, which aims to invest R\$4.8 million in 14 pilot projects for the adoption and dissemination of technology 4.0 in agribusiness. What are the main risks, and what intersection does this have with Health?*

Joyce Souza: The Government's focus on implementing digital technologies in Brazil is the investment in start-ups as a solution for the country's technological development. The priority for start-ups follows the guidelines of consultancies and international organizations that greatly influenced the Federal Government formulators of public notices and official documents. It is not only in the Agro sector that this framework is present; it also appears in documents such as the Brazilian Artificial Intelligence Strategy ([EBIA](#)), the Digital Transformation Strategy ([E-Digital](#)), and the [Digital Health](#) project. Data from different sectors can be correlated and present results with each other. The intersection between the Agro 4.0 and the Health sector is the nexus that data collection, processing, and classification from one sector can bring to the other. For example, if analyzed through predictive algorithms, data



Datafication has become an accepted paradigm in societies and is also seen as a vital form of neoliberal governance.

linked to the consumption of pesticides by specific populations can present results in classifying disease risks. In addition, it is worth noting that big techs (large digital technology companies), such as Amazon and Microsoft, produce solutions for agribusiness and health. In addition, they also offer solutions for storing data in the cloud, which has been widely used by start-ups operating in one sector and another. I have not developed a mapping of this entire chain to state the precise correlations between sectors; however, I believe that if we draw the organizational chart of the whole chain of digital technology companies operating from “field to fork” and in hospitals and pharmaceutical industries, we are likely to notice significant bottlenecks in the collection, processing, and use of data being done in different industries, but through the same companies, to increase their profits.

Idec: *You say that the jargon widely advertised in Brazil, “Agro is tech, Agro is pop, Agro is everything,” brings the idea that digital technologies are the only and best alternative for agribusiness to grow and maintain its competitive advantage on a global scale. What risks, in your opinion, does this bring to the population about the privacy of personal data?*

Joyce Souza: There is an ideology - and an illusion - when it comes to digital technologies. Currently, they are perceived to have a potential far beyond their actual capabilities. They are considered great saviors of society’s political, economic, or social problems. In more extreme cases, they are presented as capable of overcoming the very human being who created them and, in this way, solving the significant problems that permeate societies. Also supported by the belief of “dataism,” datafication processes have rapidly become normalized and popularized; and helped to consolidate and expand forms of surveillance, control, and social monitoring. Datafication has also been used for behavioral modulation through the processing of citizen data, allowing a more detailed analysis of their characteristics. As a result, micro-targeting strategies are created, as well as new products and services, thus accelerating the process of goods circulation.

Idec: *You also say that data colonialism implies new forms of exploitation and appropriation that result in dynamics of discrimination and inequality. Can you please develop this statement?*

Joyce Souza: The idea of data colonialism, as presented by Nick Couldry and Ulises Mejias in the book *The costs of connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (2019), brings the perspective that there is a systematic attempt from capitalism in making all human experiences a



There is an ideology - and an illusion - when it comes to digital technologies. Currently, they are perceived to have a potential far beyond their actual capabilities

target for profitable extraction. In this context, whoever is online is somehow being colonized by the generated, tracked, and processed data. Although the authors do not approach the increase in inequality that this process engenders, I see profound asymmetries between developed and peripheral nations. For example, data collected in Brazilian territory is being used to extract profit and generate value for companies from developed countries, such as Amazon, Google, Microsoft, and Apple, among others, located in the United States. Inequalities also occur between dominant economic groups and marginalized social groups, most often without respect for their fundamental rights, including data protection and privacy, as is the case in the “choice” between privacy and the provision of personal data in exchange for discounts on medicines at pharmacies.





2 HEALTHCARE SERVICES AND PERSONAL DATA PROTECTION

CLICK AND WATCH
THE EVENT VIDEO



INTRODUCTION: 2nd DAY OF EVENT



Personal data protection regimes must consider the specificities of data processing in the health field, such as the concern of commercial use of this information.

That was the consensus around which the participants of the *Health Services and Personal Data Protection* panel presented and debated during the second day of the event “Right to Health and Personal Data Protection: Contemporary Challenges and Potential.” The Brazilian Institute for Consumer Defense (Idec) promoted the international conference.

Sara Margaret Davis, lead researcher of a multi-country participatory action project on digital health and human rights, from the [Graduate Institute](#) (based in Switzerland), focused her approach on personal health data protection of vulnerable groups. These groups include youth, women, and digitally excluded or digitally illiterate communities.

The qualitative study carried out among young people from Bangladesh, Colombia, Ghana, Kenya, and Vietnam, which she released during the event, brought along some results that were as curious as they were surprising.

For example, despite having admitted “addiction” and even “dependence” on their cellphones, most of the young people interviewed also expressed concern about the need for online privacy and anonymity. They recognized their need for data security and digital rights training and expressed a desire for their clinical data to be anonymized by public health authorities.

“They are also aware of risks such as misinformation, incorrect virtual diagnoses, images shared without consent, exposure, cyberbullying, sexual or moral harassment over the Internet,” described Margaret Davis.

In South Korea, about 65% of the population agrees that only government agencies should process their health data. Furthermore, 58.2% disagree with any commercial use of the data by private companies, according to the study presented at the event by the second speaker, researcher Junho Jung from the University of Seoul.

Conducted among 1,370 participants between the ages of 19 and 64, the survey found that South Koreans generally reject the appropriation of their health data for commercial purposes. “Those who have had a hospitalization experience tend to agree more with the use of public data,” the researcher noted.

“People show that they are interested in better and easier access to their health information, but they are suspicious of protection mechanisms and the possible misuse of their data. Moreover, there is a general understanding that there must necessarily be public interest involved in handling the information,” Jung pointed out.

Mediated by the lawyer Camila Leite, lawyer of the Telecommunications and Digital Rights program at Idec, the panel also featured the presentations of the public health doctor Hêider Pinto - researcher in collective health, public policy, and digital transformation in Health at the Federal Universities of Bahia (UFBa) and the Recôncavo Baiano (UFRB) -, and Tainá Leandro, advisor to the National Supplementary Health Agency ([ANS](#) in Portuguese).

Hêider Pinto, who led the creation of the [e-SUS](#) in Brazil, highlighted that the interoperability of patients’ health records in a public network guarantees the follow-up and efficiency of care and avoids the demand for unnecessary tests. E-SUS is a standardized and interconnected system in which physicians from local hospitals and clinics can ensure patient care using the same cataloged database.

Another innovation in the area of digital health with gains for SUS users, according to the Public Health doctor, is the [Telessaúde Brasil Redes](#), launched in 2004. The system can offer primary care to inhabitants of remote locations that do not have easy access to specialized doctors.

“Covid-19 has made the expansion of this type of virtual service inevitable”, he commented –noting, however, that the speed-up of digital tools in health has brought the need to regulate and monitor the way data is processed. “Because new business models can be born out of them.”

Tainá Leandro highlighted the recent ANS initiative to anonymize all personal data in its database. “That makes it possible to know the market without identifying the beneficiaries,” explained Tainá, adding that one of the advances brought by LGPD in this area was to prevent private health plan operators from accessing the personal data of potential clients.



HEALTHCARE SYSTEMS DIGITALIZATION: THE SOUTH-KOREAN EXPERIENCE



Secondary Use of Public Health Data in Korea: Commercial Research and Public Interest



JUNHO JUNG

Researcher at the
Center for Health
and Social Change
(South Korea).

The advent of precision medicine, big data, and medical A.I. greatly increased the demand for health data from both individuals and the public. Public and private stakeholders are actively engaged in accumulating and utilizing health data. The Korean government selected biomedicine, especially health data, as one of the three areas that will drive the country's future economic growth. According to the survey, the government allocated USD 66 million in the budget for collecting and using public health data in 2021. The total national budget allocated for healthcare in 2021 was USD 250 million.

Along with the budget, there has been a significant shift in legal structure for public health data use since August 2020.

Amendment in Privacy Protection Law allowed pseudonymized data to be used without the consent from the data subject to compile statistics and scientific research. This change in the Korean legal structure is in line with the European Union General Data Protection Regulation (GDPR). In Recital 53, GDPR exempts individual consent for pseudonymized data processing for “archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.” This exemption quickly attracted many private companies interested in accessing the public health data, as they no longer needed to acquire individual consent to use the data.

One special request for accessing the public health data came from private insurance companies. They claimed that the current fee structure is derived from outdated data or foreign sources, creating an unfair burden for its clients. Their central argument is that private insurance can increase coverage with reasonable and data-driven prices once the government gathers free access to public health data. In July 2021, six private health insurance companies were granted the right to access from Health Insurance Review & Assessment Service (HIRA). Now they have access to sampled pseudonymized data from HIRA, including data on diagnosis, ICD-10 code, medical institution, admission date and duration, prescription, expenses, etc.

Two major organizations in Korea collect the majority of public health data. One is National Health Insurance Services (NHIS), and another is the NHIS branch called Health Insurance Review & Assessment Service (HIRA). Korea's health system is based on national health insurance, covering 60% of your medical expenses. Also, national insurance is mandatory for both institutions and residents. Therefore, all the data related to healthcare is gathered into NHIS. What attracts the private insurance companies is that NHIS public health data includes residents' financial status, as the national health insurance considers the income.

There has been a concern from both the medical community and the civil society that greater accessibility to public health data from private insurance companies will actually draw precisely the opposite outcome from what was promised. Based on the medical and financial status, personal insurance products will be more stratified with higher fees and eliminate high-risk groups to be insured. Also, there were concerns about inadequate secondary use of the pseudonymized data acquired by insurance companies, which are often the subsidiaries of financial conglomerates.

With this in mind, the final ruling of the data access from the Data Safety Monitoring Board in NHIS was directly opposite to one from HIRA. Internal regulation from NHIS states that public health data from NHIS can only be provided "if the research aimed for the public interest." After carefully reviewing the research proposal from the private insurance companies, the Board concluded that research was targeted for commercial interest, rather than public interest, violating the principle of minimum use. Companies quickly opposed the ruling, as the current 'Healthcare Data Utilization Guideline' from the Ministry of Health does not exclude commercial research from scientific research.

The current legal structure for secondary use of pseudonymized public health data does not clearly define what constitutes 'scientific' research, leaving the gray area for interpretation. In the case of GDPR, scientific research was exempt from the consent because the pursuit of science can achieve public interest. Thus, the European Data Protection Supervisor (EDPS) reports separate commercial from scientific research. The principle of GDPR is that free data flow should be secured, while commercial research hinders such principles through trade secrets. Also, the sensitivity and vulnerability of health data are well noted in GDPR, stating that special care and provision should be taken before processing it. In Korea, this decision is largely left up to the public institutions in charge of providing personal data.



What attracts the private insurance companies is that NHIS public health data includes residents' financial status, as the national health insurance considers the income.

For years, private insurance companies had access to sampled anonymized public health data in closed networks in both NHIS and HIRA. Now they have access to sampled pseudonymized data from HIRA, including data on diagnosis, ICD-10 code, medical institution, admission date and duration, prescription, expenses, etc. All information is provided in a closed network, only processed data can be exported, and all personal identifiers have been removed, so the risk of a data breach is relatively low. However, what private entities do with final processed data cannot be controlled. Although HIRA said that they mandate consent from researchers stating that data will not be used for commercial purposes and will be discarded after one month. However, there is no active monitoring mechanism to track such commitment, nor is there any way to sanction them after the misuse. This calls for constructing the instrument to safeguard the generating public interest from the public health dataset.

There are mixed voices in society. Civil society voiced the concern that this is a considerable step toward commercializing public health data. Some consumer groups welcomed the decision of HIRA that the provision of public data to private insurance companies can diversify the insurance product choices with reduced fees.

Meanwhile, the Doctors Association strongly opposed it, as access to public health datasets was rather exclusive to health-care professionals, but they were largely left out during these debates. The government is still pushing for the greater use of pseudonymized public health data, hoping this would vitalize the economy. Such complex interactions between stakeholders bring difficulties in striking a balance between securing public interest and protecting privacy.

The proper use of public health data can generate public interest. However, more assertive rules and regulations should assure the public good. Public health data has some characteristics of public good, as it can enhance the public's health. At the same time, individual health data is one of the most sensitive personal information. For secondary use of public health data, data processing entities should provide convincing evidence that their research can create greater public good that out-weighs the evident risk. Also, as provided in the principles of GDPR, the outcome of the shared data should be open to the public to secure the public interest.



This calls for constructing the instrument to safeguard the generating public interest from the public health dataset.



“The challenge is to have the public property generating public good,” says Korean researcher

Leader of a project that makes a critical analysis of Health digitalization in the East Asian country, Junho Jung talks about society’s perception and gaps in the regulatory framework



JUNHO JUNG

Researcher at the Center for Health and Social Change (South Korea).

In South Korea, a high percentage of the population (72.5%) are aware that private corporations access and process your personal data; at the same time, only 39.2% agree with its commercial use and 65.3% want the country to adopt higher penalties for whoever uses them improperly or without consent.

These are some of the results of the survey carried out by the Center for Health and Social Change, a non-profit organization specializing in transdisciplinary health studies. It turns out that Korean legislation aimed at protecting the population’s personal health data is still far from reflecting this desire, says biologist and medical researcher Junho Jung, from Jeonbuk National University of Korea and one of the research leaders.

Without differentiating scientific from commercial research or establishing active monitoring mechanisms on private entities that access citizens’s personal health data, Korea’s regulatory system has gaps and gray areas. “A more considerable concern should be how to generate public good with the public property rather than benefiting certain private entities. Current legislation has an ambiguity that requires better interpretation”, says Jung, who was one of the speakers at the event Right to Health and Protection of Personal Data: Contemporary Challenges and Potentialities and granted the following interview with Idec, in addition to your article.



A more considerable concern should be how to generate public good with the public property rather than benefiting certain private entities. Current legislation has an ambiguity that requires better interpretation

Idec: *The Center for Health and Social Change, where you are a researcher, has conducted an interesting survey on the perception of the South Korean population regarding the secondary use of personal health data. Did the survey results surprise you?*

Junho Jung: The overall survey result was as expected, with general disapproval for public health data commercial use, low confidence in data protection, and support for using data for the public good. What surprised us was the marked discrepancy in the perception of data usage by different entities. We did not expect that people would favor data usage by IT companies rather than insurance companies, as IT companies are known to be more prone to data breaches and data misuse and are largely unregulated. Another interesting finding was the influence of age. We expected that older people would be more reluctant to public data secondary usage. However, the 20-30 years old male age group showed significant opposition and mistrust in public data usage by any entities. Maybe this age group is more active in online data use, thereby having higher awareness about data misuse cases that lead to low confidence.

Idec: *South Korea has a relatively high rate of the population who are aware of the privacy law (61.4%) and aware of industry use of their data (72.5%). To what do you ascribe this high rate of awareness?*

Junho Jung: Since 2019, the Data 3 Law (amendment of privacy law) has been hotly debated in parliament with relatively large media coverage. That might explain the awareness of changes in privacy law. Also, recently MyData project in the finance sector, launched by our government, allowed people to use all financial data (balance, transaction, etc.) from any bank app, regardless of which bank you use. Conventionally, you had to install each bank app to check your balance or move money. These radical changes might alert people. Regarding the industry use of data, I guess there are two factors. First, personal data leakage cases. In 2012, 2014, and 2016, KT (the most prominent Korean telecom) was breached, and 8 million, 14 million, and 30 million personal data were leaked, respectively. There are many other cases of data breaches in Korea, and Korean people sarcastically say that our social security number is public property, as numerous companies have leaked it numerous times. Second, probably COVID-19 and contact tracing. During COVID-19 Korean government implemented electronic check-in for public places (restaurants, malls, museums, theatres). This QR system was primarily outsourced to private IT companies, Naver and Kakao. People also booked through this private SNS platform during the early vaccination phase. That allowed people to realize how much data these companies accumulate and utilize.

Idec: *The survey revealed that only 39.2% agree with the commercial use of personal health data, less than half (41.5%) agree on its use by insurance companies for the development of new products, about half (53.3%) agree with the use in IT for digital health, and a more significant proportion concurs with the use by Pharma (61%) and public agencies (65.6%). In your opinion, is the country's current legal framework in tune with this feeling of the population?*

Junho Jung: At the moment, data law in Korea states that “where personal information is necessary for compiling statistics, or scientific research purposes, etc., and the personal information is provided in a form by which a specific individual cannot be identified” (Article 18(2).4, [Personal Information Protection Act](#)) - effectively allowing secondary use of pseudonymized data without individual consent in scientific research. These regulation changes are in line with EU GDPR, in [Article 89](#), which exempts data processing for “archiving purposes in the public interest, scientific or historical research purposes or statistical purposes” for individual consent. However, the European Union’s GDPR explains that scientific research is in its nature for the public good and is different from commercial research. This understanding was not reflected in Korean regulation, and the health data processing guideline published by the Korean Ministry of Health explains that ‘scientific research can be regarded as any research that adopts ‘scientific methodology.’ Commercial research can also pass as scientific research. Although this was the ministry’s authoritative interpretation of the law, it was enough to encourage private insurance companies to request the use of public health data for commercial scientific research. Therefore, it is safe to say that the current legal structure in Korea has many gray areas, leaving too many gaps for varied interpretation, and misaligned with public perception.

Idec: *Regarding “how much can we use,” 64.2% agree with public agencies only, and 42% point to “no commercial use in any case.” In addition, about half (50.8%) have a negative impression of personal data use by private insurance companies. What aspects of South Korea’s current legislation need to be adjusted to reflect the public’s desire for privacy?*

Junho Jung: As mentioned above, the current legal structure has a large gray area, leaving the final decision to institutions. There are two primary organizations in Korea that collect most of the public health data. One is National Health Insurance Services (NHIS), and another is a NHIS branch called Health Insurance Review & Assessment Service (HIRA). NHIS oversees all national health and insurance data, including finance (as national health insurance is charged on our income status); HIRA deals with



It is safe to say that the current legal structure in Korea has many gray areas, leaving too many gaps for varied interpretation, and misaligned with public perception.

insurance claim data from medical institutions. In 2021, HIRA did provide some of its public data to private insurance companies, as they had no internal regulation that prevented them from giving data to private entities; also, higher law (Article 18 in PIP) allowed it. NHIS's internal code states that public health data can only be provided on the basis that proposed research aims to improve the public good. The debate is still ongoing, and the final decision on NHIS providing public data to private entities has not been set. This confusion was raised from ambiguity in legislation that defines the range and limits of scientific research. Thus further clarification on who, how, and what constitutes scientific research should be clearly stated.

Idec: *How much freedom do private health insurance companies currently have regarding access to citizens' data?*

Junho Jung: For years, private insurance companies had access to anonymized public health data in a closed network within NHIS and HIRA. Now they have access to sampled pseudonymized data from HIRA, including data on diagnosis, ICD-10 code, medical institution, admission date and duration, prescription, expenses, etc. All information is provided in a closed network with only processed data that can be exported, and all personal identifiers have been removed, so I presume that data breach is not much of a concern. However, private entities with final processed data cannot be controlled. Although HIRA said that they got the consent from the researcher, stating that data will not be used commercially and will be discarded after one month, I did not find any active monitoring mechanism to track such commitment, nor is there any way to sanction them after the misuse.

Idec: *South Koreans revealed that they want stricter conditions for the use of public data, such as the establishment of heavier penalties for possible transgressions in their treatment (65.3%), complete anonymization (55%), prohibition on use by third parties (53.6%) and even a complete ban on commercial use (46.8%). Do you believe the government is moving towards incorporating this desire into regulation?*

Junho Jung: As the Korean government sees data as a significant economic driver for the next generation, there are not many moves at the administration level towards protecting and limiting the use of public data. Instead, the government is at the forefront of encouraging the use of public data by all entities. Nor is there an active movement in parliament to amend the current legislation.



Proper use of public health data can generate public good. However, more transparent rules and regulations should secure the public interest.



South Koreans perception on data use by health insurance companies

South Koreans agree on the following secondary uses of data:

- Governmental Agencies: **65,6%**
- Pharmaceutical industry: **61%**
- Digital health techs: **53,3%**
- Health insurance companies (for product development): **41,5%**
- Marketing companies: **39,3%**

Negative
50.8%

Not sure
26.3%

Positive
22.9%

South Koreans know-ledge about the data protection law:
61,4%

South Koreans know-ledge of data use by companies:
72,5%

Under which conditions do South Koreans agree that health data can be processed?

65,3% More rigid penalties	55% Full anonymization
53,6% Use by tertiary sources should be prohibited	46,8% Complete ban on commercial use

Source: JUNG, Junho et al. A Survey of Public Attitudes on the Secondary Use of Public Health Data in Korea (2022).

Idec: *In terms of the behavior of the population, do you think that South Koreans, despite the apparent concern for privacy, usually share personal Health data on apps, websites, and commercial platforms?*

Junho Jung: In private insurance, I have to say yes. Our survey showed that people with recent hospital admission experience were more favorable to public health data use, even by private entities. Although medical treatment is covered mainly by national insurance in Korea, there is still a substantial private insurance market. Private insurance covers the medical cost not covered by federal insurance, such as more experimental/cosmetic/lifestyle medical uses. However, the private insurance claim is a little bothersome than the national one. National insurance claims are made automatically from medical institutions to HIRA, so you do not have to worry about it (most people do not even know how claims are made in the national scheme). When it comes to the private system, you have to get a doctor’s certification, bills, receipt; fax or send the photocopies through the apps. Thus, there is a consumer-side demand to simplify this process, to include easier store/transfer of medical records.

Idec: *Do you believe the research results will influence your country's government to change the regulatory framework?*

Junho Jung: That is our hope. We believe proper use of public health data can generate public good. However, more transparent rules and regulations should secure the public interest. Also, our study shows a large discrepancy in understanding the benefits and risks of using public health data. The general public is concerned with data leakages; however, the risk of a data breach is relatively small as they are only processed in a closed network. A more considerable concern should be how to generate public good with the public property rather than benefiting certain private entities. Current legislation has an ambiguity that requires better interpretation.



HEALTHCARE SYSTEMS DIGITALIZATION: THE BRAZILIAN PERSPECTIVE



Right to health, digital transformation and data protection¹



**HÊIDER AURÉLIO
PINTO**

Public Health Physician, Master and Post-Doctorate in Public Health, Doctor in Public Policy. Professor at UFBA and UFRB.



**JOSÉ SANTOS
SOUZA SANTANA**

Public Health Physician, Master and Doctoral Student in Public Health. Executive Secretary of FESF.



ARTHUR CHIORO

Public Health Physician, Doctor in Collective Health. Professor at Unifesp.

INTRODUCTION

The use of communication and information technologies (ICT) to promote innovations in health work has been associated with substantial and positive changes in the production of care, in the development of health surveillance actions, and in the management of health services and systems. The scientific literature provides evidence of these gains: health services with more clinical information about patients and greater ability to resolve their health problems; fewer unnecessary procedures (exams, referrals, etc.); higher decision sharing among professionals (which improves coordination and care quality); and optimization in the provision of health services, resulting in fewer lines and shorter waiting times.

In addition, population aging, higher rates of chronic diseases and the escalation in health expenditures have stimulated even more digital transformation processes in the healthcare area, both in the public and private sectors. The focus is on four aspects: computerization of health services and workflows; integration and information exchange between professionals and services; remote assistance; and use of artificial intelligence. These processes are recommended by multilateral organizations, such as the World Health Organization (WHO), and are simultaneously the object of market interests, as we will discuss later.

Considering this context, the discussion on digital transformation in health must be integrated, not opposed, to that of

¹ This article is part of an essay submitted to a scientific journal and born in the context of the Right to Health and Personal Data Protection seminar; it was specially adjusted for this publication.

governance and data protection. We should not have to choose between two extreme options: 1) give up data protection in exchange for digital transformation to achieve greater coverage, quality, effectiveness and efficiency in health services; or 2) forgo a necessary digital transformation in the Brazilian health system in the name of protecting citizens' data.

The debate on innovation, digital transformation and the use of data must be broad and has to involve policies on science, technology, and innovation (ST&I); health; and policies targeting the economic-social development model that Brazilian society wants. It is vital for policies and strategies building to combine: data protection and security, improvement in the health system, sustainable and inclusive economic and social development.

This essay presents a discussion anchored on studies and research that the authors developed in innovation and health technologies. Four focuses of digital transformation processes will be analyzed, seeking to point out their justifications, advances and promises, as well as the risks they can bring to data privacy and inappropriate and harmful commercial uses to citizens and consumers.



It is vital for policies and strategies building to combine: data protection and security, improvement in the health system, sustainable and inclusive economic and social development.

COMPUTERIZATION OF WORKFLOW AND HEALTH SERVICES

Brazil has more than fifty information systems in place within the public sector. These systems are essential for epidemiological and statistical analyses and for public policies' planning, including information regarding patients' records, health problems, and procedures performed. However, they do not replace the patient's medical record or organize health services, calendars and workflow. In other words, they gather important health and administrative information for the health system; still, they do not computerize the workflow, a function performed through electronic medical records and health service management systems.

Ten years ago, only 10% of family doctor teams, for example, had access to electronic medical records. As an outcome of the public electronic medical record (eSUS-AB) creation and implementation in 2013, 50% of the family doctor's teams use this system nowadays, and 20% use other electronic records; but 100% are required to feed the Primary Healthcare Information System - SISAB. Among the improvements that this implementation promoted are better clinical decision-making due to the storage of records from previous consultations, the formatting of more oriented and personal-

ized assistance, and the conditions to guarantee the follow-up in care without unnecessary or non-recommended procedures, all based on scientific evidence.

However, this process is not conflict-free and risk-free. The availability of free public medical records restricts the private medical record market; therefore, private stakeholders are not interested in having public and free tools widely implemented, nor in these solutions being developed and updated in order to be at a similar standard (or above) of the private sector's options. In addition, it is often private companies that, in practice, manage the data with low interference and governance from the public contractor. It can also lead to inappropriate practices, such as data commercialization without consent or even without public agency and citizen awareness.

INTEGRATION AND INFORMATION EXCHANGE BETWEEN PROFESSIONALS AND SERVICES

There is a paradox in the Unified Health System (SUS) when one considers the amount of information available about each individual and the possibilities of its clinical use for patient care. The lack of interoperability between systems makes it impossible to associate each person's information across different systems consistently. As a result, the clinical data generated in one medical appointment cannot be accessed for subsequent consultations, especially if consultations are held at different points in the healthcare network. This interoperability would be essential for a more adequate, effective service with less repeated and unnecessary procedures.

Several countries have been increasing interoperability between the information systems of their national healthcare systems. PAHO/WHO emphasize that this action is central to advancing quality and effectiveness and strongly recommends the creation and availability of Electronic Health Records (EHRs) with clinical data fed and consulted across the services of the care network.

In Brazil, efforts have been underway for more than 15 years. A significant milestone in the definition of SUS interoperability standards was MS Ordinance No. 2073 of 2011. Since then, the MS has maintained the goal of interoperating data, thus reaching the National Health Data Network ("RNDS", *Rede Nacional de Dados em Saúde*) in 2022. However, this has been evolving at a slow pace. In 2022, poor results are observed, far below expectations, due to the political turmoil that weakened the action of the MS, the successive replacements of ministers, and a process conducted with an interposition of interests.

Currently, interoperability boils down to Covid-19 data. There is a worrisome scenario. A hacker attack caused a data loss in the Health Ministry (MS), leading to problems for users who needed to prove vaccination through ConecteSUS online platform. Conflicts of interest between leaders of this process, who ended up working in the companies they had previously hired as public agents, were widely reported. The fact is that there is still no interoperability between the information systems of the care network to support clinical decision-making in health services, nor for managerial decisions related to the analysis of the population's health or the planning of health actions with collective impact.

In the face of slowness and disorganization at the federal level, states and municipalities have made an effort to move forward, resulting in experiences ranging from solutions that seek to allow interoperability between data from some care systems to more robust experiences, such as the Electronic Health Platform (iPeS), which aims for broad, customizable and collaborative interoperability. The latter involves state and local governments and an inter-federative institution, the Interstate Consortium for Sustainable Development of Northeast Brazil.

REMOTE ASSISTANCE

Brazil has been funding the Telehealth Program since 2007, aiming to offer continuing education to SUS health professionals and support clinical decisions with expert advice. The tool operates in services as diverse as cardiology emergencies, SAMU ambulances, and riverside health units in the Amazon. Starting from the principle that information and knowledge must circulate, not people, it proved that it could offer quality care with reduced infrastructure costs and decrease patient and professional displacement by up to 50%. In addition to optimizing resources, these alternatives make it possible to overcome the enormous shortage of expert doctors, especially in cities further away from urban centers.

However, the program had a very restrictive infra-legal regulation regarding remote, non-face-to-face health care possibilities as one of its conditioning factors. This was primarily due to resistance from professional councils, which sought, above all, job market reserve. In terms of teleservice, such resistance in Brazil and other countries changed during the Covid-19 pandemic, which made room for the intensive use of remote interaction technologies in many sectors. In this context, the National Congress authorized teleconsultation in the country and subsequently regulated it, opening space for its development in the public and private sectors.

It is also necessary to realize that the acceleration resulting from the pandemic, the international and national availability of technologies, the experience of use in other countries (and now also in Brazil), and the enormous market potential point to intense investment and exploitation by the private sector. We know that remote services generate data, including those in which citizens interact with an application. It is foreseeable that in the business model of some companies not only the use of an information and communication technology (ICT) solution or telecare service may be for sale, but also the capture of user data for uses that add value to them.

USE OF ARTIFICIAL INTELLIGENCE

The so-called new economy presupposes the massive use of data and artificial intelligence, which can generate gains in effectiveness, productivity and cost reduction in various sectors and activities.

This commitment also extends to the health sector, where three stand out pointing to a bright horizon for the use of artificial intelligence in public and private services: the use of artificial intelligence in managing the population's health; the improvement of work processes in the construction and application of protocols articulating conducts and referral criteria, contributing to equity and reduction in waiting lines; and the support for clinical decision making, with apps that can instantly suggest or discourage certain behaviours.

On the other hand, applications can also suggest or discourage conduct, and increase the indication of an unnecessary procedure, exam, or medication in the interest of those who profit from them. Or they can discourage the performance of necessary procedures for the benefit of health insurance, whose business model consists of using as few resources as possible in the face of an "event" involving an insured.

Personal data can be used to exclude or negatively select health plan users, as it projects that specific individuals will demand expenses above the average cost. They can also be used by several other sectors and companies, suggesting to grant or not of life insurance, credit, and even the hiring or not of workers, or their dismissal, from the projection of losses or lower profits for the company in question.

CONCLUSION

By providing gains in effectiveness and efficiency, the use of ICT in the promotion of innovations in the health work process is increasingly essential both for safety and improvement of the quality of care, as well as for the planning, management, and resilience of health systems.

Due to its complexity and the wide range of interests involved in the digital transformation process in health, it is vital to give centrality to the qualification and strengthening of public governance in health information systems. Likewise, it is urgent to elevate and guarantee data protection through LGPD's implementation and improvement to ensure citizens' data privacy when using healthcare services, and protection against inappropriate and harmful commercial use.

It is necessary to monitor LGPD implementation and application -and, above all, to advance the legislation on authorizations for access and use of data in the private sector. In addition, we need to build a new law that would prohibit the use of data to the detriment of the citizens, such as the practice of segmentation and adverse selection of customers, which disrespects criteria of equality and equity. Similar criterion already exists, for instance, in the financial market, with regulation that punishes privileged information used for price manipulation; as well as in the Justice system, where a lawsuit can be nullified if the evidence is improperly obtained.



It is urgent to elevate and guarantee data protection through LGPD's implementation and improvement to ensure citizens' data privacy when using healthcare services, and protection against inappropriate and harmful commercial use.

REFERENCES

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, Giliane 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, Hêider. 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, Hêider 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, Hêider 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.



Access and use of citizen Health data must respect equity and privacy

Public Health doctor, professor, and researcher Hêider Pinto defends platforms and other electronic tools to improve healthcare but points out that regulation needs to be strict



HÊIDER AURÉLIO PINTO

Public Health Physician, Master and Post-Doctorate in Public Health, Doctor in Public Policy. Professor at UFBA and UFRB.

Physician Hêider Pinto, Ph.D. in Public Policy, is an enthusiast of informatization in Health. When he held senior positions at the Ministry of Health, Pinto led the creation of tools that are now widely adopted throughout the country, such as the [e-SUS APS](#) (electronic medical records present in more than 4,000 cities), [SISAB](#) (a system of national information for primary healthcare), and [Telessaúde Brasil](#), in place since 2004, a service that has been intensively accessed since the beginning of the Covid-19 pandemic.

Professor at the medical schools of two federal universities in the State of Bahia - UFBA and UFRB - and with a post-doctorate in Innovation, Health, and Technologies in progress, Hêider Pinto believes that the recently enacted General Personal Data Protection Law ([LGPD](#)) means a step forward for Brazil. Still, the country needs to implement its executing agencies effectively. Also, the new law requires further regulation with clear boundaries and rules addressing the private sector.

“Brazil must introduce legislation that would sanction, for example, those companies that practice customer segmentation based on access to personal data and neglecting criteria such as equity and privacy to the detriment of the patient,” says the physician and researcher. He conferenced in the event *Right to Health and protection of personal data: contemporary challenges and potentialities*, by Idec, and gave the following interview.

Idec: *You were the project leader in two computerized health management tools, the e-SUS Primary Care in 2011 and the Telessaúde Brasil Redes, put in place in 2004. Do you believe that, in terms of expanding or democratizing access, has Telessaúde (that could be translated as “Digital Health”, meaning the use of ICT for remote health services) played a relevant role for populations living far away from urban areas?*

Hêider Pinto: It certainly has, and its importance became even more evident with the Covid-19 pandemic because Telessaúde allows information to circulate, instead of the person - whether that person is a patient in hard-to-reach locations (riverside communities, rural areas, or inner cities where physicians or certain specialists are not available) or the health professional himself. You can have, for instance, a specialist from the Medical School of São Paulo assisting a riverside indigenous community in the Amazon. The service expands access, allowing the remote performance of procedures that do not require an examination or the physical presence of the professional. Alternatively, it guarantees shared care between an on-site health-care professional with the patient and expert opinion at a distance.

Idec: *Does Telessaúde still work effectively nowadays?*

Hêider Pinto: It shrank a lot because there was an increase in funding and a reduction in resources for universities, which were essential partners. An 0800 telephone number (for calls free of charge) guaranteed access to Telessaúde for nurses and doctors in primary care, which has also been discontinued. So, Telessaúde is smaller today, compared to what we had in 2015.

Idec: *Did the medical associations resist Telessaúde?*

Hêider Pinto: The medical associations could not resist Telessaúde because the system did not offer “phone appointments”; it worked as consulting or inter-appointment. A professional assisted the patient on-site, and the doctor or specialist from another area, who was at a distance, spoke with him. “Telephone medical appointment,” which means to contact a patient remotely to assist them, was something the National Council of Medicine did not authorize. However, during the pandemic, phone appointment was allowed with the approval of a new law in the health emergency context. In a way, this cleared the ban that existed in Brazil - and once it was realized that phone appointments are viable and efficient in many cases, with quality care and without costs, I believe it will no longer be possible to move backward.

Idec: *Does the way Telessaúde operates, in your opinion, pose a risk of leaking patients’ personal health data?*

Hêider Pinto: There are different levels for that risk. Today doctors and other health professionals are exchanging information to serve people. In the pandemic, they

were doing it through WhatsApp. So, imagine that I can take the patient's data and be more or less careful. I can share them through WhatsApp; I can download photos on WhatsApp; I can send them to a colleague, who can pass them on to other people; I can send in a group and say, "guys, help me here with this disease; what is it?" So, today people already use it to chat; they do it without special tools. In Telessaúde, we had a pre-pandemic and pre-LGPD level with systems in which the professional placed the patient's information and received phone consulting from other professionals. With the LGPD and the recent progress in data security, we had to adapt and implement digital certification, a set of concerns around protecting user privacy. So, the Telessaúde mechanisms were adequate in a pre-LGPD context. Today it is still adapting, and at the same time, we understand that this is better than what happens spontaneously, which puts the exposure of private at higher risk.

Idec: By "spontaneously," you mean, for example, when people use apps that monitor flu symptoms, and they voluntarily enter their Health data?

Hêider Pinto: That too, but also in situations where the doctor at the clinic where you are assisted shares your data through WhatsApp with colleagues asking for opinions about your problem.

Idec: The e-SUS Primary Care (e-SUS APS) is a strategy to restructure Primary Care information at the national level. Can you briefly explain how it works and if, in your opinion, it has brought tangible benefits to users?

Hêider Pinto: It brings many benefits, and several studies prove this. The e-SUS is a public electronic medical record for the municipalities and is free of charge. It means an impressive reduction in costs because electronic medical records are expensive, from R\$ 4,000 to R\$ 5,000 per public community clinic. So, the first effect is that the mayor does not have to pay for the excellent medical record that the Ministry of Health offers. It is present in more than four thousand municipalities, which shows that it is very well accepted. Often, in the paper record the physician does not have the patient's previous information or cannot find it, and has to open a record from scratch. The medical record has the patient's entire history - chronic diseases, hypertension, diabetes, mental health, neoplasms - problems that health professionals need to monitor. If the medical record is lost, the harm to the patient is very significant, with the risk of having inadequate treatment prescribed and repeated or unnecessary tests being required. Having these comput-



Having these computerized data to ensure patient care continuity is critical. The e-SUS came to qualify care and reduce costs for municipalities; the health system must be computerized.

erized data to ensure patient care continuity is critical. The e-SUS came to qualify care and reduce costs for municipalities; the health system must be computerized.

Idec: *Is there any regulation that protects personal data collected via e-SUS so that secondary or tertiary entities do not access them?*

Hêider Pinto: Health professionals can only access the e-SUS data locally. If the patient leaves the municipality, the information is inaccessible. The National Health Data Network, the [RNDS](#), is a tool still under construction that aims to make medical records available for access anywhere in the country where the patient is. That is a challenge, sharing data nationally; but even so, the RNDS project provides access to a limited data set. RNDS is currently only sharing data related to Covid-19, feeding [ConectSUS](#) via an app.

Idec: *What level of regulation of health data protection do you think Brazil is at? What are the most worrying gaps?*

Hêider Pinto: We made much progress with the LGPD, but it needs improvement. Elements such as health surveillance data, we need to qualify them more in the LGPD. It is necessary to understand that health surveillance has a different nature, and it is the State's responsibility to guarantee the health protection of groups of people. So, specific data on a person infected can be of interest to Public Health, as we see happening in the world with the pandemic. We need the effective and efficient structuring of the National Data Protection Authority (ANPD) - that is, implementing the LGPD from the perspective of its executing agencies. Moreover, we must keep an eye on how the private sector captures data. Regulation has to impose barriers to both the inappropriate sharing of data and the non-consensual use of this data. For example, it is not acceptable that companies practice customer segmentation based on access to personal data, disregarding criteria such as equity and privacy, and harming the patient in the process.

Idec: *Brazilians are active users of social media. When it comes to health, the pandemic has spawned a flurry of apps that monitor everything, from flu symptoms to weight, including the measurement of an individual's stress levels. What risks does this wild sharing of personal data bring to citizens?*

Hêider Pinto: There are several types of risk. From the collection, via apps, of personal profile data (gender, age, weight, geographic location), to data related to previous symptoms and diseases – and, with all that data, the app controller can do several things. They can sell the data to a company interested in people with certain chronic diseases because they are more profitable from a health insurance point of view. They may sell some information about specific symptoms to pharmaceutical industry segments. That is why we need to advance in the regulation of the private

sector, establishing clear definitions of the terms of use with which users would need to agree. That cannot be left up to technology companies' compliance. Second, we need awareness campaigns informing the population, so society will have a proactive oversight behavior. Moreover, legislation should sanction those who collect and inappropriately use people's data, and also those who buy the information.



We need to advance in the regulation of the private sector, establishing clear definitions of the terms of use with which users would need to agree. That cannot be left up to technology companies' compliance.

Open health in supplementary health: pro or anti-competitive regulation? Reflections on the Brazilian market

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



FLÁVIA HARUMI RAMOS TANAKA

Assistance Monitoring Manager at the National Supplementary Health Agency (ANS). Postgraduate in Public Administration at Fundação Getúlio Vargas (FGV Rio).



TAINÁ LEANDRO

Advisor to the Director of Standards and Qualification of the National Supplementary Health Agency (ANS). Doctor and Master in Economics from the University of Brasília (UnB).

INTRODUCTION

In the face of technological advances, much has been discussed about the sharing of information between private institutions in order to encourage competition and achieve a better service, one with higher quality and more suited to the needs of clients. Some argue that it would be beneficial to replicate the experiences of the insurance and financial industry in the healthcare sector through the sharing of personal health data between different market participants.

The sharing of patient health information between healthcare providers has the potential to improve the population's health and save resources. However, allowing health plan operators to access information on the use and diagnosis of beneficiaries brings the possibility of risk selection, a practice that affects the mutualist structure with intergenerational solidarity on which the Brazilian supplementary health system is anchored. Also, it may lead to price increases for those who demand greater health care, such as the elderly and the chronically ill.

When translated to the supplementary health sector, many of the benefits disclosed in the Open Banking and Open Insurance initiatives can be achieved with regulatory designs that guarantee consumer safety but do not result in risk selection.

In this context, it is essential to point out some of the actions already developed by the National Supplementary Health Agency (ANS), such as the portability of the grace period, which was regulated in 2009. The measure brought several competitive benefits detached from the need for sharing individual data on the use of services as it was designed for the insurance and private pension sector ².

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



**FABRÍCIA GOLTARA
VASCONCELLOS
FAEDRICH**

Product Maintenance and Operation Manager at the National Supplementary Health Agency (ANS). Graduated from Universidade Estácio.

This article analyzes Open Health in supplementary health in Brazil under different aspects. Section 2 discusses the assumptions that underlie Open Insurance and Open Banking and their relationship with Open Health. Section 3 presents the legal framework governing the matter, while section 4 addresses the relationship between Open Health and the National Health Data Network (RNDS). Section 5 contextualizes market failures in supplementary health and their impact on the definition of Open Health policies. Section 6 discusses the evolution of grace period portability in health plans and the achievement of Open Health attributes by the policy implemented by the regulatory body. Finally, in the concluding remarks, the improvement in the rules of the ANS Guide to Health Plans as a design for Open Health is discussed.



**PAULO ROBERTO
VANDERLEI
REBELLO FILHO**

Director-President of the National Supplementary Health Agency (ANS). Graduated in Law from the University Center of João Pessoa (Unipê/PB).

DIFFERENCES IN THE ASSUMPTIONS OF OPEN INSURANCE AND OPEN BANKING VERSUS OPEN HEALTH

Due to technological advances and new services and functionalities from big data, it has become a relevant competitive advantage to possess substantial volumes of personal data, increasing the economic value of this information³. In this context, data sharing can foster competition between private institutions by expanding consumer choice, reducing switching costs and offering the final recipient a better service tailored to their needs⁴.

The first interoperability service in Brazil took place with Open Banking under rules established by the Central Bank in 2020, allowing customers to transit between financial institutions through the sharing of their data. Subsequently, the Superintendence of Private Insurance, SUSEP, established a governance structure for imple-

³ PONCE, Paula Pedigone. Direito à portabilidade de dados: entre a proteção de dados e a concorrência. RDC, v. 8, n. 1, p 138, 2020. Available at: <https://revista.cade.gov.br/index.php/revistadedefesadaconcorrenca/article/view/521>

⁴ The Right to Data Portability under the LGPD: Possible Regulatory Scenarios and Relevant Antitrust Implications. BAXAULLI, Nuria D.; CRISTOFARO, Giovanna. IN ATHAYDE, Amanda; MURTA, Giulia; MAIOLINO, Isabela; LIRA, Mydyã do Nascimento; ALMEIDA, Paloma Caetano. (Coord.). Mulheres no Antitruste. Volume IV. São Paulo: Singular, 2021.

menting Open Insurance for consumers of insurance services and supplementary pensions.

In both cases, the regulated entities provide highly relevant personal information – such as credit data and insurance usage. In supplementary health, however, health data – such as test results and disease diagnoses – are in the possession of health service providers, actors over whom the regulatory arm of the ANS is limited. In addition, the data protection rules established by the Federal Government define health data as sensitive. It is vital to assess how sharing personal health data affect each stakeholder: consumers, providers, and health plan operators.

BRAZILIAN LEGAL FRAMEWORK

The Federal Constitution (CRFB/88) guarantees in article 6 the right to health as a fundamental social right, under the scope of well-being and social justice. Article 196 of the Constitution enshrines the right to health as a right for all and a duty of the State, guaranteed through social and economic policies aimed at reducing the risk of diseases and injuries and equal and universal access to policies and services for its promotion, prevention, and recovery. Article 197 recognizes the public relevance of health actions and services, and allows their direct execution by the State or by the private sector, provided that the latter is under state control, inspection and regulation.

Thus, even though private entities can provide health services, this permission does not detract from their public character, and those who perform them cannot place their profit goals above the public interest in line with public policies.

CRFB/88 also honors the right to privacy and secrecy, even when not expressly related to personal data, and the Proposed Constitutional Amendment PEC 17/2019 was recently enacted. Inspired by the European regulation (General Data Protection Regulation) approved in 2018, the General Data Protection Law (LGPD) sets out rules for the collection, processing, storage, and sharing of personal data managed by organizations. The Law determines that Brazilians are the legal subjects of their data and can demand them, as well as any personal information, from contracted companies, including for sharing with competing companies.

The LGPD allows the use and sharing of personal data only with data subject's express consent and the communication of the purpose for using the information⁵. The aim is to preserve citizens' privacy and prevent undesirable commercial, social and political practices resulting from using personal data in an obscure or abusive

⁵ Art. 7º, inc. I, c/c art. 8º, § 4º.

way. However, the legislative forecast gave rise to initiatives abroad -and later in Brazil -for companies to link an incentive and actively request this type of data sharing authorization from their holders.

In the various sectors of the healthcare chain, the regulation for the use of personal information, especially data on health and consumption of medical and hospital services, presents an additional challenge: respecting the limits set by the Brazilian regulatory framework for risk selection strategies and price discrimination.

Legislators sought to prevent the health data of a given individual from being used to restrict their access to coverage or purchase of health plans or as a barrier in selection processes for jobs. It is not by chance that the LGPD prohibited, in article 11, §§ 4 and 5, the processing of personal data related to health for risk selection.

The LGPD is in line with health plan legislation. [Law No. 9,656 of 1998](#), article 14, limited operators in the sector to practice risk selection. In [Normative Precedent no 27 of 2015](#), ANS reinforces the veto to risk selection in any type of health plan contract. Moreover, [Normative Resolution No. 438 of 2018](#), art. 7, forbids price discrimination in the portability of grace periods.

Therefore, it is noted that the entire Brazilian legal framework clearly seeks to ensure the consumer's right to health guaranteed in the Brazilian Federal Constitution by prohibiting discriminatory practices that go against the welfare state.



In the various sectors of the healthcare chain, the regulation for the use of personal information, especially data on health and consumption of medical and hospital services, presents an additional challenge: respecting the limits set by the Brazilian regulatory framework for risk selection strategies and price discrimination.

OPEN HEALTH AND THE NATIONAL HEALTH DATA NETWORK (RNDS)

The sharing of patients' health records between health providers - whose tasks are focused on performing diagnoses and taking decisions on treatment protocols -, and the sharing of the same information between health plan operators (for-profit companies that price access to services health care for consumers) deserve different approaches.

In the first situation, sharing patients' health records among providers represents a great advance for the effective implementation of the Electronic Health Record (RES) in Brazil. In this regard, the RNDS, created by [Ordinance GM/MS n° 1.434 of 2020](#), aims to be the digital platform for innovation, information, and health services for the whole country, seeking to benefit users, citizens, patients, communities, managers, health professionals, and organizations.

The RNDS is a structuring project of the Federal Government's program Connect SUS. Its objective is to allow healthcare institutions, health professionals, and citizens to share health information and thus promote, with higher quality, the country's prevention and care in health. In addition, it aims to boost the care follow-up at different levels, which is fundamental for the effectiveness of health management processes and care coordination. It is considered essential for monitoring the health-disease process of patients.

In this regard, an Open Health proposal aimed at sharing health data is an indispensable factor for care efficiency and effectiveness. Ending the waste of resources is beneficial and fundamental to the sustainability of health systems. However, cost savings must come from real efficiency gains, health outcomes, and improved life quality, generating health value for patients. They cannot arise from the transfer of costs and treatment restrictions -or, even less, from the fall in the quality of care.

Currently, it is unclear to what extent the different healthcare providers record patients' clinical data, and little is heard about recording indicators of health outcomes and clinical outcomes, requiring standardization of these records as provided for in the [ESD28](#). Nowadays, data sharing systems allow a more efficient payment of health providers' networks, whether in the SUS or the supplementary health system -such as the Exchange of Information in Supplementary Health (TISS) ⁶.

Therefore, it is undeniable that the computerization and integration of health information systems can produce a quality leap in the management of the system as a whole and in the healthcare provided to the population.

On the other hand, sharing patient health data with and between health plan operators requires specific analysis. The misuse of data by operators can generate losses, not benefits, to the main interested party: the patient, the healthcare system user.

An Open Health proposal that allows the sale of customized plans (currently unallowed) and priced based on each user's history of use disregards the value delivery equation in a health care model based on integrated care throughout the life

⁶ The TISS is a mandatory standard for the electronic exchange of data on the use of medical services by the beneficiaries of the plans, among the Supplementary Health agents.

cycle, with a focus on primary care and prevention, which reduces the need to use more expensive, high-complexity services. Pricing based on low use encourages the opposite: to avoid the monthly health plan fee increase, users will start to perform fewer preventive procedures and seek care only when they are in more severe situations.

Furthermore, pricing based on the profile of health services usage disregards the entire logic of mutualism on which the supplementary health system is based, as we will see in the next section.



Sharing patient health data with and between health plan operators requires specific analysis. The misuse of data by operators can generate losses, not benefits, to the main interested party: the patient, the healthcare system user.

OPEN HEALTH IN SUPPLEMENTARY HEALTH, IN A CONTEXT OF MARKET FAILURES

The threat to the risk-sharing logic in Brazilian supplementary health, known as mutualism with intergenerational solidarity, is one of the main concerns associated with sharing healthcare personal history. By “mutualism,” it is understood that, within each age group, the benefit is the same for all users and is determined by the average risk of that group. In other words, healthier individuals (at lower risk) subsidize less healthy individuals (at higher risk) within the same age group. “Intergenerational solidarity” means that the beneficiaries of the younger age groups (at lower risk) subsidize older individuals (at higher risk)⁷.

It means that, in health plans, the costs of consultations, surgeries, hospitalizations, and other services are shared among the beneficiaries, which leads to the dilution of expenses, making them viable for all. That is a fundamental feature of the business model adopted by health plan operators. In this way, operators’ access to beneficiaries’ health data and the possibility that they make offers according to the users’ risk profile directly threaten the system’s structure.

Part of the competitive advantages commonly associated with Open Banking and Open Insurance is linked to expanding the practice known as cream-skimming, or “good risk selection.” In Open Insurance, for example, when sharing information about their insurance policy with a competitor company, consumers share their risk profile and can access better offers if perceived as low-risk clients.

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

In supplementary health, which is based on mutualism, as explained, and fraught with market failures like information asymmetry, adverse selection, and moral hazard⁸⁹, such strategies would represent undesirable regulatory outcomes. They may allow discrimination based on age and health condition when contracting health plans, which can cause damage to specific population sectors, such as the elderly and the chronically ill.

An Open Health proposal that enables such practices could increase the demand for health services in the Unified Health System (SUS), as population groups excluded from the supplementary system will have to resort to SUS for care. If Open Health regulation disregards the need to mitigate risk selection, the result will be operators in less effective competition to achieve social well-being, with limited effects on guaranteeing the offer and improving the quality of health services.

As already pointed out in section 2, the Brazilian regulatory framework was clear in prohibiting risk selection and preventing the possibility of price discrimination and access limitation. The LGPD, in turn, was evident in its intention to protect citizens by forbidding operators from processing health data with the aim to add or exclude beneficiaries.

Thus, it is up to the bodies with regulatory competence over the agents of the sector to implement a policy for sharing personal health data that will increase the benefits for consumers and foster competition between operators but also seek to reduce the possibility of risk selection and guarantee the improvement of the population's health and the sustainability of the Brazilian health system.



The threat to the risk-sharing logic in Brazilian supplementary health, known as mutualism with intergenerational solidarity, is one of the main concerns associated with sharing healthcare personal history.

OPEN HEALTH AND THE PORTABILITY OF GRACE PERIODS IN SUPPLEMENTARY HEALTH

In the last 10 to 15 years, ANS has made significant advances in topics that have

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

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

only recently begun to be outlined in the Open Insurance and Open Banking initiatives by SUSEP and BCB. In the supplementary health sector, many of the benefits disclosed in these initiatives do not require sharing individualized usage data, having been designed from the use of registration data and analysis of unidentified microdata already available on the ANS Open Data Portal.

The ANS regulated in 2009 the portability of grace periods, which was only included in phase 3 of the Open Insurance project. The rule made it possible for consumers who had already met the needs provided for by law to change their health plan without the burden of fulfilling them again in the destination plan, as long as they met specific requirements such as minimum period of stay, price compatibility between plans, payment, among others.

To facilitate portability, the Agency developed the [ANS Guide to Health Plans](#)¹⁰, which expands the consumer's ability to choose given the diversified offer of health plans in the country. The free tool provides data from the entire health plan database available. The ANS Guide has data intelligence with a direct interface with the other ANS information systems, containing information on beneficiaries, plans and operators, and offers the application of portability rules for grace periods in the tool itself. Thus, it simplifies the exercise of the right, reducing the bureaucracy of the process, and gives greater legal certainty and legitimacy to the act of portability. The user only needs to inform the CPF number and date of birth to have access to their health plan information, facilitating consultation. It is important to note that the data used in the tool must be sent by the health plan operators themselves to the ANS periodically.

In addition to presenting the complete offer of health plans in a given region, the Guide allows for identifying the composition of each plan's hospital network, which is one of the main elements for consumer decision-making when they sign up. In addition, it brings in a single document some other relevant features of the product, such as type of coverage, geographic reach and coverage area, and type of accommodation, among others.

The ANS Guide's transparency brings an essential gain to the sector, reducing information asymmetry and the performance of intermediaries, such as health plan brokers. Moreover, it benefits administrators, or the operators themselves, entities



If Open Health regulation disregards the need to mitigate risk selection, the result will be operators in less effective competition to achieve social well-being, with limited effects on guaranteeing the offer and improving the quality of health services.

¹⁰ <https://www.ans.gov.br/gpw-beneficiario/>

that invariably offer the products in which they have higher commercial interest. The Guide also allows for comparing plans from different operators, stimulating competition in the sector.

It is essential to clarify that the ANS assists the consumer by providing information but does not participate directly in the eventual acquisition or exchange of health plans. The completion of the transaction itself still depends on direct contact between the consumer and the operators involved.

Although it represents a significant advance for the market, the portability of grace periods could benefit from improvements included within the scope of Open Health in Supplementary Health. Some examples of further progress would be the possibility of simplifying the information flow between beneficiaries as well as between the operator at origin and destination; the addition of a search tool for hospital network; the inclusion of data on the qualification of operators, providers, and health care indicators; or, still, bringing information on price readjustments practiced by each operator.

CONCLUSION

The social well-being and sustainability of the sector must be the premises behind any proposal to implement Open Health in Brazil. Although it is desirable to share patient health data between professionals and health facilities for health management purposes, as provided for in the RNDS, there are no apparent benefits for consumers if health plan operators can access such sensitive information.

Suppose operators can sell cheaper health plans to lower-risk people. In that case, the result may be more expensive health plans for specific age groups - such as children and the elderly - and individuals with chronic diseases. It could lead to the exclusion of these groups from health plans and a consequent overload in the SUS. It is not by chance that the sector's legislation and regulation establish boundaries for risk selection and price discrimination strategies.

Considering that, we can conclude that an Open Health proposal based on pricing health plans according to the consumer's usage profile goes against the regulations and jeopardizes its viability.



Open Health proposal based on pricing health plans according to the consumer's usage profile goes against the regulations and jeopardizes its viability.

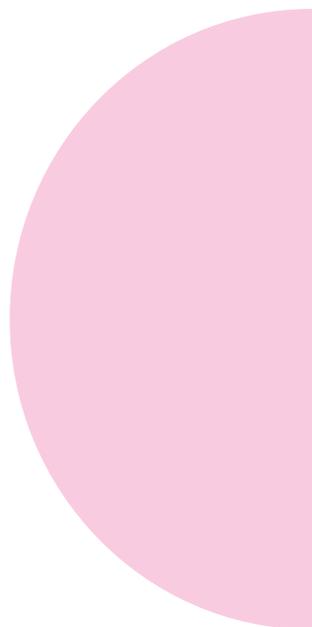
It is envisaged that improving the grace period portability can offer an Open Health that effectively encourages even more competition in the sector. In addition, it would ensure social well-being, provided that a robust impact assessment on the supplementary health market without sharing health data with Health Plan Operators will instruct it. Hopefully, soon, the ANS Plan Guide will directly exercise portability.





3 ARTIFICIAL INTELLIGENCE AND HEALTH

CLICK AND WATCH
THE EVENT VIDEO





Artificial Intelligence has evolved rapidly over the past 40 years – especially deep learning, a category of machine learning. However, society’s institutional capacity to regulate this new paradigm across the planet does not keep pace - which puts ethics at risk, especially when it comes to the intersection between the market and the human right to healthcare.

This complex, sensitive and multifaceted convergence involving technology in permanent transformation and which is at the base of the business of global giants such as Apple, Microsoft, Google, and Facebook, was the target of the *Artificial Intelligence and Health* panel discussions. The debate occurred on the third day of the event “Right to Health and protection of personal data: contemporary challenges and potential,” an international conference promoted by the Brazilian Institute for Consumer’s Defense ([Idec](#)) with the support of [Icict/Fiocruz](#) and the [South Center](#) (Switzerland) between May 17 and 19, 2022.

“Data is the oil of new Artificial Intelligence technologies,” explained speaker Daniel Dourado, physician and lawyer, professor of Medicine at the School of Health Sciences at Anhembi Morumbi University, and a researcher at [Cepedisa](#). “The processing of patient’s health data feeds high-precision Medicine, as it will indicate diagnostic and treatment actions, for example,” he explained.

The deep learning process takes place through self-taught algorithms that learn from experience and identify population behavior patterns and parameters. They run on computers with an excellent capacity for processing big data (vast amounts of data, simultaneously analyzed).

Family history, immune system, medication, alcohol and drug use, social environment, and behavioral pattern are examples of types of personal data that can yield inputs via the use of Artificial Intelligence and generate advances in health care around the world, highlighted Dourado.

However, in a context without regulation and in which ethics and transparency are weak or absent, the use of populations’ personal health data could lead to more discrimination, stigma, inequality, and more expensive access to healthcare. “An



An equity-oriented approach to AI must prevent algorithms from reproducing the logic of discrimination and prejudice.

equity-oriented approach to AI must prevent algorithms from reproducing the logic of discrimination and prejudice”, he emphasized.

In addition, the tool born from a new technology does not necessarily mean evolution, as a study by the independent Consortium AI Sur found when analyzing sixteen Latin American apps created to face the Covid-19 pandemic. The survey results were released by speaker Jamila Venturini, Journalist, Social Scientist, and executive co-director of [Derechos Digitales](#), one of the eleven organizations involved.

After studying applications designed to perform contact tracing and exposure alerting, Derechos Digitales’ researchers made several worrying findings. For example, public management over them is precarious and not evidence-based; normative frameworks, specific rules, transparency, and analysis of human rights impacts are absent; the apps do not include the implementation of monitoring, oversight, or public participation mechanisms.

“Still, in countries like Argentina, Colombia, and Uruguay, these apps had a penetration that reached 20% of the population”, pointed out Jamila. “The free access to these tools can be accompanied by opaque transactions of their users’ data,” warned the researcher. “This demonstrates that it is not enough to have an [LGPD](#) if we do not have an institutional framework capable of implementing it,” she stressed.

Lawyer Analuza Dallari, Ph.D. and Master in International and Comparative Law from USP and co-coordinator of the collective work [LGPD in Health](#), was the mediator of the panel on the third day of the event. She drew attention to the fact that AI, in addition to still lacking a universal and specific concept, is a technology in a rapid transformation that is applied to a range of segments intertwined with Health, “from Agro to robotic surgeries.”



RIGHT TO HEALTH AND PERSONAL DATA PROTECTION: CHALLENGES AND POTENTIALS



NICOLETTA DENTICO

Journalist and senior policy analyst in global health and development. Director of Médecins Sans Frontières (MSF) and leader of the Society for International Development (SID) global health program.

Covid-19 has ushered an unprecedented disruption to healthcare globally, on the twofold front of the pandemic's *direct* effects on the healthcare infrastructures and of the *indirect* effects deriving from governments' efforts aimed to mitigate the contagion.

The shift has pushed the health sector to quickly deploy tools that were confronted with [resistance before the pandemic](#), extending the analytical firepower of Big Tech players. [The Global Pandemic App Watch](#) shows that by December 2020, at least 74 countries had launched apps to automate and support established manual contact tracing. Smartphone apps were interconnected with a wider range of digital technologies, including syndromic surveillance, machine learning, natural language processing, [digital diagnostic, and genomics](#). This "[smartphone pandemic](#)" has considerably expanded governments' capacity to discipline individual behavior and citizens have now become "ever more visible to their governments, but not the other way round", as flagged by [Philip Alston in 2019](#).

While the global technological industry "remains virtually a human rights-free zone", a new focus has emerged on the downsides of this new dimension of digitalization and its potential to [exacerbate pre-existing social inequalities](#). The question is: may the tech rush injure the future of health rights? The riddle looks obviously at future pandemics. The choice between public health safety and data privacy has triggered many ethical, societal, and human rights dilemmas that lie at the watershed between the private and [public value of health and personal data](#).

Differences in the regulatory strategies for data collection and management were revealed by how governments chose to organize the digital tracing of SARS-CoV-2. Oftentimes health or health-related data derived from mobile apps and online interactions have not been used to trace contacts but to limit people's movements and monitor societal compliance with emergency rules, and more.

The criteria for announcing a national health predicament and the implementation of crisis regulations are associated with the countries' experiences of national emergencies. The Asian openness to mandated sharing of data to fight Covid-19 surely derives from previous experiences with SARS. In Europe, societies ignored massive deaths from infectious diseases before the pandemic, while the experience of fascist totalitarian rule through emergency decrees and governmental control of private lives led to the conviction that citizens shouldn't allow the government access to personal data even under a health plight. This reluctance was further stirred by the surveillance revelations of the [Snowden affair](#) and by [the Facebook-Cambridge Analytica scandal](#), which also eroded the American public's confidence in the state collecting and processing data of its citizens.

Big Tech have embedded themselves deeper within countries' health systems after Covid-19, so it will be harder to disentangle them from the new health service architecture. They seized the pandemic to increase market share and wealth, but their respite moment may have ended as Covid-19 has placed a more sensitive microscope on tech power.

If properly governed, the new availability of health data must facilitate timely and transparent decisions and communication to health systems and patients. Tensions between health and digital transformations should be resolved in favor of the core values of health and the WHO [Health for All strategy](#), the normative ground that can best advance health data solidarity for a new social contract.



If properly governed, the new availability of health data must facilitate timely and transparent decisions and communication to health systems and patients.



AI WILL BE A REVOLUTION IN SOCIETY AND MEDICINE



Researcher at Cepedisa/USP and the Institut Droit et Santé at the University of Paris, Daniel Dourado believes in the potential of Artificial Intelligence but does not accept privacy violations



DANIEL DOURADO

Physician and Sanitary Lawyer. Associate Researcher at the Sanitary Law Research Center at the University of São Paulo (Cepedisa/USP); Researcher at the Institut Droit et Santé at the Université de Paris (France). Doctoral candidate and Master (MSc) in Public Health at the Faculty of Medicine of the University of São Paulo (FMUSP).

While the debates on ethics & Artificial Intelligence are only beginning in Brazil, the spread in the use of this tool - including in Medicine - is exponential, says the physician and public health lawyer Daniel Dourado. “Algorithms will be able to enter healthcare long before we have organized ourselves for them to do so,” says Dourado, one of the *Artificial Intelligence and Health* panel participants during the third day of the Idec event.

Researcher at the Center for Studies and Research in Health Law ([Cepedisa](#)), a non-profit association linked to the University of São Paulo (USP), and at the [Institut Droit et Santé](#) from the University of Paris, Daniel Dourado is currently studying the European model of ethical regulation for Artificial Intelligence in Health. His purpose is to help shape a framework for Brazil. In this interview for Idec, the researcher emphasized that he advocates for a model that would help universalize healthcare access and bring gains to patients without violating privacy or perpetuating healthcare inequalities.

Idec: *In your speech at the event, you noted that deep learning, a category of machine learning in Artificial Intelligence, has improved very quickly in the last ten years; however, the institutional capacity to regulate this new paradigm by societies across the planet does not keep up with the pace. In your opinion, what are the main risks of this unbalance in terms of ethics regarding the Right to Health?*

Daniel Dourado: Deep learning has developed enormously in the last ten years, five years, because programmers started using big data, a massive volume of heterogeneous data processed at high speed, with the possibility of transporting and using many data. Institutional capacity cannot keep up with this. What will happen is that the algorithms will be able to enter health care long before we have organized ourselves for them to do so. Think about it; it is not a trivial thing for us to have a machine intermediating or doing an activity that human beings have been doing for centuries, such as reaching a diagnosis, a prognosis, or prescribing treatment. I do not doubt that this will happen soon; some computers are already capable of doing that. So, we will have to organize societies for this, not only in healthcare but in all areas. Because Artificial Intelligence will be like electricity, it will be a tool for almost everything, with numerous implications.

Idec: *You also mentioned in your lecture that it is through Artificial Intelligence that it is possible to develop high-performance Medicine. Could you explain what this high-performance Medicine means?*

Daniel Dourado: The algorithms will be used in clinical practice and healthcare. Moreover, they will allow the patients themselves to process their data - something that today is not easy, nor is it common to do. Today, when people feel symptoms, they use the algorithms not of machine learning but of Google, where they find something that someone wrote. When the patient uses Artificial Intelligence, they will have their data in an application - where he is on the planet, how much he walks per day, how many hours of sleep, clinical history, etc. These data will generate a response from symptoms with much more precision, closer to what he expects from medical advice.

Idec: *You just gave us an example on the patient's side. And what about the health professional side?*

Daniel Dourado: Thinking from the professional's perspective, the algorithms will significantly increase clinical efficiency: we will have much faster and more accurate diagnoses, more effective treatments (because they will be better targeted), and even the development of specific drugs and treatments for people with different charac-



The algorithms will be able to enter health care long before we have organized ourselves for them to do so.

teristics. Artificial Intelligence algorithms have already helped in the discovery of new therapies and medications because they can look at variables, formulate clinical research questions, and organize groups more effectively. So, there are several elements, several layers of algorithm use – and, of course, there will be a type of Artificial Intelligence for each of these moments. That will revolutionize our society and Medicine; it is progressing very fast, and the growth is exponential.

Idec: *What are, in general, the inputs that AI brings to this Medicine?*

Daniel Dourado: In addition to those I have already mentioned, I can add the inputs for preventive Medicine, for decision-making in public policy. Because AI will work with population data. For example, it will indicate the communities most vulnerable to a particular endemic or ecological relationship between animals and humans at risk for transmitting infectious agents. It gained importance with Covid-19 and in the discovery of the change in smallpox pattern transmitted by monkeys, just to name two recent cases. AI will bring to Public Health, to the relationship between ecology and Health, elements that will provide substrates that we do not have today, and in a speedy and very efficient way because the computer has a much greater capacity for “directed thinking” than the human brain.

Idec: *Speaking now of the risks of privacy violation, you mentioned that they could be of a deontological or consequentialist nature. Can you explain please explain that?*

Daniel Dourado: I will start with the consequentialist risks. When someone’s data is used to make algorithms, and that data leaks into the hands of another company or other people, it can harm the person whose data was leaked. For example, a person may lose their job because their employer discovered that they had a history of a particular health problem; or the health insurance finds that they tend to a specific disease and raises that person’s monthly fee. That is, the person suffers an adverse consequence due to leaked data without consent. That has to do with the idea of data privacy. From the deontological perspective (which in law means “what it should be”), it is about the fact that, even if it does not cause harm, mechanisms to protect the person must be created, as it is a moral duty of society. That is, data privacy is, in itself, a moral value that society must pursue.

Idec: *The World Health Organization establishes some ethical guidelines for the topic of Artificial Intelligence in Health. Could you explain a little what they are?*



AI will bring to Public Health, to the relationship between ecology and Health, elements that will provide substrates that we do not have today, and in a speedy and very efficient way because the computer has a much greater capacity for “directed thinking” than the human brain.

Daniel Dourado: The [WHO guide](#) is relatively recent, less than a year old. Countries still do not have rules, so the WHO put together a committee of experts and built an ethics guide for Artificial Intelligence in Health based on six principles. First of them is autonomy, the idea that the person, the human being, has the right to make decisions about themselves and not delegate those decisions to AI. The second is non-maleficence/beneficence, a principle derived from bioethics, which, in this case, points out that algorithms cannot harm people – on the contrary, they must do good. The third is transparency/explainability, the idea that the algorithm has to be understandable, at least in its general lines; there must be a mechanism of transparency understood by the human being, at least in its general logic. The fourth principle is connected to this third one; it is the principle of legal accountability of those who are manipulating the algorithm in case they use it to harm someone. The principle of equity, or inclusion, is the idea that algorithms must incorporate means of non-discrimination – they cannot discriminate people by social status, race, country, age, gender, etc. The last one is the principle of responsiveness/sustainability, which is a little more comprehensive, indicating that algorithms have to respond to society's needs and be sustainable from the point of view of the social structure. You cannot, for example, create an algorithm to eliminate jobs.

Idec: *What stage do you think Brazil is at today? Where does the country need to improve?*

Daniel Dourado: Brazil is at a very early stage. In June of this year, the National Parliament Committee ([CJUSBIA](#)) discussing Artificial Intelligence asked for an extension of its work for 120 days. They are listening to experts from other countries to understand, for example, the necessary ethical elements. However, Brazil still has no drafted law to regulate AI in Health. The discussion runs over a general AI usage law, and the Senate committee is formulating a bill that will detail and specify AI elements by sector. I think Brazil has advanced a lot in terms of privacy; LGPD is a good law inspired by European regulation. However, in practice, we are late because we took too long to implement the law. The [National Data Protection Authority](#) only started operating in 2021. So it will happen in the next few years; Brazil still has much to dig into this topic. For example, technology development companies, how will they enter the market? What will be needed for an algorithm to be usable?

Idec: *Do you believe that Artificial Intelligence can help societies achieve universal healthcare coverage for their populations? How will it happen?*

Daniel Dourado: Public health systems are recent; they have been around only since 1948. So, it is the first time in these decades that we see the possibility for health systems to reduce costs. So far, they have always incorporated technology accompanied by an increase in price. In addition, populations began to live longer, and as

a result, people use more health services for longer. Consequently, the expenditure is higher. That is a significant barrier to universal coverage, even in rich countries. With Artificial Intelligence, there is the possibility that this technology will be incorporated at a low cost. Much lower, for example, than the cost of building industry to produce a vaccine. The algorithm is inexpensive to implement, and the application is immediate, which can accelerate the possibility of increasing coverage, benefiting populations with a shortage of human health resources.



LATIN AMERICAN EXPERIENCE: THE NEED FOR PARTICIPATION AND MONITORING MECHANISMS



Public Debate Is Essential When Implementing Technologies is Naturalized in Latin America

An analysis of 16 digital applications created in the region during the pandemic revealed that the lack of participation and monitoring mechanisms put human rights and privacy at risk



JAMILA VENTURINI

Journalist and Master in Social Sciences with a focus on Education from FLACSO (Argentina). She is co-executive director at Derechos Digitales.

The digital contact-tracing tools introduced in fourteen Latin American countries to slow down the coronavirus transmission were born faulty, warns the [report](#) “A critical analysis of technologies implemented in Latin America against the pandemic,” produced by the Covid-19 Observatory of the [Al Sur Consortium](#).

“The introduction of apps as part of health emergency measures reproduced the culture that traditionally permeates public policies formulation in the region: it took place on the sidelines of scientific evidence, without prior analysis of human rights impact, and disconnected from mechanisms such as public participation, monitoring, and assessment of effectiveness,” summarizes Jamila Venturini, Brazilian journalist, social scientist and co-executive director of [Derechos Digitales](#), one of the eleven organizations responsible for the research carried out in 2020. She is also one of the authors of the report.

That trend, the study warned, explains a generally passive attitude of the States towards adopting technologies that can directly affect the exercise of the population’s fundamental rights , as well as a systematic lack of consultation with various stakeholders. “These were purely administrative decisions, even though they were applications that could have important consequences for privacy,” she points out.

In this interview with Idec, the researcher highlighted that the Latin American States’ practice of implementing technologies without a broad debate with society and the Legislative Houses to support, base, and legitimize them is perceived as natural, which she finds worrying.

Idec: What motivated the AI Sur Consortium to assess digital tools created to face the Covid-19 pandemic?

Jamila Venturini: The research was born out of great concern in Latin America about abuses related to digital rights during the pandemic. The pandemic had recently started in the region, and a trend was already observed in States approving emergency decrees with ambiguous content. In addition, agreements between states and telecommunications companies to monitor isolation measures were multiplying. They did not provide information about the limits of data sharing, either from governments to companies or companies to governments. Also, it was unclear how this mobile network connection data was being interpreted. It is worth remembering that Latin America had been turbulent since 2019, when various types of abuse were recorded during popular demonstrations in the region. For all these reasons, we decided to assess which applications were being used and the limits of that use, including the possible risk of data obtained from them being reused for different purposes.

Idec: How was the process of studying the apps?

Jamila Venturini: The first step was identifying which countries were implementing these applications. In all cases, we analyzed the applications introduced at the national level. One application per country, although some countries had more than one; the only exception being Bolivia, from where we analyzed three applications. We looked into documents and media reports about these apps; access requests were our primary mechanism for obtaining detailed information. In most cases, it was possible to get certain information through these requests; in some cases, and for certain information, we found barriers, which is also reflected in the results of our research. That information is in the public interest and should be accessible for independent and citizenship review. In some cases, technical tests were performed to identify evidence of data sharing - it was done by [InternetLab](#), for example, which identified data traffic with some companies that were not identified in the privacy policy of the Brazilian application. In the case of Ecuador, whose survey was led by Derechos Digitales, we conducted interviews with actors involved in the application development or implementation process.

Idec: A conclusion from the study concerning legality was the absence of normative frameworks or specific rules disciplining which citizens' health data would be collected, stored, and processed. Was this finding general for all countries surveyed? Are none of them a little more advanced than the others in terms of regulation?

Jamila Venturini: Some countries are ahead of others in data protection and regulation related to Telemedicine. One of these is Uruguay, which equates to the European standard. The government had a legal resolution from its Data Protection Authority

for data processing during the pandemic. In other countries, the context is uneven. Some do not have a general data protection law or specific rules that apply to the matter – which is the case of Bolivia, for example, and it was the case of Ecuador at the time of the research, as the Ecuadorian norm was approved after the study was completed. There were also countries that, despite having a data protection law, that law was not sufficiently updated for the current challenges in the digital world. That is the case in Chile, which has one of the first data protection laws in the region but has been quite out of date in terms of technological and regulatory developments since its enactment. Chile does not have, for instance, an independent data protection authority capable of overseeing the implementation of this type of application for data transactions.

Idec: *And what was the situation in Brazil in this regard?*

Jamila Venturini: Brazil was still implementing its data protection law (LGPD), and our assessed application predates it. Many countries have established exceptions to the principle of consent for processing health data during the pandemic. It is understandable and justifiable in a health emergency: data needed to be processed, accessed and shared to develop an adequate response to contain and prevent the spread of the pandemic. Furthermore, we saw and felt the challenges and consequences of not having such a policy here in Brazil. However, the big question is, what are the limits for sharing with the private sector. Because the private sector developed many of these applications, so we did not have as much transparency regarding the conditions of access and use or the reuse of this data for other purposes. Once the private sector accesses the information, it may incorporate it into other databases, and eventually, control over this processing chain is lost. Another point we call attention to when discussing legality in the implementation of technologies by the public sector is related to which actors debated each implementation. In most cases, they were purely administrative decisions, although the execution could have significant consequences for privacy. Other emergency measures, such as the case of emergency aid for citizens in Brazil, were discussed in the Legislature. Furthermore, when we think about the use of technologies by the State, it appears that there is almost a naturalization that a broader debate with other sectors of government and society is not necessary.



Once the private sector accesses the information, it may incorporate it into other databases, and eventually, control over this processing chain is lost.

Idec: *When the research report points out that there was no analysis of the impact on human rights, what exactly is it referring to?*

Jamila Venturini: Our research shows that the type of consequence and impact of these technologies on the exercise of rights goes far beyond privacy. You run the risk of discriminatory use of this data by the private sector; you run the risk of data leakage, which can even have economic consequences for people, depending on how this data is used. Moreover, in some cases, using these applications was mandatory for people who needed to move around cities. When there were periods of strict isolation and authorization for circulation was required - as was the case in Argentina, for example - these applications mediated this access. Thus, any failure in these systems could affect rights such as freedom of movement, access to work, and a host of other rights and services. So, we advocate, together with Human Rights specialists and international organizations such as the Inter-American Commission on Human Rights, for the development of a preliminary study that could foresee the types of impacts these systems can have. In other words, a comprehensive analysis of human rights. A prior assessment of implications on privacy has already been established in some countries, including Brazil, and we are proposing an evaluation of human rights impacts that would include a more holistic analysis of the technology to be implemented. The objective is to precisely identify what consequences it can bring when applied, what risks it represents, and how to mitigate those risks.

Idec: *About proportionality and necessity, it was found that the development of public policies was not evidence-based; also, there was no room for monitoring and participation. Do you think this was intentional, or could it have been the rush of the health emergency?*

Jamila Venturini: This is part of a culture of public policy-making with our backs to the evidence and without public participation. As much as our region has a broad and precious history of creating mechanisms for public consultation and participation - such as the great conferences in Brazil, for example, on Health, Human Rights, and Education - it seems that we are losing this practice in recent years. And it is almost non-existent when it comes to implementing technological tools by the State. Derechos Digitales studied several other cases of technology use that go beyond the health emergency context. In them, we see the same lack of evidence-base. This indicates a kind of blind trust in the value of technology in responding to a particular problem. So blind that it does not include a preliminary analysis of whether a given solution is really appropriate to the situation, nor a subsequent assessment of its effectiveness. There is no evaluation mechanism - neither within the public sector nor available to the population - on whether the use of a given technology was effective, whether that financial, human resources, or other expenditure was justified and deserves to be followed up, which is troublesome.

Idec: *The survey showed that the apps had significant penetration in Argentina, Colombia, and Uruguay, reaching 20% of the population. What were the implications and risks of this penetration?*

Jamila Venturini: The range was higher in these countries because some applications were mandatory. In most countries, adoption was voluntary and reached between 0.5% and 3% of the population, which is very incipient due to several factors, including digital inequalities, something that got very exposed during the pandemic. In addition to the lack of coordinated publicity of applications as a strategy to prevent and combat the coronavirus, these initiatives had low legitimacy since no one monitored the implementation. The very rhetoric that justifies these apps in some countries was so optimistic that any frustration from their use could contribute to a scenario of discrediting public institutions and scientific solutions to combat Covid-19. However, in Argentina, Colombia, and Uruguay, the application was associated with other services related to movement authorization for those coming from abroad and those transiting into the country. That is why there was a greater adherence. We also had groups of the population that were forced to monitor symptoms through these apps at times of flexibility – in the case of Uruguay, the sports sector, for example. The concern here is whether the possible malfunction of these applications or wrong results could impact the right to free movement and the right to work, among others.

Idec: *Did the study find any good practice?*

Jamila Venturini: Yes, in Uruguay, where the policy did not assume, by default, that all individuals had a cell phone, one individually available to use the app. By design, the application was provided for use by multiple users. It seems to be an interesting practice – in addition to other procedures related to accessibility, for example – because it does not assume a type of access to technology that does not necessarily represent the context of a country or a family in Latin America. It is worth mentioning that Uruguay, the country with the highest access to the Internet in Latin America, has good digital inclusion policies aimed at the young and elderly populations and pervasive e-government policies. In Brazil, the previous assumption that every person within the same family would have access to their own devices created many problems and barriers for them to getting emergency aid, such as excluding people from benefits meant to help them face the pandemic.



CONCLUSION



Since 1987, when it was created, Idec has had a duty to the Brazilian population: to fight for consumer rights in all areas where they can be impacted. Many changes have taken place over the years.

At the beginning of the Institute's activities, in 1988, the first Idec's action aimed at banning the use of DES (Diethylstilbestrol), a substance proven to be carcinogenic but widely used for fattening cattle. A colossal struggle that only came to an end in 2017 with consumers' triumph.

This is how Idec performs its work on behalf of the population. Idec will always be there no matter the time elapsed, technological changes, or transformations in the country.

With the protection of personal data in health, it is no different. A new subject, recent, but that brings issues very similar to what Brazilian consumers go through daily every year.

The Institute, with its work, wants to show that it is possible and necessary to provide public, accessible, and quality health care for all Brazilians and that this must always be done concerning privacy, freedom, and other fundamental rights and guarantees that all people own in this country.

Protecting personal data in the internet and technology era is essential to guarantee rights. Such protection must be ensured in all areas, hence the existence of this interface between the two themes. So that Idec can fight, together with the Brazilian population, for what is right, what is fair.

Health as a right, the principles that guide the SUS - universality, integrality, community participation - and the expanded idea of health itself, which inspired the creation of the system in the context of the Health Reform, offer means to deal with the new challenges of this time.



