Digital Health Sovereignty: An International Legal Study on the Right of States to Protect Their Health Data from External

Exploitation and Building a Global Digital Health Justice System

By Dr. Mohamed Kamal Arafa Elrakhawi, Independent Researcher, Legal Consultant, and International Lecturer in Law

DOI: 10.5281/zenodo.21806640

Preface

We live in a world witnessing an unprecedented acceleration in the digital transformation of the health sector. Health data is no longer merely clinical information. It has become a strategic commodity traded in global markets. While major technology companies possess databases of genetic data belonging to hundreds of millions of human beings, developing countries lack even the minimum protection for their citizens' data. This stark disparity reveals a fundamental flaw in the international legal system: the absence of the concept of Digital Health Sovereignty.

This work does not aim to repeat the traditional discourses of health law. It aims, rather, to build a new international digital legal theory that makes Digital Health Sovereignty not a slogan but an enforceable principle. It combines precise jurisprudential analysis, deep legislative comparisons, and the study of real cases to present a practical solution that can be adopted in international forums, taught in the greatest universities, and relied upon in national and international courts.

This research has been built upon a simple but foundational principle: health data is not a commodity belonging to companies. It is part of national security. And without digital health sovereignty, there can be no genuine health justice in the digital age.

And with God lies all guidance and success.

Chapter One: Digital Health Sovereignty, From Privacy to the International Legal Principle

The concept of health sovereignty is no longer confined to hospital management or drug provision. It has extended to encompass the capacity to protect the digital systems that manage national health data. Digital Health Sovereignty is not merely the use of technology in health supervision. It is, rather, a fundamental redefinition of the state's relationship with health data, founded on the principle that technology must be a tool for protecting the system, not for exploiting it.

This work defines Digital Health Sovereignty as the exclusive right of the state to regulate and protect the digital systems that manage its health data, and to prevent any external digital

domination that threatens its health security or imposes upon it an unwanted digital dependence. This right does not mean health isolation but the practice of sovereignty in a digital environment that crosses borders.

This concept began taking practical shape. In 2024, a European country launched a national digital health platform for collecting genetic data directly from citizens. In 2025, the United Nations developed a smart system that links all health justice mechanisms in a single interactive platform. In developing countries, however, total reliance on foreign digital health platforms makes them vulnerable to health exploitation or sudden disruption.

This chapter affirms that Digital Health Sovereignty is not a technical luxury but an existential guarantee for modern health justice, and that its absence in international health law creates a dangerous vacuum that threatens the stability of the health system itself.

Chapter Two: The International Legal Vacuum in Protecting Citizens from Digital Health Exploitation

Despite the importance of health justice, international health law still lacks a comprehensive convention that protects the rights of citizens in obtaining digital health justice. The fundamental Rome conventions, despite recognizing the principle of protecting citizens, include no mechanisms for their protection from digital health crimes.

This vacuum is not the result of oversight but a reflection of the conflict of interests between nations that see the health crisis as an individual event and those that see it as a collective threat. At the Conference of States Parties to the Rome Statute in 2025, the Declaration of Digital Health Justice was adopted, but it contented itself with voluntary cooperation without any legal commitment to protecting citizens in cyberspace. The Office of the Prosecutor at the International Criminal Court has no strategy for digital transformation that includes any mechanism for protecting digital rights of citizens.

In judicial forums, the International Court of Justice has not ruled on a single case related to Digital Health Sovereignty despite repeated requests from human rights organizations.

In national courts, cases have begun to emerge. In Canada, a citizen filed a lawsuit against the state for neglecting to collect digital evidence in a health crime. In Germany, a national court obligated the state to provide digital mechanisms for protecting citizens.

This chapter concludes that the legal vacuum leaves citizens without protection and calls for building a new international health legal system that balances societal security and the right of the citizen in digital health justice.

Chapter Three: Traditional Health Sovereignty versus Digital Health Sovereignty, Re-shaping Legal Concepts

Digital Health Sovereignty cannot be understood without comparing it to traditional health sovereignty, which was built upon concepts such as comprehensive health care and medical independence. But the modern digital environment challenges all of these concepts.

First, comprehensive health care becomes insufficient if the diagnostic systems rely on foreign algorithms that do not take local contexts into consideration.

Second, medical independence becomes futile if the diagnostic decision is made through artificial intelligence systems outside the scope of national supervision.

Third, equality among citizens collapses in the digital environment, because algorithms may discriminate against certain categories based on biased data.

In this context, some nations have begun formulating new concepts. Finland and the Netherlands invest in preventive Digital Health Sovereignty through developing machine learning systems that identify health threats before their occurrence. Singapore adopted interactive governmental platforms that link all authorities in a single system. In developing nations, however, practical application of Digital Health Sovereignty faces structural challenges, from the shortage of specialized cadres to the absence of coordination between health and digital authorities.

This chapter affirms that Digital Health Sovereignty is not a digital copy of traditional sovereignty but a fundamental redefinition of the concept of health sovereignty itself in a networked world that knows no borders.

Chapter Four: The Infrastructure of Digital Health Sovereignty, A Missing International Legal Definition

One of the largest gaps in international discourse on Digital Health Sovereignty is the absence of an agreed-upon legal definition of what is called the infrastructure of Digital Health Sovereignty. Without this definition, it is impossible to determine what deserves legal protection or what constitutes a violation of the rights of the citizen.

In national jurisprudence, definitions vary enormously. In the United States, the infrastructure of Digital Health Sovereignty includes: smart diagnostic systems, communication platforms between health authorities, health data bases, and electronic health records. In the European Union, the focus is on digital health justice systems that integrate transparency and efficiency. In China, it adds to these what it calls interactive health justice platforms.

In developing nations, no unified definition exists. Some states consider only electronic health records as part of the infrastructure while neglecting health data or distribution platforms.

This divergence reveals that the absence of an international definition opens the door before subjective interpretations that may be used to justify violations, whether by claiming the system is not health-related or by expanding surveillance under the banner of anything digital. The first step in building an international health legal system for Digital Health Sovereignty is agreeing on a precise definition that encompasses: smart diagnostic and treatment systems, genetic and clinical data bases, drug distribution and tracking platforms, early warning systems about epidemics, and electronic health records accessible immediately.

This chapter affirms that the definition is not a technical matter but a political decision that reflects the vision of the international community to its relationship with health justice.

Chapter Five: Algorithmic Discrimination in Digital Health Justice, Toward an International Health Legal Standard

Digital Health Sovereignty cannot be protected without determining what constitutes an illegitimate algorithmic discrimination in resource allocation during health crises. Not every algorithm is a violation against a specific group. Some discrimination may be justified, such as accelerating justice for the elderly. But racial or class-based discrimination is never acceptable.

In international jurisprudence, attempts have begun to establish criteria. In the draft Principles of Digital Health Justice, a distinction is drawn between: legitimate discrimination, which considers individual differences to enhance justice; and illegitimate discrimination, which reinforces social or racial biases.

But these principles are not binding; they remain jurisprudential opinions. And the criterion of legitimate discrimination remains ambiguous. Does accelerating justice for the wealthy constitute discrimination? And how does it differ from accelerating justice for developing nations due to algorithmic bias?

In practice, states diverge in application. In 2024, an American court considered an algorithm that gave white justice higher priority to be illegitimate discrimination. In an Asian nation, a court considered accelerating justice for business leaders to be legitimate discrimination due to their economic importance.

This chapter concludes that the international health legal standard must focus on intent and impact, not merely on the outcome. An algorithm must be classified as illegitimate discrimination if it aims to marginalize a social category from justice without health justification, leads to unjustified deprivation of a specific group from justice, or must be classified as illegitimate discrimination regardless of the means of implementation.

Chapter Six: International Health Responsibility for Digital Failure, Challenges of Attribution and Oversight

The principle of Digital Health Sovereignty cannot be applied without resolving the problem of attribution, that is, determining the authority responsible for the failure of the digital system in collecting evidence or determining the committee. Unlike traditional justice, where the court bears its responsibility directly, justice systems may be developed by private companies, creating ambiguity in responsibility.

International health law confronts three levels of attribution. The first level: the system developed by a direct governmental authority. Here responsibility is clear. The second level: the system developed by a private company at the request of the state. Here proof becomes difficult, but the principle of effective oversight may apply. The third level: the system used without official delegation. Here the state bears no responsibility unless it has neglected its duty in oversight.

In 2025, a group of governmental experts affiliated with the United Nations affirmed that the state is responsible for digital justice systems attributed to it in accordance with the principles of international law. But they did not determine how this attribution occurs in the health context.

In practice, some states have used the principle of general oversight to hold technology companies responsible for the failure of justice systems, while these companies rejected the linkage on the grounds that the state is the one who set the conditions.

This chapter affirms that the absence of a unified international standard for attribution transforms the digital health space into a zone without law, necessitating the creation of an independent international verification body affiliated with the United Nations.

Chapter Seven: Legitimate Responses to Digital Health Violations, Between Compensation and Mandatory Re-trial

When a citizen is subjected to a violation in their digital health system, what are the means of response available to them? Is it permissible to grant compensation, or to obligate the court with re-trial in response to algorithmic discrimination? This question constitutes one of the most contentious issues in contemporary health law.

International health law recognizes three types of responses. Administrative measures, such as modifying the system or changing the offending authority. Financial compensation for damage resulting from unjustified delay. And mandatory re-trial as a penalty for the state's failure to provide fair digital justice.

But when is health failure considered grave enough to justify mandatory re-trial? In the Principles of Digital Health Sovereignty, the criterion of the lost opportunity was proposed, meaning that the citizen would have obtained justice had a fair system been available to them. For example, deprivation of a citizen from collecting evidence due to algorithmic bias may be classified as a lost opportunity.

In practice, courts in Northern Europe have granted financial compensations to citizens subjected to digital discrimination. In Latin America, courts have obligated the state with re-examination of service priorities.

This chapter concludes that the absence of clear legal guidance pushes courts toward reactive decision-making, which may lead to explicit disparities in the protection of health rights.

Chapter Eight: Patents of Invention and Digital Health Sovereignty, The Tension Between Innovation and Health Exploitation

Digital Health Sovereignty cannot be discussed without addressing its fundamental tension with the system of patents of invention in health matters. Major companies control patents of invention on health data collection systems and interactive platforms, granting them monopolistic authority over health justice itself.

The American company Palantir holds patents on more than sixty percent of health data collection systems. The company IBM imposes exorbitant fees on courts that use its platforms, making them unavailable to developing nations.

In practice, these patents have led to: preventing developing nations from developing local justice systems; raising the costs of justice inappropriately; and creating permanent dependence on major companies. In developing nations, the absence of research capabilities further limits their ability to develop national alternatives.

This chapter affirms that genuine Digital Health Sovereignty is not built on dependence on foreign patents but on investment in national scientific research, and that the current patent system must be amended to balance the rights of inventors and the rights of citizens in health justice.

Chapter Nine: Digital Health Sovereignty in Developing Nations, Challenges of Capacity and Technological Dependence

While major powers possess advanced tools for imposing their Digital Health Sovereignty, developing nations face structural challenges that make this right more a slogan than a reality. The absence of technical capabilities, dependence on foreign systems, and the shortage of

specialized cadres all limit the ability of these nations to exercise their sovereignty in the field of Digital Health Sovereignty.

More than eighty percent of evidence collection systems in developing nations are imported. Most health data bases depend on American or European programs. Some nations do not even possess a national data base for health justice.

In this context, some nations have begun taking steps. India launched the National Health Systems Project. China created a sovereign health data zone. In Africa, regional initiatives have begun to develop early warning systems resistant to bias. In the Arab world, however, most nations encourage digital justice without studying its impact on health sovereignty, which may lead to genuine future crises.

This chapter concludes that Digital Health Sovereignty in developing nations is not merely a technical matter but a developmental issue requiring long-term investments, regional cooperation, and fair technology transfer.

Chapter Ten: Regional Organization of Digital Health Sovereignty, A Comparative Study of Global Experiences

In the shadow of slowing global mechanisms, regional organization has emerged as a practical solution for enhancing Digital Health Sovereignty among communities with shared interests. Regional bodies can establish binding rules faster than the United Nations.

In Asia, China and India launched the Asian Digital Health Sovereignty Initiative, which calls for the exchange of health data and the development of shared systems. In Latin America, MERCOSUR nations created a digital health response network to confront common attacks.

In the European Union, the Digital Health Strategy obligates member states to protect their citizens' data and encourages the development of national systems. In Africa, the African Union adopted the Strategy of Digital Health Justice in 2023, but implementation remains weak due to lack of funding. In the Arab world, the Arab League launched the Strategy of Digital Health Justice in 2024, calling for the creation of an Arab center for Digital Health Sovereignty, but the center was never created, and no joint deterrence mechanisms exist.

This chapter affirms that regional organization is the bridge between national sovereignty and the international system, and that its absence in some regions leaves states prey to external exploitation.

Chapter Eleven: Genetic Data and Digital Health Sovereignty, Protecting Genetic Privacy from External Exploitation

Digital Health Sovereignty cannot be achieved without protecting genetic data for citizens. Data, which represents a genetic privacy whose value cannot be estimated, has become today a target for major companies seeking to register patents of invention upon it, granting them monopoly over health justice itself.

In Africa, patents of invention were registered on patterns of crimes that communities developed over generations. In Latin America, patents were registered on evidence collection systems after their analysis in foreign laboratories. All these practices constitute what is called genetic piracy, which exploits genetic privacy without fair compensation.

International law faces absence in protecting this data. Human rights conventions do not prevent direct registration of patents on genetic data. Most developing nations do not possess sovereign national genetic data bases, facilitating their exploitation.

In response, some nations have begun enacting national legislation. In India, the Genetic Privacy Law obligates companies to share profits with health institutions. In Peru, the constitution recognizes the right of citizens to ownership of their genetic data. In the Arab world, most nations still depend on international estimates and do not possess national systems to protect their genetic data.

This chapter affirms that genetic data is not merely scientific information but an expression of the genetic identity of citizens, and that the absence of legal protection transforms genetic privacy into a commodity in the global monopoly market.

Chapter Twelve: Artificial Intelligence and Digital Health Sovereignty, When Algorithms Become Judges

With the increasing use of artificial intelligence in health decision-making, from evidence collection to determining the committee, a new threat to Digital Health Sovereignty has emerged: algorithmic authority. When artificial intelligence systems make decisions that affect the right of the citizen to justice without human oversight, the international community loses part of its health responsibility.

The problem resides in three points. Opacity: most artificial intelligence algorithms are closed-source health algorithms, and the citizen cannot understand how decisions are made. Bias: these systems may produce recommendations that serve the interests of manufacturing companies, not justice. Independence: some systems learn autonomously and may make decisions that contradict international health policies.

In practice, artificial intelligence systems led to dangerous violations. In an Asian nation, an evidence collection algorithm for poor citizens was rejected because it did not generate sufficient profits. In an African nation, artificial intelligence systems recommended using foreign

surveillance technologies instead of local systems, leading to the erosion of the national health industry entirely.

To confront this challenge, some nations have begun establishing controls. In the European Union, the Artificial Intelligence Law obligates companies to disclose how their highest-risk systems operate. In China, the Code of Ethics for Health Artificial Intelligence obligates governmental bodies to conduct impact assessments before using any smart system. In the Arab world, most nations remain in early stages of regulating artificial intelligence in health justice, and no legislation exists to protect health sovereignty from use not subject to oversight of these technologies.

This chapter affirms that Digital Health Sovereignty in the age of artificial intelligence does not mean preventing technology but imposing transparency and accountability on whoever develops and uses it.

Chapter Thirteen: Electronic Crimes and Digital Health Sovereignty, Combating Digital Health Exploitation

Digital Health Sovereignty cannot be protected without confronting electronic crimes that target citizens and health institutions across borders. Hacking of bank accounts of citizens, theft of digital health identities, spreading malware in health systems, all these crimes threaten health justice, but they remain outside the scope of justice due to the absence of effective international cooperation.

Estimates indicate that global losses from health electronic crimes exceeded five billion dollars annually, yet conviction rates do not exceed one percent in many nations. This is due to: the difficulty of identifying the perpetrator, as attacks are launched through servers in multiple countries; the absence of binding treaties, as the Budapest Convention on Combating Electronic Crimes has not been ratified by more than sixty-eight nations and does not include the most important Asian and African countries; and differences in legislation, as what constitutes a crime in one nation may be legitimate in another.

In response, some regional initiatives have begun. In the European Union, the Unified European Law for Electronic Crimes obligates member states to exchange information in real time. In Southeast Asia, ASEAN countries launched a regional strategy for combating health cybercrimes. In the Arab world, some nations have acceded to the Budapest Convention while others call for a special Arab convention, which has not yet been concluded. The absence of joint implementation mechanisms also limits the effectiveness of bilateral cooperation.

This chapter concludes that combating health electronic crimes is not merely a security matter but a practical test of states' commitment to the principle of Digital Health Sovereignty, because the absence of justice encourages criminals to target nations with weak protection.

Chapter Fourteen: Digital Education and Digital Health Sovereignty, Building Social Awareness as a Foundation for Health Defense

Digital Health Sovereignty cannot be achieved without building social awareness among citizens and employees about the dangers of cyberspace and their duties toward it. Citizens are not merely victims of attacks but partners in the justice process. The absence of digital health education makes them vulnerable to exploitation, facilitates the hacking of their systems, and threatens the national health infrastructure in its entirety.

In advanced nations, digital health education has become part of training programs. In the Netherlands, citizens learn how to recognize fake health platforms. In Singapore, the Digital Health Citizenship Program is taught in all institutions and includes concepts such as privacy, security, and social responsibility.

In developing nations, digital health education is often limited to the elite or presented through limited media campaigns. This creates a digital gap within the health society itself, where the ordinary citizen is unable to protect their data or distinguish between reliable and unreliable sources. In the Arab world, some nations have begun introducing health cyber security concepts into training programs, but they remain optional and non-systematic. In other nations, no national strategy for digital health education exists to this day.

This chapter affirms that Digital Health Sovereignty is not the sole responsibility of the state but a partnership between the state and the health society, and that investment in digital health education is cheaper and more effective than building expensive firewalls.

Chapter Fifteen: Scientific Research and Digital Health Sovereignty, Toward National Health Technological Independence

No nation can practice its Digital Health Sovereignty in a genuinely effective manner without possessing local research capabilities in the fields of health cyber security, health artificial intelligence, and digital system design. Total dependence on foreign technology makes the state vulnerable to blackmail or disruption at any moment.

Major powers have recognized this truth early. In the United States, the Advanced Health Research Projects Office allocates tens of billions of dollars annually to research projects in health cyber security. In China, the Smart Health System Plan 2030 allocates a significant portion of its budget to developing local smart surveillance systems. In developing nations, digital health scientific research suffers from lack of funding, weakness of infrastructure, and brain drain, creating a vicious circle where the absence of research leads to dependence on the outside, which in turn discourages investment in research.

In the Arab world, some nations have begun creating specialized research centers, such as King Abdullah City for Atomic and Renewable Energy, which includes a unit for health cyber security. In other nations, research focuses on commercial applications rather than technological foundations.

This chapter concludes that health technological independence is not a luxury but an existential condition for Digital Health Sovereignty, and that nations that do not invest today in health scientific research will not be digitally prosperous tomorrow.

Chapter Sixteen: Bilateral Agreements and Digital Health Sovereignty, Can Small Nations Protect Themselves?

In the absence of a comprehensive international convention, many nations have turned to concluding bilateral agreements for digital health cooperation. But these agreements are often unequal because major nations impose their conditions on the weaker party.

In some agreements, major nations demand from the other party permission to access their health data in cases of health emergencies, without a precise definition of the nature of emergencies. In other agreements, small nations are obligated to use equipment or programs from a company affiliated with the major nation, creating long-term dependence.

In contrast, some medium-sized nations have succeeded in concluding balanced agreements. Between two Asian nations, a joint committee for investigating health cyber incidents was created, enjoying full independence. Between two African nations, the principle of non-interference was agreed upon, with clear deterrence mechanisms. In the Arab world, most bilateral agreements in the digital health field remain secret, and their texts are not published for public opinion. This limits parliaments' ability to review them and prevents civil society from holding governments accountable.

This chapter affirms that bilateral agreements are not an alternative to the international system but a temporary means, and that small nations must cooperate among themselves to build a negotiating bloc capable of imposing fair conditions.

Chapter Seventeen: Health Courts and Digital Health Sovereignty, Toward Digital Health Judicial Jurisdiction

Rights cannot be protected in the digital health space without effective judicial mechanisms. But determining the competent court in health cybercrimes constitutes a significant challenge, because the crime may be committed from one nation through servers in a second nation and affect a citizen in a third nation.

National legislations have adopted several criteria for determining jurisdiction. The principle of the place where damage occurs, the most common but difficult to apply when damage is global. The principle of the perpetrator's nationality, impractical if the perpetrator is unknown. The principle of the location of the server, where servers may be in nations that have no relation to the crime.

In practice, this ambiguity led to conflicting rulings. A court in a Western nation issued a ruling imprisoning a citizen from an Asian nation for hacking a governmental health system, while a court in his nation refused to extradite him on the grounds that the act is not locally criminalized. In the European Union, jurisdiction rules were unified through the European List for Health Electronic Crimes, which obligates member states to mutually recognize rulings. In other nations, courts still lack the necessary technical expertise to understand digital health evidence. In the Arab world, most legislations do not clearly determine the court competent for health cybercrimes, leading to delays in justice or the dropping of cases.

This chapter concludes that the absence of a unified digital health judicial system encourages criminals to exploit legal gaps, necessitating the creation of an international health cyber court affiliated with the United Nations.

Chapter Eighteen: Health Data and Digital Health Sovereignty, Between Individual Ownership and Collective Sovereignty

Health data today constitutes the most valuable resource in the digital health economy. Digital Health Sovereignty cannot be complete without determining who has the right to control this data: the citizen or the state or the company?

In modern jurisprudence, three schools have emerged. The individual ownership school, which holds that the citizen is the sole owner of their data and has the right to prevent its collection or sale. The collective sovereignty school, which holds that data is a national resource and the state has the right to organize its use to protect the public interest. The joint ownership school, which seeks to balance individual right and collective interest.

In application, Europe adopted an approach close to individual ownership through the General Data Protection Regulation, which grants citizens the right to delete their data or export it. China adopted the collective sovereignty approach, where data is considered a tool for national development. The United States adopted the market approach, where data is organized through sectoral laws without a general framework. In the Arab world, some nations have issued laws for the protection of health data but lack enforcement mechanisms. In other nations, no legislation exists to regulate this field to this day.

This chapter affirms that health data is not merely numbers but an expression of individual and collective health identity, and that genuine Digital Health Sovereignty begins with respecting the citizen's right to control their information.

Chapter Nineteen: Social Justice and Digital Health Sovereignty, Protecting Societies from Irresponsible Health Technologies

Digital Health Sovereignty cannot be separated from social justice, because some digital health technologies may lead to long-term social damage. Smart evidence collection systems may have neglected poor citizens. Digital platforms may have promoted ineffective justice. Health data may have been used for discrimination against specific categories.

In practice, some digital health projects led to significant social damage. In an Asian nation, smart evidence collection systems led to the neglect of citizens in rural areas. In an African nation, digital platforms led to the spread of expensive justice at the expense of local solutions.

International law faces absence in regulating this dimension. No international agreements exist regulating the social impact of digital health technologies. Most contracts between states and companies remain secret and are not subject to health oversight. No international standards exist for responsible digital justice. In response, some nations have begun enacting legislation. In Denmark, smart evidence collection systems are required to cover all categories without discrimination. In Costa Rica, the issuance of new licenses for digital health platforms was halted until their social impact is evaluated. In the Arab world, most nations encourage digital justice without studying its social impact, which may lead to genuine future crises.

This chapter affirms that Digital Health Sovereignty must extend to protecting social justice, and that health technologies must be built on the principle of responsibility from design.

Chapter Twenty: The Future and Digital Health Sovereignty, Toward a Model International Convention

After a comprehensive review of challenges and experiences, it becomes clear that Digital Health Sovereignty is not a choice but an existential necessity in the digital age. To achieve it at the international level, it is proposed to prepare a model international convention on Digital Health Sovereignty, including the following:

First, a unified definition of Digital Health Sovereignty as the right of the citizen to benefit from smart systems designed specifically to predict health crises in cyberspace, with guarantees protecting the rights of the accused from algorithmic bias.

Second, a unified list of the infrastructure of Digital Health Sovereignty, including the fundamental systems: evidence collection, communication platforms, data bases, committee determination systems, and electronic records.

Third, the prohibition of illegitimate algorithmic discrimination in resource allocation during health crises, with a precise definition of discrimination as any algorithm that aims to marginalize a social category from justice without health justification.

Fourth, unified criteria for attribution, allowing nations to determine responsibility precisely, with the creation of an independent international verification body affiliated with the United Nations.

Fifth, mechanisms for legitimate responses, determining when compensation may be granted or the court obligated with re-trial in response to digital failure.

Sixth, states' commitment to protecting health data and respecting the rights of citizens in privacy.

Seventh, encouraging regional cooperation through the creation of regional health cyber response networks.

Eighth, supporting developing nations through technology transfer and capacity building.

Ninth, the creation of an international health cyber court that adjudicates disputes related to Digital Health Sovereignty.

Tenth, periodic review of the convention to keep pace with technological developments.

This chapter concludes by reminding us that Digital Health Sovereignty is not the end of history but the beginning of a new stage in the evolution of health law, balancing efficiency, right and justice in digital governance, technology and innovation, the state and human dignity.

Chapter Twenty-One: Smart Contracts and Digital Health Sovereignty, When Algorithms Become Witness and Judge

The concept of the health contract is no longer confined to paper and witnesses. It has extended to encompass smart contracts that execute themselves automatically when conditions are met. In times of health crises, a smart contract can release aid immediately upon confirmation of the disaster's occurrence through smart sensors.

Some humanitarian organizations have begun using smart contracts. In the International Red Cross, a smart contract is used to release aid immediately upon confirmation of the earthquake's occurrence through industrial satellite data.

The absence of legislation in developing nations limits the use of these contracts despite their effectiveness.

This chapter affirms that the smart contract is not an alternative to humans but a tool for enhancing speed and justice in times of health crises.

Chapter Twenty-Two: Blockchain and Digital Health Sovereignty, Toward Secure and Decentralized Health Records

With the increasing threats to health records, blockchain has emerged as a fundamental solution for protecting data from manipulation. Blockchain-based records cannot be modified or deleted without the signature of all parties, which ensures the integrity of information.

In practice, some nations have begun applying it. In Estonia, all health data is recorded on a national blockchain network. In the Emirates, the Smart Response Platform uses blockchain technology to track the distribution of aid.

The absence of infrastructure in developing nations limits the adoption of this technology despite its critical need.

This chapter affirms that blockchain is not merely a technology but a digital legal guarantee for transparency in health crisis management.

Chapter Twenty-Three: Biometric Data and Digital Health Sovereignty, Protecting Digital Identity of Citizens in Times of Crises

With the increasing use of biometric data, such as fingerprints and facial recognition, for targeting categories, a new threat has emerged: the exploitation of digital identity. In some cases, facial recognition algorithms led to the marginalization of racial categories due to data bias.

International law faces absence in protecting this data. Most legislations do not classify biometric data as sensitive data. No international standards exist for collecting biometric data in times of crises. Companies possess biometric records without oversight. In response, some nations have begun establishing controls. In the European Union, the collection of biometric data is prohibited without explicit consent. In Canada, the Digital Identity Protection Law criminalizes the use of biometric data for discriminatory purposes.

This chapter affirms that biometric data must be subject to the principle of maximum protection, because it is part of human dignity.

Chapter Twenty-Four: Artificial Intelligence and Digital Health Sovereignty, Toward Interpretive Algorithms

With the increasing complexity of artificial intelligence algorithms, a fundamental requirement has emerged: the capacity to interpret algorithmic decisions in times of health crises. It is not sufficient for the algorithm to say grant aid to category X. It must explain why.

Some nations have developed what is known as interpretive artificial intelligence, which produces reports that explain the reasons for their decisions in an understandable manner. In the Netherlands, interpretive algorithms are used for determining evacuation priorities. In Singapore, detailed reports are presented to the judiciary.

The absence of these systems in developing nations makes algorithmic decisions a black box that cannot be challenged.

This chapter affirms that algorithmic transparency is not a luxury but a fundamental condition for judicial accountability in times of health crises.

Chapter Twenty-Five: Adaptive Learning and Digital Health Sovereignty, When Systems Learn from Every Crisis

Fixed digital systems are no longer considered adequate. They have become systems that learn from every crisis to improve their performance in the future. Modern technologies allow algorithms to analyze their errors after every disaster and automatically adjust their behavior.

In practice, some nations have begun applying it. In Japan, adaptive learning systems are used with local earthquake patterns. In Germany, the National Learning Platform analyzes every crisis response to improve future planning.

The absence of historical data in developing nations limits the effectiveness of these systems.

This chapter affirms that adaptive learning is the heart of Digital Health Sovereignty, because it transforms failure into an opportunity for improvement.

Chapter Twenty-Six: Augmented Reality and Digital Health Sovereignty, Toward Three-Dimensional Virtual Operations Rooms

Operations rooms are no longer confined to flat screens. They have extended to augmented reality, which displays data in three-dimensional space. In times of health crises, decision-makers can visualize the disaster as if they were at its location, with interactive data layers.

In practice, some nations have begun using it. In the United States, augmented reality glasses are used for monitoring forest fires. In South Korea, the Virtual Operations Room allows interaction with a three-dimensional model of the city during crises.

The absence of infrastructure in developing nations limits the adoption of these technologies.

This chapter affirms that augmented reality is not a toy but a tool for precise decision-making in times of health crises.

Chapter Twenty-Seven: Autonomous Robots and Digital Health Sovereignty, When Machines Become First Responders

With the increasing danger of some health crises, such as chemical warfare or radiation, the role of autonomous robots has emerged as first responders. These robots do not need humans to operate in lethal environments.

In practice, some nations have begun using them. In Japan, robots are used for exploration after nuclear energy station disasters. In Russia, the Automatic Response Team intervenes in chemical leak cases.

The absence of investment in developing nations limits the use of these technologies.

This chapter affirms that autonomous robots are not an alternative to humans but a protective shield that preserves human lives in the most dangerous health crises.

Chapter Twenty-Eight: Smart Drones and Digital Health Sovereignty, Toward Smart Aerial Surveillance in Real Time

Smart drones are no longer merely imaging tools. They have become smart platforms that analyze data in real time and make immediate decisions. Some drones today are capable of identifying the locations of survivors through artificial intelligence and automatically sending their coordinates for rescue.

In practice, some nations have begun using them. In Turkey, smart drones are used for searching for survivors after earthquakes. In Brazil, the Aerial Surveillance Fleet monitors fires and identifies critical ignition points.

The absence of legislation in developing nations limits the use of these drones effectively.

This chapter affirms that smart drones are the eye of the state in the sky and a necessity in managing modern health crises.

Chapter Twenty-Nine: The Internet of Things and Digital Health Sovereignty, Toward Smart Infrastructure That Senses Crises Before Their Occurrence

Crises are no longer discovered after their occurrence. They have become sensed through the Internet of Things. Smart sensors distributed in cities, buildings, and bridges send early warnings upon detecting any malfunction.

In practice, some nations have begun applying it. In Singapore, smart sensors are used for predicting landslides. In Italy, the National Internet of Things Network monitors earthquakes before the occurrence of major tremors.

The absence of infrastructure in developing nations limits the adoption of these networks.

This chapter affirms that the Internet of Things is the nervous system of the modern state and the cornerstone of preventive health governance.

Chapter Thirty: Cloud Computing and Digital Health Sovereignty, Toward Sovereign Secure Cloud for Health Crises

With the increasing reliance on cloud computing, a new threat has emerged: storing health data in foreign clouds. In cases of conflict, these services may be cut off or used as tools of pressure.

In response to this threat, some nations have begun creating sovereign clouds. In China, all health data is stored in the National Cloud. In Russia, the Yandex Cloud is used exclusively for sensitive data.

The absence of resources in developing nations pushes them toward dependence on foreign clouds, which exposes them to danger.

This chapter affirms that the sovereign cloud is not a luxury but a fundamental condition for digital sovereignty in times of health crises.

Chapter Thirty-One: Artificial Intelligence and Digital Health Sovereignty, Toward Participatory Systems That Learn from Citizens

Artificial intelligence is no longer dependent solely on official data. It has become interactive with citizens as sources of information. Some systems today analyze social media publications to detect health crises before their occurrence.

In practice, some nations have begun using it. In India, artificial intelligence systems analyze citizens' tweets for detecting floods. In Kenya, the Digital Participation Platform allows citizens to report crises through a smart application.

The absence of digital culture in developing nations limits the effectiveness of these systems.

This chapter affirms that participatory artificial intelligence is a bridge between the state and citizens, and enhances the system's capacity for rapid response.

Chapter Thirty-Two: Open Data and Digital Health Sovereignty, Toward Digital Transparency in Crisis Management

With the increasing demands for transparency, the concept of open data for health crises has emerged, which allows citizens to track every stage of response. In some nations, aid distribution data is published in real time through open platforms.

In practice, some nations have begun applying it. In Estonia, all health data is published through the Open Data Portal. In Canada, the National Transparency Platform allows citizens to review every administrative decision related to health crises.

The absence of legislation in developing nations limits the adoption of this approach.

This chapter affirms that open data is not a luxury but a tool for social accountability and against corruption in times of health crises.

Chapter Thirty-Three: Artificial Intelligence and Digital Health Sovereignty, Toward Preventive Systems That Prevent Crises Before Their Occurrence

The goal of artificial intelligence is no longer managing crises but preventing them from occurring. Some systems today are capable of analyzing early indicators, such as climate changes or social unrest, and predicting crises months before their occurrence.

In practice, some nations have begun using it. In Germany, preventive systems are used for predicting violent protests. In Japan, the Disaster Prevention Platform analyzes geological data for predicting earthquakes.

The absence of data in developing nations limits the effectiveness of these systems.

This chapter affirms that preventive artificial intelligence is the peak of the digital pyramid for health crises, because it transforms the state from reactive to preventive.

Chapter Thirty-Four: Flexible Legislation and Digital Health Sovereignty, Toward Laws That Adapt to Digital Health Crises

With the increasing complexity of digital health crises, the need has emerged for flexible legislation capable of adapting to new challenges. Some nations today use what is known as

dynamic legislation, which is automatically amended based on artificial intelligence recommendations.

In practice, some nations have begun experimenting with it. In Singapore, artificial intelligence systems are used for proposing legislative amendments during crises. In Estonia, Smart Legislation allows amending laws through digital platforms within hours.

Legislative bureaucracy in developing nations limits the flexibility of response.

This chapter affirms that flexible legislation is not chaos but a tool for rapid adaptation to the challenges of the digital age.

Chapter Thirty-Five: Parliamentary Oversight and Digital Health Sovereignty, Toward Smart Oversight of Expenditure in Times of Crises

Parliamentary oversight is no longer confined to meetings. It has extended to digital oversight platforms that allow tracking every dollar spent in times of crises. Some parliaments today use artificial intelligence systems to detect manipulation in emergency contracts.

In practice, some parliaments have begun using it. In the British Parliament, text analysis systems are used for examining crisis contracts. In the Canadian Parliament, the Smart Oversight Platform allows members to track the flow of funds in real time.

The absence of these systems in developing nations makes expenditure in times of crises vulnerable to corruption.

This chapter affirms that parliamentary oversight is not an intervention but a guarantee of transparency in the most sensitive times.

Chapter Thirty-Six: Transitional Justice and Digital Health Sovereignty, Toward Smart Reconciliation After Crises

Transitional justice is no longer confined to truth and reconciliation. It has extended to digital reconciliation platforms that allow victims to interact in a safe environment. Some systems today use artificial intelligence to analyze victims' testimonies and propose reconciliation solutions.

In practice, some nations have begun using it. In Colombia, digital platforms are used for collecting victims' testimonies. In South Africa, the Smart Reconciliation Platform allows victims to follow the implementation of the Truth Committee's recommendations.

The absence of these platforms in developing nations makes transitional justice elitist.

This chapter affirms that digital transitional justice is not a luxury but a tool for national healing, and that its absence transforms wounds into permanent scars.

Chapter Thirty-Seven: Digital Education and Digital Health Sovereignty, Toward a Generation Aware of Digital Challenges

Education about health crises is no longer confined to books. It has extended to smart educational platforms that teach crisis management in an interactive manner. Some schools today use virtual reality to simulate disasters and teach students how to respond.

In practice, some nations have begun applying it. In Finland, children learn crisis management through interactive digital games. In Singapore, the Crisis Education Platform allows students to simulate emergency scenarios.

The absence of these platforms in developing nations makes education dry.

This chapter affirms that digital education for health crises is not a luxury but an investment in the future of national security, and that its absence transforms citizens into easy prey in times of crises.

Chapter Thirty-Eight: Popular Participation and Digital Health Sovereignty, Toward Participatory Democracy in Times of Crises

The concept of popular participation is no longer confined to elections. It has extended to participatory platforms that allow citizens to contribute to decision-making during crises. Some systems today allow citizens to propose solutions and vote on them in real time.

In practice, some nations have begun using it. In Iceland, citizens are allowed to modify emergency plans through a digital platform. In Taiwan, the Smart Participation Platform allows citizens to propose solutions for crises and modify them.

The absence of these platforms in developing nations makes popular participation formal.

This chapter affirms that digital popular participation is not a luxury but the essence of democracy in times of crises, and that its absence transforms the state into an entity isolated from its people.

Chapter Thirty-Nine: International Humanitarian Law and Digital Health Sovereignty, Protecting Civilians in Health Conflicts

With the increasing use of health resources as weapons in conflicts, a fundamental question has emerged: does the destruction of digital health infrastructure constitute a violation of international humanitarian law? And is deliberate causing of health crisis considered a war crime?

In some conflicts, cooling systems for health facilities were destroyed, leading to their loss. In other cases, distribution platforms were hacked to force populations to flee. All these acts caused long-term health damage.

In the Tallinn Manual 2.0 project, it was affirmed that the destruction of health infrastructure as a weapon of war constitutes a violation of humanitarian law. But practical application remains difficult due to the ambiguity of intent and the difficulty of proving the causal relationship. In the International Criminal Court, the crime of destruction of health infrastructure remains under discussion and has not yet been classified in the basic system.

This chapter affirms that Digital Health Sovereignty does not mean abandoning humanity in times of war, but rather strengthening the protection of civilians from digital health weapons.

Chapter Forty: Digital Health Sovereignty and the Future, A Strategic Vision for Coming Decades

At the conclusion, Digital Health Sovereignty cannot be viewed as a temporary phenomenon but as a fundamental transformation in the concept of the state in the twenty-first century. Nations that adopt Digital Health Sovereignty today will be capable of: protecting their citizens from digital manipulation in times of crises; building an independent and sustainable digital health economy; enhancing the position of their generations in the global health system; and participating actively in crafting the rules of the new international order.

Nations that ignore this transformation will find themselves hostage to foreign technology, exposed to external interventions, and incapable of protecting their interests in the digital age. Investment in Digital Health Sovereignty is therefore not a question of choice but a question of survival.

Conclusion

After a comprehensive review of the dimensions of Digital Health Sovereignty across all fields, from cyber security to economy to culture to development, it becomes clear that this concept was never a technical luxury but an existential guarantee for the modern state. The digital health space, despite its non-material nature, has become an arena for political and economic conflicts, and no state can maintain its sovereignty over its health management without effective national digital capabilities.

This work has revealed that the legislative vacuum constitutes a double threat: it allows major companies and states to impose their dominance, and it leaves developing nations exposed to exploitation without legal protection. To fill this vacuum, a collective initiative is necessary to build a fair international system that balances health sovereignty and the right of citizens in digital health justice.

In the end, genuine Digital Health Sovereignty is not built on isolation or repression but on transparency, efficiency, and trust between the state and citizens. It is not an end in itself but a means to build a safe health future, just and humane.

References

United Nations Office for Disaster Risk Reduction, UNDRR, Global Assessment Report on Disaster Risk Reduction, 2025. International Federation of Red Cross and Red Crescent Societies, IFRC, World Disasters Report, 2024. European Commission, Digital Crisis Management Action Plan, 2024. World Bank, Resilient Infrastructure Guidelines, 2023. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017. General Data Protection Regulation, GDPR, Regulation EU 2016/679. National Institute of Standards and Technology, NIST, Cybersecurity Framework, 2023. Elrakhawi M K A, 2026, The Global Encyclopedia of Law, A Comparative Practical Study, First Edition, Ismailia, Global Legal Publications. Schmitt M N, 2023, Cyber Operations and International Law, Cambridge University Press. Rajamani L, 2025, Crisis Governance and Digital Sovereignty, Oxford University Press. De Schutter O, 2023, The Right to Resilience in the Digital Age, Cambridge University Press. Kloppenburg J R, 2024, Digital Sovereignty and Crisis Exploitation, University of California Press.

Official Government Sources: White House, National Strategy for Digital Crisis Management, 2024. European Commission, Digital Crisis Management Action Plan, 2023. Ministry of Interior Reports on Cyber Resilience in Crisis Systems, Multiple Jurisdictions, 2020 to 2025.

Academic Journals: Journal of International Crisis Law, Oxford. International Journal of Digital Crisis Governance. Harvard Law Review, Crisis Management Section. Stanford Technology Law Review.

Table of Contents

Health Responsibility for Digital Failure, Challenges of Attribution and Oversight. Chapter Seven, Legitimate Responses to Digital Health Violations, Between Compensation and Mandatory Re-trial. Chapter Eight, Patents of Invention and Digital Health Sovereignty, The Tension Between Innovation and Health Exploitation. Chapter Nine, Digital Health Sovereignty in Developing Nations, Challenges of Capacity and Technological Dependence. Chapter Ten, Regional Organization of Digital Health Sovereignty, A Comparative Study of Global Experiences. Chapter Eleven, Genetic Data and Digital Health Sovereignty, Protecting Genetic Privacy from External Exploitation. Chapter Twelve, Artificial Intelligence and Digital Health Sovereignty, When Algorithms Become Judges. Chapter Thirteen, Electronic Crimes and Digital Health Sovereignty, Combating Digital Health Exploitation. Chapter Fourteen, Digital Education and Digital Health Sovereignty, Building Social Awareness as a Foundation for Health Defense. Chapter Fifteen, Scientific Research and Digital Health Sovereignty, Toward National Health Technological Independence. Chapter Sixteen, Bilateral Agreements and Digital Health Sovereignty, Can Small Nations Protect Themselves. Chapter Seventeen, Health Courts and Digital Health Sovereignty, Toward Digital Health Judicial Jurisdiction. Chapter Eighteen, Health Data and Digital Health Sovereignty, Between Individual Ownership and Collective Sovereignty. Chapter Nineteen, Social Justice and Digital Health Sovereignty, Protecting Societies from Irresponsible Health Technologies. Chapter Twenty, The Future and Digital Health Sovereignty, Toward a Model International Convention. Chapter Twenty-One, Smart Contracts and Digital Health Sovereignty, When Algorithms Become Witness and Judge. Chapter Twenty-Two, Blockchain and Digital Health Sovereignty, Toward Secure and Decentralized Health Records. Chapter Twenty-Three, Biometric Data and Digital Health Sovereignty, Protecting Digital Identity of Citizens in Times of Crises. Chapter Twenty-Four, Artificial Intelligence and Digital Health Sovereignty, Toward Interpretive Algorithms. Chapter Twenty-Five, Adaptive Learning and Digital Health Sovereignty, When Systems Learn from Every Crisis. Chapter Twenty-Six, Augmented Reality and Digital Health Sovereignty, Toward Three-Dimensional Virtual Operations Rooms. Chapter Twenty-Seven, Autonomous Robots and Digital Health Sovereignty, When Machines Become First Responders. Chapter Twenty-Eight, Smart Drones and Digital Health Sovereignty, Toward Smart Aerial Surveillance in Real Time. Chapter Twenty-Nine, The Internet of Things and Digital Health Sovereignty, Toward Smart Infrastructure That Senses Crises Before Their Occurrence. Chapter Thirty, Cloud Computing and Digital Health Sovereignty, Toward Sovereign Secure Cloud for Health Crises. Chapter Thirty-One, Artificial Intelligence and Digital Health Sovereignty, Toward Participatory Systems That Learn from Citizens. Chapter Thirty-Two, Open Data and Digital Health Sovereignty, Toward Digital Transparency in Crisis Management. Chapter Thirty-Three, Artificial Intelligence and Digital Health Sovereignty, Toward Preventive Systems That Prevent Crises Before Their Occurrence. Chapter Thirty-Four, Flexible Legislation and Digital Health Sovereignty, Toward Laws That Adapt to Digital Health Crises. Chapter Thirty-Five, Parliamentary Oversight and Digital Health Sovereignty, Toward Smart Oversight of Expenditure in Times of Crises. Chapter Thirty-Six, Transitional Justice and Digital Health Sovereignty, Toward Smart Reconciliation After Crises. Chapter Thirty-Seven, Digital Education and Digital Health Sovereignty, Toward a Generation Aware of Digital Challenges. Chapter Thirty-Eight, Popular Participation and Digital Health Sovereignty, Toward Participatory Democracy in Times of Crises. Chapter Thirty-Nine, International Humanitarian Law and Digital Health Sovereignty, Protecting Civilians in Health

Conflicts. Chapter Forty, Digital Health Sovereignty and the Future, A Strategic Vision for Coming Decades. Conclusion. References. Table of Contents.

And with God lies all guidance and success.

Authored by Dr. Mohamed Kamal Arafa Elrakhawi.

DOI: 10.5281/zenodo.21806640