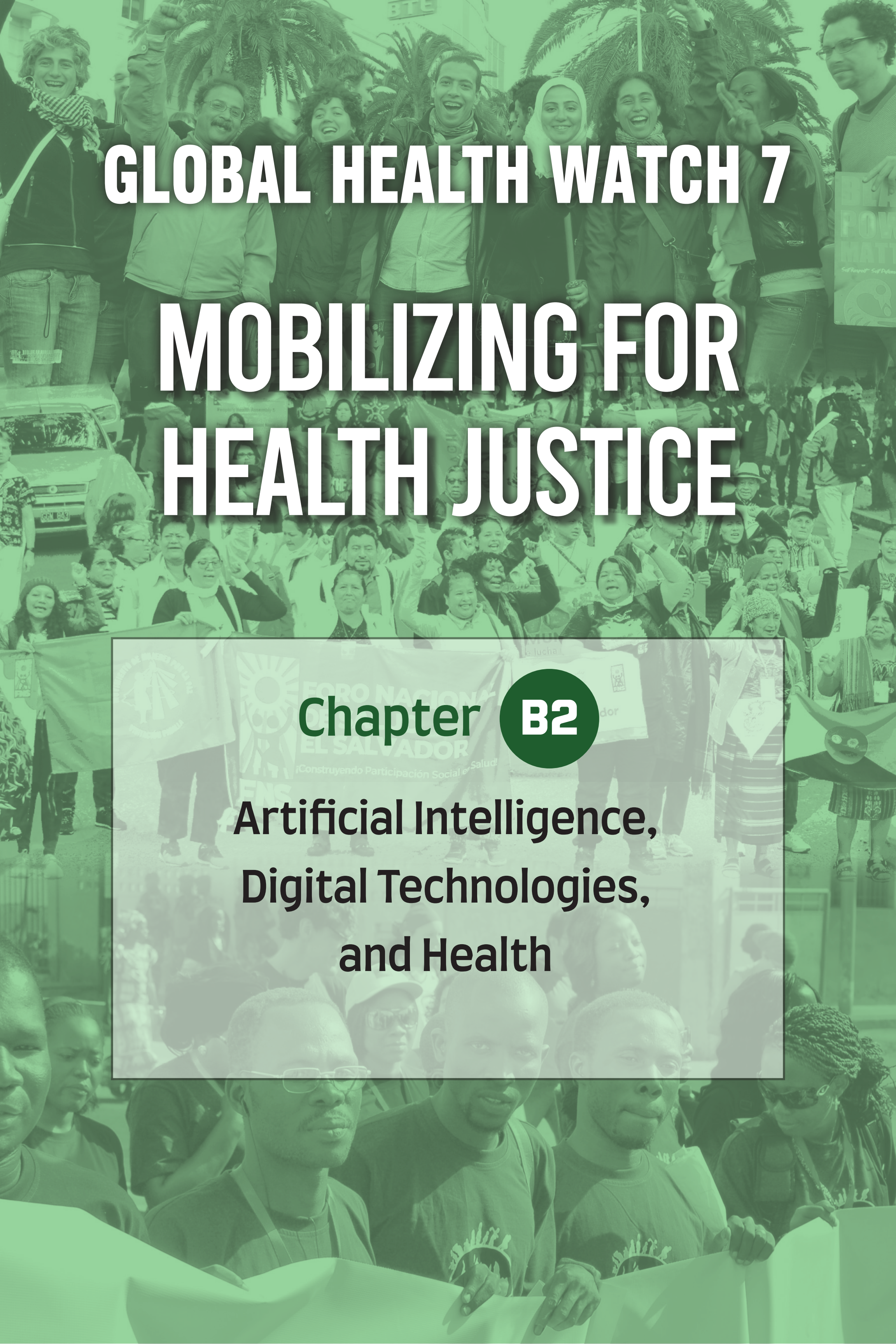


GLOBAL HEALTH WATCH 7

MOBILIZING FOR HEALTH JUSTICE

Chapter B2

Artificial Intelligence, Digital Technologies, and Health

Published by
Daraja Press
https://darajapress.com
Wakefield, Quebec, Canada

This paper will be a chapter in the forthcoming book *Mobilizing for Health Justice: Global Health Watch 7*. ISBN: 978-1-998309-48-1 (softcover)

Chapters A2 and A3 were translated from Spanish by Lila Esther Silgado Villadiego

EU Safety Information

Publisher: Daraja Press, PO BOX 99900 BM 735 664 Wakefield, QC J0X 0C2, Canada

info@darajapress.com | https://darajapress.com

EU Authorized GPSR Representative: Easy Access System Europe - Mustamäe tee 50, 10621 Tallinn, Estonia, gpsr.requests@easproject.com

For EU product safety concerns, please contact us at info@darajapress.com

Table of contents

Artificial Intelligence, Digital Technologies, and Health

Introduction

Global Health Watch 6 was the first edition to devote a chapter on digital health. Although much has since changed, the foundational concerns remain similar: digital technologies, including Artificial Intelligence (AI), need to be steered by states to protect the right to health and not increase inequalities. Concerns with mass surveillance, including of political activities, remain particularly important with the rise of autocratic regimes (see Chapter A1).

Digital health is defined by the WHO as "the field of knowledge and practice associated with the development and use of digital technologies to improve health" characterized by the interactions between communication and information technologies (ICTs) and the field of health. A commonly used earlier term, 'e-health,' was amplified and renamed digital health to include new technologies, such as robotics, genetics, and AI, with raised expectations around AI leading to more work being done with this technology (Box B2.1).[1]

Box B2.1: Understanding AI

The development of artificial intelligence (AI) began in the 1950s, with British mathematician Alan Turing laying its conceptual groundwork. Early research was heavily funded by military institutions, particularly through the US-based Advanced Research Projects Agency (ARPA), which collaborated with universities like Stanford and the Massachusetts Institute of Technology (MIT). However, funding declined in the 1970s as interest shifted to emerging technologies such as personal computers and the internet. AI research persisted and saw renewed interest in the 2000s, driven by increased computational power, large datasets and advancements in machine learning (ML), a subset of AI that allows systems to improve performance through data analysis.

AI techniques are primarily categorized into Symbolic AI and Machine Learning. Symbolic AI relies on predefined rules to perform tasks and are sometimes referred as expert systems, whereas ML enables systems to learn from data and make generalizations. The effectiveness of ML-based AI depends on three critical components: computing power, datasets and algorithms. Algorithms are the coded structure of AI models, but they require vast amounts of data to recognize patterns and create inferences. Training these models involves extensive mathematical computations, necessitating powerful computational resources. Advances in microprocessor

Continues on next page

Box B2.1 continued

technology and data collection, especially through the internet and connected devices (technically named as Internet of Things or IoT), have significantly enhanced AI capabilities, with quantum computing expected to drive future breakthroughs.

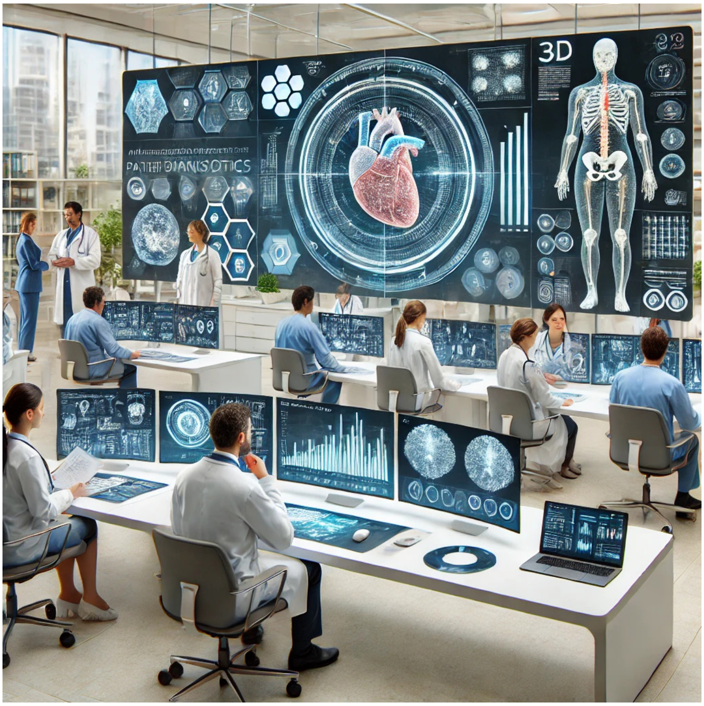
From an infrastructure standpoint, AI relies on data centers and high-performance microprocessors. Large technology firms, often referred to as GAFAM (Google, Amazon, Facebook, Apple and Microsoft), dominate data storage and processing, while advanced microchips are produced by a few manufacturers like TSMC and NVIDIA. The recent rise of Generative AI (GenAI), which can generate text, images and other media, is largely attributed to Large Language Models (LLMs). These models use deep learning techniques involving multiple computational layers to process data and generate human-like content. However, their complexity makes them difficult to interpret, raising concerns about transparency and decision-making.

The first widely adopted LLM was ChatGPT-4, launched by OpenAI in 2022. Since then, companies like Microsoft and Meta have developed their own models. Despite growing interest from startups and research institutions, foundational models remain controlled by a few major providers who, in turn, rely on even fewer for specialized hardware. As a result, the AI ecosystem is shaped by a small number of dominant players, leading to significant technical, economic and infrastructural dependencies.

Fornazin et al (2021) conducted an extensive bibliometric analysis of the waves that led to digital health, starting in the 1960s with the medical informatics field.[2] They describe five waves of the medical informatic research field, with correspondent technologies starting with the origins of medical informatics (1961-89), followed by its consolidation in the 90s with technologies such as clinical decision support systems (CDSS), picture archiving and communication systems (PACS) and telemedicine. In the first decade of the 21st century, the WHO started to actively work with digital technologies as the field of health informatics consolidated the expansion of the technology with the rise of the use of electronic health records (EHR) and Health Information Systems (HIS).

The fourth wave would come in the next decade when the concepts of electronic health (e-health) and mobile health (mHealth) gained relevance and led to the adoption of e-health strategies across countries. The end of this period was deeply impacted by the COVID-19 pandemic that broke regulatory constraints for the use of digital technologies, especially with telemedicine, and accelerated the adoption of digital solutions. The last wave, currently happening, is the digital health one, that began with the amplification of the e-health concept to include new technologies, such as the Internet of Things (IoT) and the surge of Artificial Intelligence (AI).

Figure 1: AI generated image with the prompt "AI in the near future in health care"



ChatGPT; note the racial features of all the health professionals, which reveal the bias in ML-trained AI that relies upon skewed data sets.

Potential applications of digital health and AI in health

There is a vast literature exploring potential applications of digital health and particularly AI starting with publication of WHO guidance documents on use of the technology.[3,4] As is often the case with new technologies, innovations in digital health can have great potential if steered for the public good, but also can be badly used or be part of an exaggerated technologic euphoria that aims to resolve all the problems of health systems with technologies in the name of efficiency, without properly addressing structural underlying issues. Part of the critical work developed in this chapter is acknowledging that these technologies present a set of possibilities that can be used for good if well-regulated and steered.

AI use in digital health has some benefits: improving diagnostics, increasing access and reducing waiting times are often quoted among them. Telehealth can be used to reach distant communities, particularly in rural areas, and AI could be deployed to reproduce medical knowledge in low resource settings. These benefits can emerge in different parts of health systems: healthcare, health systems management, research and development and workforce training and education.[5]

In healthcare, AI benefits include treatments that are more personalized and the possibility to reach more people with automatization of decisions and actions. In health systems management, AI can be used to operationalize procedures and increase efficiency, and for making decisions on resource allocation. GenAI can be applied to help professionals, such as doctors, with clerical tasks, scribing what patients tell them and connecting it directly with their electronic health records, and even offering possible treatment options.[6]

AI has transformative potential in the discovery of new drugs and therapies. By analyzing vast datasets, such as electronic health records, AI systems can identify novel therapeutic applications and contribute to post-market drug surveillance. At a more foundational level, AI can predict and identify molecular structures, accelerating breakthroughs in biomedical research. A notable example is the 2024 Nobel Prize in Chemistry, which highlighted AI's role in advancing basic drug research.[7] AI also has applications in training and educating healthcare professionals. It can provide interactive, adaptive learning platforms and simulations that enhance the skills of healthcare workers, ensuring they remain equipped to meet evolving challenges.

Emerging issues of concern

Personal health information

The use of digital health technologies involves handling vast amounts of personal health information that pertains to an individual's health status. This can include information on genetics, sexual behavior, consumption habits or even geolocation data, especially when combined with other datasets. Personal health information is increasingly being viewed as an extension of an individual's body, warranting the same ethical considerations and legal protections associated with human dignity. These protections are often grounded in human rights frameworks, particularly the obligation of states to refrain from violating health rights and to safeguard individuals against third-party infringements.[8] The protection of personal health information is critical due to its sensitive nature and potential for misuse, which can lead to discrimination and harm. Davis (2020) and Sekalala (2020) explored a few examples of those issues in the context of the COVID-19 pandemic, in which governments increased surveillance and partnerships with Big Tech companies.[9] Two primary concerns in this regard are cybersecurity and undue use.

Cybersecurity involves safeguarding personal health information from breaches and unauthorized access. Data breaches can have serious consequences, particularly for vulnerable populations, such as individuals with chronic illnesses or those experiencing pregnancy. The exposure of such data can lead to stigmatization, discrimination or workplace repercussions, highlighting the critical need for robust cybersecurity measures.

Undue use refers to the intentional misuse of personal health information by governments or corporations in ways that conflict with the data subject's interests and autonomy. Authoritarian regimes may repurpose health data for mass surveillance or repression. This aligns with the World Health Organization's (WHO) concept of "repurposing" where data is used for purposes other than those initially intended, often to the detriment of the individual.

On the corporate side, a common example is the denial of insurance coverage based on pre-existing health conditions. In some cases, AI systems are employed to score individuals based on health data, leading to increased premiums or outright denial of coverage. This concept of a "health score" is rooted in insurance industry practices but is now technically feasible with AI, raising concerns about exacerbating inequality. By undermining the principle of pooled risk—where resources are shared to support individuals equitably—such practices threaten the foundational ethics of insurance systems. In Brazil, health insurance companies tried to approve such a measure, which is currently expressly prohibited by the legislation in the country.

Health data is also valuable for other economy activities. Marketing is one of them. While receiving tailored advertisements may not seem as harmful as being denied care, it still constitutes an undue use of personal health information, as it often violates the individual's autonomy and personal interests. It can be used as well for research and development of new AI models. Those uses are called secondary use of data, and regulations are imperative to ensure proper protection. A survey in Korea, for example, expressed the disagreement of people on the secondary use of their own health data.[10]

AI bias

Bias is one of the main concerns with the use of AI and it can be potentially harmful in the context of health. ML-based AI applications basically reproduce what they infer from the datasets used as input to create generalizations. From a technical point of view, there are several types of bias that can affect an AI model.[11]

Data bias occurs when datasets are either unrepresentative or skewed. Unrepresentative datasets exclude a significant part of the population that will use the AI system, potentially rendering it less efficient to them. A good example is an application to detect skin cancer lesions trained on a population with lighter skin. At a broader level, populations in the Global North and high-resource settings have well-documented and accessible data, while rural populations, Indigenous communities and those in low-resource settings are often underrepresented.

The issue with skewed datasets refers to the reproduction of practices that are rooted on racism,[12] gender-based inequalities,[13] income discrimination and other forms of discrimination. Different inequities present in healthcare can be maximized by the deployment of AI.

External bias refers to factors beyond the AI system itself that influence its deployment and impact. One example is contextual bias,[14] which arises when an AI system is implemented in an environment for which it was not designed. For instance, an AI system developed in a Global North hospital to assist with treatment prescriptions might perform poorly in low-resource settings where the recommended treatments are not feasible.

AI environment impact

Another relevant impact of AI is on the environment and consequently on human societies. Many publications, including this GHW, acknowledge the impacts of climate change on human health and how this crisis is one of the main challenges faced by humanity. The reliance of AI systems, especially generative AI, on data centers is the reason for this environmental concern. Data centers consume a significant amount of energy to function and fresh water to cool down. Currently, they consume together around 6 per cent of all human-produced energy. Dhanani (2024) compiled several sources to indicate the current footprint of generative AI.[15] Increasing our reliance on a new technology that intensifies the carbon imprint can be potentially a bad choice for humans, especially if this technology is being deployed on harmful or frivolous applications. Additionally, data centers can have local impacts, such as increasing local temperatures of the air and water bodies and produce sound disturbance.

Health workforce

Digital health technologies, while useful, also carry additional risks, particularly concerning labor market dynamics. A prominent concern is the “uberization” of work, where stable, long-term employment contracts are replaced with on-demand work arrangements. In this model, platforms enable healthcare institutions, such as hospitals, to hire workers—nurses, for example—on a per-shift basis, rather than maintaining consistent employment relationships. This shift can lead to increased job insecurity, reduced benefits and lower overall remuneration for healthcare workers.

The uberization of work in healthcare is closely tied to broader trends driven by the expansion of the Big Tech industry and the financialization of healthcare services (see Chapter B1) and is already well reported in the USA with nursing work.[16] Platforms offering on-demand labor are often framed as cost-saving innovations, enabling private providers to minimize salaries and maximize profits. However, this model has significant implications for workforce stability, job quality and equity, as it prioritizes financial efficiency over the well-being of healthcare professionals (see Chapter C3). Gurumurthy et al (2022) also stress how much those platforms can be used to collect and use personal data of workers without their consent.[17]

Corporate power and commercialization

The institutional practice of quantifying actions and information is not a new phenomenon. In the field of healthcare, information has been collected and quantified for decades as a fundamental tool for developing public policies in the sector and advancing health science. However, with the advancement of digital technologies this landscape intensifies and transforms into a crucial asset for market concentration and corporate power.[18]

The debate about the exponential collection and quantification of data involves, on one hand, perspectives that argue that quantified data can solve problems previously deemed insurmountable by humanity and, therefore, should grow and become central to public policies and business model development. Others point out how this quantification is primarily an approach beneficial to corporate power that transforms such data into profitable assets.

This process, known as datafication, has advanced in the healthcare sector due to a strong belief in the potential of big data technologies in providing economic benefits, such as better pricing and cost reductions, as well as social advantages, like expanded healthcare access, reduced waiting times and predictive analyses for prevention, among others. The enthusiasm for these benefits is reflected as a central element in discussions and actions aimed at developing a global digital health ecosystem. Organizations and institutions in the sector, such as the WHO, have emphasized that the use of data-driven technologies is crucial to achieving the United Nations' Sustainable Development Goals. Since 2005, the WHO has promoted strategies to transform healthcare into a global digital ecosystem, grounded in guidelines and recommendations for implementing digital technologies in the sector, as well as encouraging the sharing of health data across various levels.

To implement these strategies, governments have turned to private companies which take on the responsibility of collecting, storing and processing health data, particularly during COVID-19 pandemic, as showed by Storeng (2021).[19] These Big Tech corporations, which are mostly based in economically powerful countries, operate in a monopolistic manner, concentrating and controlling digital infrastructures and technologies that are essential not only to healthcare but to various areas of social life. This control extends from transoceanic optical cables through which digital data flows; to data centers responsible for storing and processing this data; to Internet Service Providers which can monitor and conduct behavioral surveillance; and finally, to digital platforms which facilitate user interactions and collect large volumes of real-time data, including data used in the development of AI models. Through the extraction and analysis of information derived from the vast amounts of data they store, these corporations gain deep insights into individuals, enabling them to influence and shape behaviors using algorithmic systems to determine how users interact, with whom, and in which environments within their platforms. Alphabet, the parent company of Google, and AWS, from Amazon, are representative examples of this dominance, operating across all layers of this digital ecosystem.

In a system where data has become a crucial input for business development and profit growth, large corporations have recognized that digital platforms serve as the essential virtual space to drive their socio-economic activities. A clear example of this is social media platforms—private virtual spaces where users must adhere to established rules, including consenting to the use of data generated by their interactions, whether public or through private messages. This data feeds into the business models of these corporations, which can range from marketing strategies to the development of AI systems and other products or services.

Some platforms also provide infrastructure for data storage and processing, a service known as cloud computing, which plays a central role in the digitization of economic, political and social spheres. Given the growing volume of digital interactions and the massive collection of digital traces, these platforms have become yet another highly profitable service in the business models of Big Tech companies. In the healthcare sector, the impact of this market is evident in both the Global North and South.

One of the main consequences of this scenario is the almost unprecedented power these companies wield, allowing them to use the collected data for their own purposes, reaching into strategic engagement with political and legislative classes in the countries where they operate and shaping regulations that often favor their corporate interests. An example of this is the intense lobbying activities of companies like Meta (the owner of Facebook and Instagram) and Alphabet (the owner of Google) in the United States and the European Union to undermine data regulation proposals, such as the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR). In countries in the Global South, such as Brazil, the impact is even more pronounced, as governments often rely on these companies for technological infrastructure, which reinforces power inequalities and complicates the oversight of their practices. Most recently the role of US Big Tech in financing or promoting the 2024 election of Donald Trump is one side of this coin; the other is how Big Tech can be coopted by political leaders such as Trump to serve their personal political interests.*

In the healthcare sector, this issue is reflected in how states are becoming clients and funders of Big Tech business models, often in an uncritical manner. Instead of investing in their own public digital infrastructures and platforms, they come to rely on solutions provided by these private companies, compromising technological sovereignty and becoming vulnerable to digital monopolies. Three examples illustrate this dynamic: the digitalization of social care in Denmark, that created lock-in situations with private providers,[20] the partnership between Google Cloud and the National Health Service (NHS) in the UK and the collaboration between AWS Cloud and the Unified Health System (SUS) in Brazil.[21] In the case of the NHS in the UK, the transfer of sensitive health data to the US company Palantir raises concerns about privacy and the ethical management of data. In Brazil, the Unified Health System (SUS) uses Amazon's services to

*The front-row presence during the inauguration of Donald Trump's second presidency (20 January 2025) of the US 'tech bros', the CEOs of the world's largest technology corporations and the world's richest men, was a striking image of the unhealthy link between political, financial and technology power.

host the National Health Data Network (RNDS), the country's primary system for health data interoperability. These political choices strengthen dependence on foreign actors and can limit governments' ability to ensure the security, control and public use of this data for social rather than commercial purposes.

Figure 2: Campaigners in the UK against Palantir involvement in the NHS

Talia Woodin/Medact

With all this power, these companies not only dominate the present but also shape the future through predictive analyses often presented as infallible yet rarely questioned due to the lack of studies on potential errors and the consequences of this scenario. Furthermore, the innovation environment is strongly influenced by data-driven technologies, such as AI, which advance mainly thanks to the resources and infrastructure these companies possess. The monopoly in the field of innovation tends not only to be maintained but also to be expanded.

It is also important to understand this scenario in relation to computational power, particularly the significance of microprocessors, which represent the physical dimension of digital technological innovation. These components, mainly made of silicon, are essential for the calculations performed by computers and digital devices. The control of this production is concentrated in a small number of companies on the global stage, following the monopolistic logic of Big Techs. Other essential infrastructures, such as microchips, also follow the monopolistic logic of these corporations.

The global arena of digital health

The digital transformation of health has led to different initiatives worldwide to provide guidance and steer the adoption of digital technologies in healthcare. This section explores the main actors in the global arena, which are international organizations working with digital health, and legal trends in terms of regulation that are influencing the way jurisdictions deal with the topic.

Global actors

In terms of international organizations, the WHO in partnership with the International Telecommunications Union has been publishing guidance documents to help countries adopt technologies, especially AI. The most important document is the Global Digital Health Strategy 2020–25, recently extended to 2027. This strategy defines general principles for digital health and encourages a lot the participation with the private sector.

Another organization that has played a major role internationally is the Organization for Economic Co-operation and Development (OECD), which has led different initiatives to discuss and influence the adoption of AI in healthcare. Other initiatives aim to influence countries to implement and harmonize their regulation on digital health, for example, the Global Partnership for AI, an OECD-fostered organization to bring together countries and academics. The nature of digital health also invites activists to understand further the dimensions of internet governance.[22] New technologies have also influenced the adoption of legal frameworks that, although different at each jurisdiction, get their inspiration from international standardized frameworks, discussed below.

Legal trends

The regulation of privacy and personal data protection was the first major international regulatory response to the challenges of the digital economy. The European Union's General Data Protection Regulation (GDPR) has become a global benchmark, inspiring similar laws in various jurisdictions to promote transparency, accountability and greater individual control over personal data.* An important exception to this trend is the United States, which lacks a comprehensive federal data protection law. Its Health Insurance Portability and Accountability Act, approved in 1996, does not meet the needs of the digital economy, creating concerns about use of health data by US-based companies.

Despite the widespread adoption of data protection regulations, significant limitations persist. In some regions, efforts to enact robust data protection laws have stalled. For instance, India's attempts to pass a comprehensive data protection law, including rights for data subjects and community protections, have not succeeded, leaving a regulatory gap in one of the world's largest digital markets.

Even where such laws are enacted, enforcement remains inconsistent. Brazil's data protection legislation, for example, has faced implementation challenges due to limited resources for regulatory agencies and difficulties in ensuring compliance across sectors.

Beyond enforcement challenges, a fundamental critique of existing data protection frameworks is their predominantly individualistic approach. As Anita Gurumurthy (2024) has pointed out, this perspective often fails to account for the

*The GDPR is not without some problems. As Chapter E2 discusses, it has been used to launch court cases against environmental activist organizations (so-called 'SLAPP' injunctions, or 'strategic lawsuit against public participation').

collective dimensions of data and its broader societal implications.[23] The digital economy does not extract value from individual data points alone but rather from aggregated datasets, yet current regulations do not adequately address this reality.

While data protection laws focus on the handling of personal data, AI regulation primarily concerns the outputs of AI systems—that is, when and how they can be deployed. AI regulatory models can be classified based on their scope (general vs. sectoral) and their foundation (rights-based vs. risk-based). At the general level, there is ongoing debate about regulating AI comprehensively through broad legislative frameworks such as the EU AI Act, which was approved by the European Parliament in 2024. Several other countries are currently considering their own AI legislation.

In contrast, sector-specific regulation focuses on particular domains where AI applications have significant impact. One prominent example is the regulation of Software as a Medical Device (SaMD)—software applications used in clinical care, which must meet safety and efficacy standards similar to those governing medicines and vaccines. Since 2021, regulatory agencies have been exploring ways to oversee AI-powered SaMD, particularly those using machine learning. The challenge lies in regulating “unfixed” AI-based applications that continuously evolve as they learn from new data. For products requiring market approval, this poses difficulties, as their safety and efficacy must be reassessed over time. Moreover, sector-specific regulations have inherent limitations. In the case of medical AI, regulations primarily focus on clinical care applications, excluding other critical AI-driven areas such as public health management, research and development and administrative decision-making.

Speaking of rights-based vs risk-based regulatory approaches, while these concepts are not always strictly defined and often overlap, they represent distinct philosophies of governance. Rights-based regulation takes fundamental rights as its starting point, ensuring that AI systems do not infringe upon individual or collective rights. Under this model, companies must design AI systems in a way that respects legal and ethical principles from the outset, whereas risk-based regulation focuses on identifying and mitigating specific risks associated with AI applications. This approach assesses AI systems based on the potential harm they could cause and develops safeguards accordingly. One example is the International Medical Device Regulators Forum (IMDRF), a regulatory authority-based organization, with participation of the medical device industry in their working groups, working to create uniform standards for AI-enabled SaMD.

Political economy approach to digital health

A few new theoretical approaches have emerged in scholarship and across civil society movements to proper diagnose the emerging issues around digital health, especially to address it from a political economy point of view. One of these concerns data colonialism. Data has become a critical resource, akin to a new form of raw material. Countries in the Global North, with greater access to data, proprietary regimes and infrastructure, are consolidating their dominance, creating a new form of colonialism, in which low-resource nations remain dependent on more powerful, technologically advanced states that are the global centers of AI technology and development. This represents an extension of economic colonialism in which the periphery keeps participating in the world economy by providing raw material, in this instance data. Khauja (2024) illustrates this process as primitive accumulation of data, in the same mode of the Marxist concept of primitive accumulation of capital.[24]

Another theoretical approach rooted on the colonial structural is digital colonialism, in which the Global North controls which technologies are being deployed and used in the South, in spite of its needs (see Chapter B5). Sekalala and Chatikobo (2024) highlight this point by addressing the colonialism in the digital health agenda, that often disregards local context and approaches technology as a magic wand.[25] This is aggravated by the increasing power of Big Tech companies over states.

A third theoretical concept developed to address this complexity from the perspective of states is that of ”platformization”, which describes the process of digitizing public services inspired by practices common in the private sector. In this context, new forms of mediation are introduced that connect the different stages of service provision, as well as the transfer of parts of their implementation to private companies, often through contracts established with public authorities. This phenomenon is based on the large-scale collection of population data, the transformation of citizens into consumers and the privatization of state infrastructures as a means of generating financial revenue. The adoption of business-oriented methods by the state is not a recent process and traces back to initiatives driven by the logic of the managerial state. However, platformization incorporates innovations from private digital platforms, reflecting a new stage in this process of imitating corporate practices.[26,27]

Another interesting approach is the claiming of digital sovereignty. The word sovereignty can be polysemic, especially as it is used more frequently in the public debate. Rikap et al (2024) in their manifesto reclaiming digital sovereignty enunciated a few actions that could help to protect people from corporate power.[28]

Gurumurthy and Chami[29,30] propose a feminist and critical approach to understanding the implications of menstrual apps and data collection. Their research highlights how existing legal frameworks for personal data protection, which are rooted in an individualistic perspective, fail to adequately address the expansive reach of digital capitalism. This critique aligns with political economy theories of the digital economy, particularly Shoshana Zuboff’s concept of surveillance capitalism which emphasizes the extraction and commodification of behavioral data to generate predictive inferences.[31] Additionally, it resonates with Cecilia Rikap’s (2021) more recent analysis of data-driven intellectual monopolies, which explores how dominant tech corporations leverage data control to consolidate intellectual and economic power.[32] Together, these perspectives underscore the limitations of current data governance models and the need for alternative collective approaches to data regulation.

Opportunities

Beyond theoretical perspectives for diagnosing the current landscape, it is essential to explore concrete actions that can drive change in the political governance of digital health. One key avenue for intervention is leveraging legal frameworks to shape the regulatory environment, in both lawmaking processes and through court and administrative litigation.

With the rapid advancement of AI there is an ongoing and intense debate over its regulation, reminiscent of the discussions that took place a few years ago around personal data protection laws. Similarly, digital health is now at the center of regulatory discussions, particularly regarding the development of digital health platforms, data infrastructures and governance models. This presents a critical opportunity to engage with these policy debates and advocate for equitable, transparent and rights-based digital health regulations.

At the same time, existing legal frameworks, such as those designed to protect privacy and personal data, remain relatively new and underutilized by civil society organizations. These frameworks offer opportunities for public interest litigation, strategic advocacy and legal interventions to ensure greater accountability and fairness in digital health governance. Furthermore, legal mechanisms that are not explicitly designed for digital health—such as benefit-sharing agreements—can be creatively repurposed to promote more equitable outcomes.

The benefit-sharing approach, established under the Nagoya Protocol and effectively implemented in the Pandemic Influenza Preparedness Framework (see Chapter D2), could serve as a model for data governance and innovation in digital health. Applying benefit-sharing principles to the processing and use of health data could help redistribute the economic and technological gains derived from digital health assets, ensuring that communities and stakeholders—rather than just private corporations—benefit from innovation.

Finally, an important recommendation for social movements and governments, particularly at the local level, is to invest in digital literacy and information technology capacity-building. Much of the corporate dominance in digital health stems from states losing their technological and regulatory capacity to private companies. Strengthening public-sector expertise in data governance, AI and digital infrastructure management is essential for reclaiming agency and ensuring that digital health ecosystems serve the public interest rather than being driven solely by commercial imperatives.

Reference List

1 World Health Assembly. WHA 71.7 Digital health. Geneva: World Health Organization; 2018 [cited 2024 Dec 15]. Available from: https://bit.ly/3TeMucL

2 Fornazin M, Penteado BE, de Castro LC, de Castro Silva SL. From Medical Informatics to Digital Health: A Bibliometric Analysis of the Research Field. In AMCIS 2021 Aug (pp. 18-18).

3 World Health Organization. Global strategy on digital health 2020-2025. Geneva: World Health Organization; 2021. License: CC BY-NC-SA 3.0 IGO; World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. [S.l.]: WHO; 2021 [cited 2024 Dec 15]. Available from: https://bit.ly/3RGwaRC

4 World Health Organization. Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models. [S.l.]: WHO; 2024 [cited 2024 Dec 15]. Available from: https://bit.ly/44ckw8t

5 World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. [S.l.]: WHO; 2021 [cited 2024 Dec 15]. Available from: https://bit.ly/3HzHGw7.

6 World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. [S.l.]: WHO; 2021 [cited 2024 Dec 15]. Available from: https://bit.ly/3HtKo6x.

7 Abriata LA. The Nobel Prize in Chemistry: past, present, and future of AI in biology. Commun Bio. 2024 Oct 29;7(1):1409. Available from: https://bit.ly/4jMTJ6O

8 Mofokeng T. Digital innovation, technologies and the right to health. United Nations Human Rights Council; 2023 Apr 21 [cited 2025 Mar 8]. Report No.: A/HRC/53/65. Available from: https://bit.ly/45gyCWU

9 Davis SL. The trojan horse: Digital health, human rights, and global health governance. Health Hum Rights. 2020 Dec;22(2):41; Sekalala S, Dagron S, Forman L, Meier BM. Analyzing the human rights impact of increased digital public health surveillance during the COVID-19 crisis. Health Hum Rights. 2020 Dec;22(2):7.

10 Jung J, Kim H, Lee SH, Park J. Survey of Public Attitudes Toward the Secondary Use of Public Healthcare Data in Korea. Healthc Inform Res. 2023 Oct 31; 29(4):377-85. Available from: https://bit.ly/3Fw7JUv

11 Obermeyer Z, Nissan R, Stern M, Eaneff S, Bembeneck EJ, Mullainathan S. Algorithmic bias playbook. Center for Applied AI at Chicago Booth; 2021 Jun. Available from: https://bit.ly/43YP7ER

12 Hussain SA, Bresnahan M, Zhuang J. The bias algorithm: how AI in healthcare exacerbates ethnic and racial disparities–a scoping review. Ethnicity & Health. 2025 Feb 17;30(2):197-214. Available from: https://bit.ly/3TgQmtS

13 Lau PL. AI gender biases in women's healthcare: Perspectives from the United Kingdom and the European legal space. In: Gill-Pedro E, Moberg A, editors. YSEC Yearbook of Socio-Economic Constitutions 2023. Cham: Springer Nature Switzerland; 2024. P.247-74. Available from: https://bit.ly/4kzo6yA

14 Price II, N. Medical AI and contextual bias. Harv. JL & Tech. 2019;33(1):65-116.

15 Dhanani R. Environmental impact of generative AI – 20 stats & facts [Internet]. The Sustainable Agency; 2024 Sep 27. Available from: https://bit.ly/4jMauiz

16 Wells KJ, Spilda FU. Uber for nursing: how an AI-powered gig model is threatening health care. Roosevelt Institute; 2024 Dec 17 [cited 2025 Mar 8]. Available from: https://bit.ly/3SJpjHp

17 Gurumurthy A, Chami N, Chatterjee S, Shah S. Workers' data rights in the platformized workplace: a new frontier for the labor agenda. IT for Change; 2022 Jun [cited 2025 Mar 8]. Available from: https://bit.ly/43XPcIQ

18 Viljoen S. A relational theory of data governance. The Yale Law Journal. 2021 Nov; 131(2): 370-81. Available from: https://bit.ly/4mVpHjX

19 Storeng KT, de Bengy Puyvallée A. The Smartphone Pandemic: How Big Tech and public health authorities partner in the digital response to Covid-19. Global Public Health. 2021 Sep 2;16(8-9):1482-98. Available from: https://bit.ly/3ZkeC1S

20 Collington R. Disrupting the welfare state? Digitalisation and the retrenchment of public sector capacity. New Political Economy. 2022 Mar 4;27(2):312-28. Available from: https://bit.ly/4kzgrjZ

21 Rachid R, Fornazin M, Castro L, Gonçalves LH, Penteado BE. Digital health and the platformization of the Brazilian Government. Science & Collective Health. 2023 Jul;28(7):2143-53. Available from: https://bit.ly/43A2uw7.

22 Kurbalija J. An introduction to internet governance. Geneva, Switzerland. DiploFoundation; 2016 Nov 8.

23 Gurumurthy A. Towards Feminist Futures in the Platform Economy: Four Stories from India. Epistemic Rights in the Era of Digital Disruption. 2024 [cited 2025 Mar 10]. P.113-26.; Available from: https://bit.ly/4dSs1nD

24 Khauaja P. Dependência e Soberania nas Tecnologias de Inteligência Artificial: uma análise a partir dos conceitos de acumulação primitiva de dados e Data Processing Inequality. Liinc Rev. 2024 Dec 3;20(2). Available from: https://bit.ly/3HygGNG

25 Sekalala S, Chatikobo T. Colonialism in the new digital health agenda. BMJ global health. 2024 Feb 1;9(2):e014131. Available from: https://bit.ly/4dSs2rH

26 Rachid R, Fornazin M. From the UK to Brazil: digital health and the platformization of public health systems [Internet]. Society for Social Studies of Science; 2024 Feb 19 [cited 2025 Mar 9]. Available from: https://bit.ly/4jUVb7q

27 Rachid, R; Fornazin, M.; Castro, L.; Gonçalves, L.; Penteado, B.. Digital health and the platformization of the Brazilian Government. Science & Collective Health. 2023 Jul;28(7):2143-53. Available from: https://bit.ly/42BNo8Q

28 Rikap C, Durand C, Paraná E, Gerbaudo P, Marx P. Reclaiming Digital Sovereignty: A roadmap to build a digital stack for people and the planet. 2024 Dec 3. Available from: https://bit.ly/4e1lwiI

29 Gurumurthy A, Chami N. Beyond data bodies: New directions for a feminist theory of data sovereignty. SSRN Journal [Internet]. 2023 [cited 2025 Mar 28]; Available from: https://bit.ly/43ClYQT

30 Gurumurthy A. Towards Feminist Futures in the Platform Economy: Four Stories from India. Epistemic Rights in the Era of Digital Disruption. 2024 [cited 2025 Mar 10]. P.113-26. Available from: https://bit.ly/3GLWyqE

31 Zuboff S. Surveillance capitalism and the challenge of collective action. New Labor Forum. 2019 Jan;28(1):10-29. Available from: https://doi.org/10.1177/1095796018819461

32 Rikap C. Capitalism, Power and Innovation: Intellectual Monopoly Capitalism Uncovered. London: Routledge; 2021. 295 p.