ÉTUDES
DE L'IFRI

GEOPOLITICS OF TECHNOLOGY PROGRAM

JULY
2021

Health Data Governance

Lessons Learned from the COVID-19 Pandemic in Europe, China, and the United States

Julie MARTINEZ
Clément TONON

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization. As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience.

Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers, and internationally renowned experts to animate its debate and research activities.

ISBN: 979-10-373-0413-1

Translated from the French by *Cadenza Academic Translations*

How to cite this publication:
Julie Martinez and Clément Tonon, "Health Data Governance: Lessons Learned from the COVID-19 Pandemic in Europe, China, and the United States", *Études de l'Ifri*, Ifri, July 2021.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

Authors

Julie Martinez is a registered lawyer with the Paris Bar, specializing in information technology and data privacy law, and holds three European LL.M.s in legal aspects of international affairs and emerging technology.

Clément Tonon is a senior civil servant, and a graduate of the École des hautes études commerciales (HEC) business school and the École nationale d'administration (ENA). He is coauthor of the *Étude de l'Ifri* "Europe: Subject or Object in the Geopolitics of Data?," published in July 2018, and author of the *Étude de l'Ifri* "GovTech, The New Frontier in Digital Sovereignty," published in November 2020.

Abstract

The COVID-19 public health crisis has triggered a tectonic shift in the reconfiguration of models of health data governance and protection around the world, and accelerated the entry of the big tech companies into the e-health sector. This study provides a comparative analysis of approaches to managing health data in the European Union, the United States, and China: an area characterized by reconfigurations and confrontations that will form an essential component of future power relations within this strategic triangle. As data are the material of transnational digital flows, understanding these models takes us beyond the purely legal aspects to reveal the ways in which they are related, come into conflict, and influence one another. As such data constitute an issue of international politics in its own right in relation to these three major poles of the global digital economy.

The COVID-19 pandemic has exposed the shortcomings of the pre-existing governance models in every part of the globe, and the need to move toward a "health data-driven" model of managing public health crises. In Europe, and France in particular, the public health crisis has also revealed a long-standing "technological innocence" with whose consequences the authorities are now coming to terms. Despite this strategic wake-up call, questions remain about the ability of the European states to work together effectively and move toward a shared digital health space, when they do not currently have an industrial player comparable to the US and Chinese tech giants.

This study makes one thing clear: one of the shockwaves resulting from the COVID-19 pandemic will be a digital one. Through its lasting impact on the relations between states, companies, and citizens, the public health crisis has ushered nations into the "geotechnological" twenty-first century, in which health data will be one of the main vectors of power and wealth.

Table of contents

Introduction

On May 20, 2021, an episode of the television show *Cash Investigation*, entitled "Nos données personnelles valent de l'or!" [The Goldmine of Our Personal Data], was broadcast on France 2. It reported on how the United States (US) company IQVIA had set up a health data "warehouse" through the French pharmacy network. Questions about the operation of this database prompted a public response from the *Commission nationale de l'informatique et des libertés* (CNIL) (French Data Protection Authority) recalling the European legal framework and guarantees concerning such use.[1] A few days later, on May 17, 2021, the French government unveiled its "National Cloud Strategy," setting out the tools (including technology under license, trusted cloud status, and industrial partners) it intends to put in place in order to give French companies and public institutions "access to the world's most powerful tools while ensuring data is processed in accordance with European values."[2] The goals of this strategy include protecting the data of French people "from all extra-EU regulation," i.e., laws with extraterritorial reach—particularly those of the US and China.[3]

As these recent events have shown, the COVID-19 pandemic has put data—and particularly health data, which have seen a boom in their production and use—at the heart of the French and European public debate about the balance between fundamental freedoms and sovereignty in the digital space. It has also served as a catalyst for three key dynamics that lie at the heart of this study.

First, the pandemic has revealed the strategic importance, for states, of understanding and controlling health technologies and the use of individual health data in managing a major public health crisis. As such, it questions the suitability of the models of health data governance and regulation that had been developed or were being developed before the pandemic broke out. Several governments have already begun considering mass digitization of their health system

1. Commission nationale de l'informatique et des libertés, "Entrepôt de données santé IQVIA: la CNIL rappelle les conditions et le cadre légal ayant permis son autorisation en 2018", May 17, 2021, available at: www.cnil.fr.
2. Cédric O, Secretary of State for the Digital Transition and Electronic Communications, at the press conference to unveil the "National Cloud Strategy" on May 17, 2021. Translator's note: Quotation our translation from the French. Unless otherwise stated, all translations of cited foreign language material in this article are our own.
3. *Ibid*.

and changes to their regulations on the back of the pandemic: on June 22, 2021, for example, the United Kingdom (UK) government published an ambitious strategy that includes a list of proposals and legislative changes to be implemented over the period 2021–2030 in order "to unleash the unlimited potential of data in health and care, while maintaining the highest standards of privacy, ethics, and accountability."[4]

Second, the public health emergency has demonstrated the growing importance, across all aspects of social life, of the digital health economy, which is characterized by an extremely buoyant commercial ecosystem in which most of the leading global technology actors are taking a stake. Between 2013 and 2020, the volume of health data produced globally increased by a factor of 15, from 153 exabytes to 2,314 exabytes.[5] This level of growth has made the health care "big data" market one of the most attractive sectors of the e-health market. According to certain estimates, it is set to grow in value from around $11.5 billion (€ billion) in 2016 to $70 billion in 2025.[6]

Finally, the pandemic has intensified the power relations that are developing within a veritable "geopolitics of data" on the world stage.[7] In addition to comparing legal and political models, there is therefore a need to consider the actors involved in this global competition, namely the public health, industry, digital, and scientific complexes that, within a given space, manage the collection and processing of health data in accordance with a set of rules and values. This study shows that, in the post-COVID global digital competition, without such alignment between a value system, a legal framework, and an industry ecosystem, there can be no real power or sovereignty. According to Cédric Villani and Gérard Longuet, there is a real risk that France "will see the development of foreign algorithms that are not regulated by French laws, if our country does not equip itself with the means to advance at the pace of others."[8] Similarly, for the German health minister, Jens Spahn, "the question [for Europe] is whether the services required have to come solely from US companies

4. Department of Health and Social Care, "Data Saves Lives: Reshaping Health and Social Care with Data (Draft)", June 22, 2021, available at: www.gov.uk.
5. Stanford Medicine Health Trends Report, "Harnessing the Power of Data in Health", 2017.
6. Statista, "Global Healthcare Big Data Market Size in 2016 and a Forecast for 2025", October 22, 2020, available at: www.statista.com.
7. A. Cattaruzza, *Géopolitique des données numériques. Pouvoir et conflits à l'heure du Big Data*, Paris: Le Cavalier Bleu, 2019.
8. C. Villani and G. Longuet, on behalf of the Office parlementaire d'évaluation des choix scientifiques et technologiques, "L'intelligence artificielle et les données de santé", March 21, 2019.

or whether we can develop them ourselves, based on European data protection criteria."[9]

This study provides a comparative analysis of approaches to managing health data in order to identify legal and political models whose overlapping, opposition, and alignment will have significant medium-term diplomatic repercussions. First, we look at the specific characteristics of health data within a broader typology of digital data. Second, we present the governance models of the European Union (EU), US, and China: an area characterized by reconfigurations and confrontations that will form an essential component of future power relations within this strategic triangle. As German health minister Jens Spahn has observed, while the European model has developed on the basis of a normative approach committed to protecting fundamental rights, there are also "models of police and capitalist surveillance that differ from our own."[10] Finally, we analyze the changes for which the COVID-19 pandemic has been a catalyst, including the different approaches to managing the crisis taken by the EU, US, and China, which have used health data-driven tools to track chains of transmission.

This study shows that the public health crisis has triggered a tectonic shift in the reconfiguration of models of health data governance and protection around the world, largely centered on health data, and has accelerated the entry of the big tech companies into the e-health sector. In particular, we draw two main conclusions from the crisis.

First, the COVID-19 pandemic has revealed the shortcomings of the pre-existing governance models in every part of the globe, and the need to move toward a "health data-driven" model of managing public health crises. In Europe, and France in particular, the public health crisis has also revealed a long-standing "technological innocence" with whose consequences the authorities are now coming to terms.[11] Despite this strategic wake-up call, questions remain about the ability of the European states to work together effectively and move toward a shared digital health space, when they do not currently have an industrial player comparable to the US and Chinese tech giants. In the US, the pandemic has created tensions around the model of health data governance arising from the gaps illustrated by technological management of the crisis—in particular the relationship between the federal government and state authorities. President

9. Jens Spahn, in an interview: N. Steiwer, "Données de santé: comment l'Allemagne tente d'échapper à l'emprise américaine", *Les Échos*, March 11, 2020.
10. *Ibid*.
11. T. Gomart, "COVID-19 and the End of Technological Innocence", *Politique étrangère*, Vol. 85, No. 2, Summer 2020.

Joe Biden has announced changes that shift the country toward a model of global regulation of personal data. Finally, in China, the pandemic has accelerated the transition toward a surveillance capitalism model: one whose true success during the crisis may not be as clear-cut as it appears, and which in the short-term could bring about a new power struggle between the regime and the country's tech giants.

Second, the COVID-19 crisis has accelerated the advances made by major global private actors into the management of a crisis involving the regalian functions of the state.[12] These advances, which question both the role of the state and the very concept of public interest, are by no means neutral from the point of view of the relations between governments and private actors. Tech companies, which are now positioning themselves throughout the health data value chain, from raw collection through connected objects to mass processing for insurance purposes, now hold all the levers they need for the economic—and in future potentially political—exploitation of such collection through big data processing and artificial intelligence (AI).

This study makes one thing clear in particular: one of the shockwaves resulting from the COVID-19 pandemic will be a digital one. Through its lasting impact on the relations between states, companies, and citizens, the public health crisis has ushered nations into the "geotechnological" twenty-first century, in which health data will undoubtedly constitute one of the main "powers of the future."[13]

12. C. Tonon, "GovTech, The New Frontier in Digital Sovereignty", *Études de l'Ifri,* Ifri, November 2020.
13. S. Grumbach and S. Frénot, "Les données, puissance du future", *Le Monde*, January 7, 2013.

The specific characteristics of health data within the "datasphere"

Health data are key to current technological issues because they have two specific characteristics within the typology of the digital world. First, the definition of health data is extremely broad and ever evolving: the concept covers data that are health data by nature (such as medical history, details of care provision, test results, medications, and disabilities), data that become health data through being matched to other data (such as matching a weight measurement to number of daily steps), and data that become health data by virtue of their end use in a medical context.[14] A second distinction is made between personal health data and non-personal health data, in particular "anonymized" data where the link to an individual's identity is entirely and permanently broken.

Conversely, health data that have undergone "pseudonymization"—a process frequently used in medical research, which consists of replacing directly identifying data (such as first name and surname) with indirectly identifying data (such as alias or sequential number) are still considered to be information about an identifiable physical person and thus remain personal data. This is a key distinction in the European legal regime derived from the General Data Protection Regulation (GDPR), which outlines the boundary—a particularly slim one, in the case of health data—between personal and non-personal data. As health data are often an integral part of mixed databases derived from electronic medical records, clinical trials, and data series collected through various health apps, the European normative framework now requires initial processing operations and further data processing operations to comply with the GDPR.[15]

14. One definition includes: "All primary data resulting from human activity—even with no apparent link to health—may contribute—through being matched to other data that are not linked to them—to creating new information concerning an individual's health. Health data can no longer be limited solely to personal data gathered in the context of medical care (laboratory test results, genomic characteristics, clinical data, etc.)." French National Consultative Ethics Committee, "Données massives (big data) et santé : une nouvelle approche des enjeux éthiques", May 29, 2019, available at: www.ccne-ethique.fr.

15. European Commission, "Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union", May 29, 2019.

In addition to this, the particular sensitivity of personal health data, which is enshrined in almost all personal data legislation around the world, reinforces the need for security, transparency, and responsibility demanded by democratic societies in relation to their collection and use. In Europe, the GDPR thus singles out health data, genetic data, and biometric data in the category of sensitive data in article 9, and states that "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."[16]

This particular sensitivity, which reflects the weighty ethical scholarship on patient confidentiality in the medical profession, and its long history,[17] results primarily from the particular risks involved in the exploitation of these data and the questions they raise about our relationship to the personal: matching these data weakens the boundary between private and public life, and provides a basis for very detailed profiling that may go as far as discrimination or manipulation for political or commercial ends, and their collection and analysis provide a gateway into the health care sector for new tech actors that may not have the same commitment to the principles of solidarity, equity, and ethics enshrined in Western health care systems. According to the French National Consultative Ethics Committee for Life Sciences and Health: "one of the characteristics of health big data is that they do away with the distinctions that provide the basis for the implementation of the ethical principles underpinning the protection of individual rights in the health care sphere [...] care and commerce are becoming increasingly difficult to tell apart, due to the transformation of care and the health market."[18]

These two specific characteristics of health data (their ubiquity, and sensitivity)[19] trigger two observations concerning the sphere of power relations. In security terms, in a context of increased international competition between public and private actors for control of the "datasphere," health data have become a key battleground in cyberspace. The health economy has become one of the world's most targeted sectors, with the number of cyberattacks doubling in 2020,[20] and attacks taking place on an increasingly

16. GDPR, Article 9, para. 4.
17. As far back as the Hippocratic Oath, maintaining confidentiality, patient–physician trust, and refraining from exploiting privileged access to information have been cardinal principles in medicine and medical research.
18. French National Consultative Ethics Committee, "Données massives (big data) et santé".
19. INRIA Grenoble, "Concilier ubiquité et sécurité des données médicales", *Cahiers du CRID*, No. 32, January 6, 2011.
20. Compliance Home, "Healthcare Cyberattacks Doubled in 2020 According to IBM X-Force", March 2021.

frequent basis on hospital facilities and national health care information systems (with the latest on May 14, 2021, when a massive ransomware cyberattack on the Irish health care system shut it down for several hours.)[21]

In France, this escalation has been very clear: Cédric O, the Secretary of State for Digital Affairs, reported to the Senate in February 2021 "that while there were twenty-seven major attacks on hospitals in 2020, there have been one a week since [the beginning of] 2021," with attacks on hospitals in Dax and Villefranche-sur-Saône covered extensively in the press.[22] In September 2020, Germany saw the world's first deadly cyberattack, when the shutdown of the Düsseldorf University Hospital computer system resulted in patients being transferred to other hospitals in the region, and a critically ill female patient died in transit.[23]

The prospect of a "digital Pearl Harbor," in which an attack on a health care facility results in mass deaths in real life, can no longer be excluded as a possibility. This phenomenon has intensified in the context of the COVID-19 pandemic and has resulted in over forty high-level diplomats and leading figures, including Ban Ki-moon, Madeleine Albright, and Mikhail Gorbachev, joining with the International Committee of the Red Cross (ICRC) in calling on governments to agree on cyberspace regulation in order to prevent attacks on health care, an area in which major international collaboration is required in the coming months.[24]

From a political and democratic point of view, health data throw the question of trust between citizens and governments into sharp relief. This is not simply a domestic political issue for governments, but—as illustrated in particular by the controversy over contact tracing apps and "health passports" during the COVID-19 pandemic—determines their capacity for effective international collaboration and, in the case of the EU, to move toward the creation of a genuine European health space. As Margareth Vestager, Executive Vice President of the European Commission for A Europe Fit for the Digital Age, explained in an interview on May 7, 2021: "So it's really important that we get this right to create the trust that people's health data can be in a health data space. In particular, since we know that the majority of Europeans actually say, no, we are not interested in

21. BBC, "Cyber Attack 'Most Significant on Irish State'", May 14, 2021.
22. Cédric O, cited in *Le Figaro*, "Cybersécurité des hôpitaux: '27 attaques majeures en 2020 et une par semaine en 2021,'" February 17, 2021.
23. F. Dèbes, "En Allemagne, une première cyberattaque mortelle", *Les Échos,* October 19, 2020.
24. International Committee of the Red Cross, "Call to Governments: Work Together to Stop Cyber Attacks on Health Care", May 2020.

sharing our health data for no matter what purpose."[25] A survey carried out in January 2021 showed that 47% of Europeans surveyed were opposed to their government sharing their health data with private companies such as Google, while 45% were in favor.[26]

Governments are thus faced with the need to manage two separate temporalities: the democratic temporality, which requires them to ward off the distrust provoked, particularly in Europe, by the collection of health data by governments or private companies; and the urgent need, identified by researchers and those in industry, not to fall behind in the global digital health app race. As observed in the report from the French Parliamentary Office for Evaluating Scientific and Technological Options, the only real risk for a country like France, "would be not to embrace AI, digital, and a data-driven approach".[27] The controversy that recently broke out in the UK over then health minister Matt Hancock's plan to centralize the data of 55 million patients in England in a single database run by NHS Digital for the purposes of medical research and improving the efficiency of the health care system, which led to the opt-out date being pushed back from July 1, 2021 to September 1, 2021, reveals the scale of this tension in Western democracies in the wake of the public health crisis.[28]

25. M. Mc Mahon, "Margrethe Vestager Explains the EU's Position in the Global Battle for Data", Euronews, May 17, 2021.
26. Center for the Governance of Change, "European Tech Insights 2021. Part I: How the Pandemic Altered our Relationship with Technology", available at: www.ie.edu.
27. Villani and Longuet, "L'intelligence artificielle."
28. *The Guardian,* for example, one of the UK's most influential daily newspapers, published an editorial in favor of pushing back the reform and holding a democratic debate on the issue. See "*The Guardian* View on Medical Records: NHS Data Grab Needs Explaining", *The Guardian,* May 30, 2021.

Health data governance and regulation prior to the COVID-19 pandemic

Prior to the COVID-19 pandemic, the EU, US, and China had developed distinct models of health data governance and regulation. A comparison of these models reveals structural differences between them, as a result of different political and industrial foundations, but also the potential for greater alignment. As data are the material of transnational digital flows, understanding these models takes us beyond the purely legal aspects to reveal how the ways in which they are related, come into conflict, and influence one another constitute an issue of international politics in its own right in relation to these three major poles of the global digital economy, whose center of gravity is increasingly shifting to Asia from the Atlantic.[29]

The European Union

The heterogeneity of health data governance within Europe

Prior to the public health crisis, there were three main identifiable models for managing health data in Europe: the decentralized German model, the open Nordic model, and the centralized French model. Analyzing the heterogeneity of the approaches and nature of the available databases enables us to identify the commonalities required if we are to move toward a true European digital health space.

Germany

In November 2019, the e-health market in Europe was forecast to reach $234 billion by 2023, equating to 160% growth over this period.[30] While Germany has the most buoyant e-health market in Europe, with an estimated value of €57 billion in 2025 and annual growth of €19 billion, it is hampered by the highly decentralized way

29. T. Gomart, J. Nocetti, and C. Tonon, "Europe: Subject or Object in the Geopolitics of Data?", *Études de l'Ifri,* Ifri, July 2018.
30. BPI France, "E-santé: vers un marché de 234,5 milliards de dollars", November 2019.

in which the German health care system is organized.[31] This gives the Länder a leading role in regulating care provision and the hospital system, resulting in database fragmentation and heterogeneity. Germany has since been catching-up on challenges raised by its decentralized system, especially thanks to a major digitization project spearheaded by health minister Jens Spahn, which has helped create a buoyant digital health market since 2018. Spahn has clearly put this at the heart of his ministerial agenda, with the ambition of bringing the digital performance of the German health care system in line with that of the Nordic countries. The "Digitale-Versorgung-Gesetz," a law passed in November 2019 "designed to improve digitization and innovation," constitutes a key step in this move toward digitization of the German health system.

At the national level, around 73 million patients insured under the German mandatory health insurance scheme can now be prescribed a digital health application (DiGA) reimbursed by the mandatory insurance providers. Since June 2020, e-health companies from around the world have been able to submit an online application for fast-track approval of their DiGA to the German Federal Institute for Drugs and Medical Devices (BfArM). Since becoming health minister, Jens Spahn has also launched patient electronic medical record and electronic prescription initiatives. Despite this investment, prior to COVID-19 professionals had concerns about the hasty way in which medical practices and hospitals had been digitized since 2019, at the expense of security concerns. After inspecting over thirty practice systems, Harald Mathis, from the Fraunhofer Institute for Applied Information Technology (FIT), reported that only "a third of systems were secure."[32]

The Nordic Countries

The approach taken by the northern European countries, comparable to that of the UK, places greater emphasis on governing health data through open data that are freely accessible and available to users and researchers. Prior to the public health crisis, Norway and Sweden were already leading the way in health data governance: Norway had 16 national health data registries (the first one created in 1951) for a population of 5 million, and Sweden had 73 national registries for a population of 10 million. Before the pandemic, Sweden, Finland, Norway, and Iceland had a joint open data project combining analytical tools, AI, and machine learning, to bring together data in

31. R. Berger, "Future of Health – The Rise of Healthcare Platforms", September 30, 2020, available at: www.rolandberger.com.
32. N. Steiwer, "Données de santé".

order to create a shared drug prescription database including 25 million people.[33]

France

France's centralized system, primarily built around the National Health Insurance Cross-Scheme Information System (SNIIRAM), has enabled it to develop large databases whose quality is "unrivaled in Europe, in terms of the number of people concerned and the range of available data."[34] In a 2016 report, however, the French Court of Audit expressed concerns that this database, "which has considerable potential for public health, research, the efficiency of the health system, and cost control,"[35] was not being used to its full potential.[36]

Although the law of January 26, 2016, on modernization of the French health care system has consolidated health data governance, this latter is still developing through a partnership between the state and industry players in the sector. The law also created the National Health Data System (SNDS), which is a unique database for describing population health through the health care system. The SNDS is designed to bring together pre-existing health care administrative data—such as the SNIIRAM, the PMSI hospital care database containing data analyzing the activity of health care facilities, and the CépiDc (Center for the Epidemiology of Medical Causes of Death) database.

France has been able to create specialist databases and then set out the foundations of the SNDS. These databases, however, remain inadequately used.[37] In 2018, the Court of Audit reported that this situation stood in stark contrast "to the countries that went down this road most rapidly, in particular Sweden and to a lesser extent Italy and the United Kingdom", and highlighted the lack of a system for electronic prescribing of drugs, medical devices, and medical care in causing major financial waste for Assurance Maladie, the French state health insurance provider.[38] France's relative backwardness in exploiting health data explains the attempt to revive this public policy in 2019 by attaching a Directorate for Digital Health to the office of

33. Deloitte Legal, "Bridging Nordic Data: Legal Overview of Possibilities and Obstacles for Secondary Use of Health Data for Innovation and Development", June 2020, available at: www.norden.diva-portal.org.
34. Cour des Comptes, "Les données personnelles de santé gérées par l'assurance maladie", March 2016.
35. *Ibid.*
36. B. Lebray, "Les données de santé: une mine d'or pour l'économie française?", January 15, 2020, available at: www.bignonlebray.com.
37. É. Chapel *et al.*, "La révolution du pilotage des données de santé: Enjeux juridiques, éthiques et managériaux", *LEH Edition*, May 2019.
38. Cour des Comptes, "La Sécurité Sociale – Rapport sur l'application des lois de financement de la sécurité sociale", October 2018.

the Ministry of Health, tasked with steering the ministerial digital health roadmap up to 2022 and supervising the Agency for Digital Health responsible for establishing reference materials and developing database interoperability, as well as handling related ethical and cybersecurity concerns.

Finally, in the wake of the Villani report on AI published in March 2018,[39] and President Macron's speech of September 18, 2018, on the "Ma Santé 2022" plan, the law of July 24, 2019, on the organization and transformation of the health care system announced the extension of the SNDS to all health data associated with a procedure reimbursed by Assurance Maladie. It also set out the creation of the Health Data Hub (HDH), a technology platform designed to be open to numerous stakeholders (including researchers, patient organizations, and companies), the organization of which has raised the issue of the security of hosting health data in France and Europe, which we will come to in the second part of this study.

Efforts to create a true European digital health space

Before the COVID-19 pandemic broke out, the EU had no regulatory or governance framework through which it could take a health data-driven approach to a public health crisis at the Union level. The seeds of this failure were sown at the time of the construction of Europe, with the abortive attempt to found a "European Health Community," first proposed in 1952 by the French government and its then health minister, Paul Ribeyre.[40] Dubbed the "White Pool"—in contrast to the "Black Pool" of the European Coal and Steel Community—this organization was designed to create interdependency between the Member States by creating a shared health insurance regime, harmonizing public health policies, and combining medical research efforts.

Significantly, this initiative died a death at the same time as the European Defence Community (EDC), of which it had been envisaged as the functionalist counterpart, with similar strategic ambitions. As Paul Ribeyre observed: "It is a new form of European Defence Community in which the French government is asking you to participate: this time, a European Defence Community against

39. C. Villani *et al.*, "Donner un sens à l'intelligence artificielle", March 2018.
40. See A. Davesne, "L'Europe de la santé, une histoire française?" in: G. Coron (ed.), *L'Europe de la santé. Enjeux et pratiques des politiques publiques,* Rennes: Presses de l'EHESP, 2018, pp. 19–40.

suffering and disease."[41] The project was abandoned due to a clash with French commercial interests and opposition from Gaullists: in the treaties, health care is merely a shared Community competency and each Member State remains responsible for its own health policy and governance. In the silence of the texts, the European Health Space lay dormant for decades (with the notable exception of drug regulation), and paradoxically emerged by way of data, through the major regulations of the late 1990s.

Without being subject to special regulation in the EU, health data have had special protection under general personal data protection regulation since the adoption, in 1995, of directive 95/46/EC, the first in this area.[42] Since the GDPR came into effect on May 25, 2018, personal health data have been subject to a special, comprehensive definition at the European level: "data concerning health" are defined as all personal data "related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[43] This broad definition provides increased protection on the grounds of their "sensitive" nature, based on the principle of the general prohibition on collecting health data that may only be lifted in very strict and narrowly defined circumstances, such as through obtaining clear and express informed patient consent or in the context of the activities of social security, preventive medicine, and in the interests of public health.

For many actors in the e-health sector, the restrictive approach taken by the GDPR therefore represents an obstacle to the commercial exploitation of health data—as it prevents the creation of European industrial ecosystems of critical size, and paradoxically strengthens the monopoly of the actors already in place[44]—but also to the progress of basic research.[45] For others, the GDPR is the emblem of the European digital model and may give "European-style" health innovation a comparative advantage.[46]

41. "Exposé de Paul Ribeyre à la conférence préparatoire à la Communauté européenne de la santé", Paris, December 12, 1952, in "Notes et documents concernant la Communauté européenne de la santé", *Notes et études documentaires*, March 18, 1953, No. 1718, série sociale XXV, p. 15.
42. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
43. GDPR, Article 4, para. 15.
44. A. Lazarègue, "Là où le RGPD a échoué, le droit de la concurrence peut encore gagner", *Le Monde*, June 14, 2019.
45. ALLEA, EASAC, and FEAM, "International Sharing of Personal Health Data for Research", April 2021.
46. L. Morlet and A. Templier, "Tribune: Notre cadre juridique est un rempart contre l'appétit des GAFA pour nos informations médicales", *Le Monde*, June 20, 2019.

It should be noted that the protective nature of the GDPR did not prevent anticipation of the issue of tackling public health crises through processing health data, as the legislation is flexible enough to implement data processing in relation to a pandemic: the prohibition on processing personal health data may be lifted when provided for in Union or Member State law, where it is in the public interest, in particular for the purposes of controlling communicable diseases and other serious threats to health.[47] Despite the practical difficulties raised by numerous organizations, the European approach had already integrated the need for continuity of data flows and the importance of international co-operation in relation to health data, with these exemptions permitting international data exchange between services responsible for public health, such as for the purposes of contact tracing for contagious diseases.[48]

In relation to non-personal health data, the EU has launched several initiatives designed to establish an economy based on sharing and co-operation: the regulation on the free flow of non-personal data in the European Union,[49] the regulation on cybersecurity,[50] and the Open Data Directive[51] have laid the foundations for a genuine European digital health market. In 2018, Regulation 2018/1807 was adopted with a view to facilitating the circulation of non-personal data, including health data. Through this regulation, the EU seeks to encourage the development of new health-related technological applications and industry dynamics in the Union.

The joint AI strategy published in 2018 sets out major investment in AI in health, with a view to making up European ground on the US and China, where the so-called "GAFAM" tech companies (Google, Amazon, Facebook, Apple, and Microsoft) and BATX (Baidu, Alibaba, Tencent, Xiaomi) are leading the way,[52] but also on the advances of Japan in relation to AI and medical robotics, South Korea, Canada, Israel, and Russia: advanced nations that have developed ambitious digital health investment strategies. In order to tailor these strategies specifically to health data, the European Commission has launched the construction of digital services

47. GDPR, recital 52.
48. GDPR, recital 112.
49. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union.
50. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
51. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-Use of Public Sector Information.
52. Chapel *et al.*, "La révolution du pilotage."

infrastructure (eHealth) to provide basic transborder services for electronic communication of medical procedures and patient profiles. In March 2017, the EU published the "European Interoperability Framework" for existing electronic health records, culminating in a recommendation in February 2019 concerning a European format of exchanging digitized health records, though this has by no means been adopted by all Member States.[53]

Finally, on February 19, 2020, a few days after the pandemic reached Europe, the European Commission presented its data strategy, which includes a specific section on health data. Aware of the continent's weaknesses in relation to co-operation and sharing health data, the Commission stated that "Strengthening and extending the use and re-use of health data is critical for innovation in the healthcare sector,"[54] notably with the objective of steering health care systems, increasing the competitiveness of European industry, and supporting the assessment of medical products.[55] This document walks a fine line between the EU's customary approach, based on the protection of fundamental liberties of health data—recalling that these must be processed in accordance with the GDPR, which accords health data special protection—and an affirmation of the economic importance of such data: "Health is an area where the EU can benefit from the data revolution, increasing the quality of healthcare, while decreasing costs."[56] Before the public health crisis broke out, the Commission was already aware of internal fragmentation within and between Member States, and a range of models of governance for data access, and the strategy unveiled in February sought to resolve these issues.

United States

Health data regulation offering fewer protections than in the EU

In the US, processing of health data is regulated by several dozen pieces of data protection regulations at both the federal and state level. The country does not currently have a global data protection regulation based on the European model: although plans to create such a regulation are often discussed, it only has sector-specific

53 . European Commission, "Electronic Cross-Border Health Services", available at: www.ec.europa.eu.
54. European Commission, "A European Strategy for Data", https://eur-lex.europa.eu.
55. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European Strategy for Data", February 2020.
56. European Commission, "A European Strategy for Data."

legislation.[57] From this regulatory whole we can identify an approach to data protection—including that of health data—that differs from the European approach. In Europe, personal health data protection is associated with a fundamental right, but in the US it is primarily an issue of whether or not these data are of a commercial nature. While some data—such as data collected by hospitals—benefit from greater protection, private companies are free to exploit them as long as they do not engage in "unfair practices."[58]

The first major law concerning personal data protection, the 1974 Privacy Act, applied to processing of data by the federal government, and implemented the Fair Information Practices developed by the US Department of Health, Education and Welfare in 1973. In line with the 1974 Privacy Act, the federal legislator developed a series of laws designed to protect personal data in the private sector, including the 1996 Health Insurance Portability and Accountability Act (HIPAA), which remains the main framework for health data protection. The HIPAA requires health care organizations to implement detailed technical and organizational security measures, to disclose to patients how their data will be processed, and to obtain their consent in certain narrowly defined situations.

The HIPAA applies to various entities including hospitals, health care providers, and their billing service providers. Its rule of confidentiality regulates the use of protected health information (PHI)—defined as any information held by a covered entity about health status, provision of health care, or payment for health care that can be linked to a specific individual. Disclosure of such information requires express written patient approval, with a few exceptions for specific circumstances, such as where there is a legal obligation to disclose or where disclosure enables the receiving entity to help the disclosing entity fulfill its care functions. It is generally on these legal grounds that hospitals are able to share patient information, without obtaining their consent, to private entities such as the GAFAM.

The HIPAA was extended by the Obama administration with two pieces of legislation concerning health data. In 2009, Congress adopted the Health Information Technology for Economic and Clinical Health (HITECH) Act, which extended the scope of the HIPAA requirements in relation to data protection, including by prohibiting the sale of protected information without patient consent

57. Such as the 1998 Children's Online Privacy Protection Act (COPPA) and the 2003 Fair and Accurate Credit Transactions Act (FACTA).
58. W. J. Maxwell, "La protection des données à caractère personnel aux États-Unis: Convergences et divergences avec l'approche européenne", in B. Fauvarque-Cosson and C. Zolynski (eds.), *Le Cloud computing. L'informatique en nuage*, Paris: Société de législation comparée, 2014.

under certain circumstances.[59] In 2013, the Genetic Information Nondiscrimination Act (GINA) prohibited the commercial use of genetic data held by health and insurance companies. Extending the data protection requirements of the HIPAA was thus a way of mitigating the risks linked to new e-health technologies, which have made vast quantities of new medical information available online. In addition to these federal laws, all US states have adopted laws to protect certain aspects of the private lives of their citizens, such as the California Consumer Privacy Act (CCPA), which came into force on January 1, 2020, and is primarily based on the EU's GDPR, though does not go as far.

Finally, one of the main objectives of HITECH, which was accompanied by a $37 billion budget as part of the 2009 American Recovery Act designed to incentivize digitization of the medical sector, was to promote significant utilization of certified electronic health records in the US. Six years after the law was adopted in 2015, dramatic progress has undoubtedly been made: 96% of hospitals and 78% of physicians now use a certified electronic health record technology, compared to 10% and 17% respectively when the law was passed.[60]

Fragmented data governance: an opportunity for the ambitions of the tech giants

In response to the fragmentation of the US health care system, numerous transformation projects designed to improve the co-ordination of actors have been instigated at the national level by both private and public actors. At the national level, the development of open health data, which has a long history in the US, was accelerated by the drivers implemented by the Obama administration. In the 1960s, the federal government decided to improve public access to data via the Freedom of Information Act, and from 2009 onward, following on from the Open Government Initiative launched by Barack Obama on the first day of his presidency, and the Affordable Care Act in 2010, the US Ministry of Health opened up access to new data that can be consulted on a dedicated website, "healthdata.gov."[61]

59. HITECH also increased the legal liability for cases of noncompliance and strengthened the enforcement rights of the Office of Civil Rights (OCR, a division of the Department of Health & Human Services). See P. Bailin, "Executive Summary: Evolution of Health Data Regulation", April 2, 2019, available at: https://medium.com.
60. Institut Montaigne, "E-santé: augmentons la dose", report, June 18, 2020.
61. "Panorama international de l'open data en santé: principaux enseignements", available at: www.departement-information-medicale.com.

In addition to this, several initiatives have emerged designed to create unified federal databases. In 2010, the "Blue Button" initiative brought together Veterans Affairs (VA) with the Department of Defense (DoD) and federal health insurers (Medicare and Medicaid), the three public institutions with the largest health databases in the country, enabling their users to download all data from their medical records.[62] During this period, Vice President Joe Biden strongly supported the National Cancer Institute, as part of the Cancer Moonshot initiative, in enabling a project involving supercomputers at the Department of Energy analyzing the medical data held by the VA for the purposes of cancer research. During Barack Obama's second term, $215 million were spent on the Precision Medicine Initiative, which aimed to create a huge database of genetic and other biological data from a million volunteers. In 2017, these efforts culminated in the launch of the "All of Us" program run by the National Institutes of Health (NIH), one of the world's biggest research programs in this area.[63]

Initiatives by the federal government have been unsuccessful in effectively unifying or joining up health databases in the US, which have low interoperability and are populated by numerous public and private aggregators.[64] In response to this fragmentation, several private actors have stepped into the breach with storage, co-ordination, and aggregation services. During the 2010s, the GAFAM thus entered the health data market by forming partnerships with hospital and clinic networks centered around their cloud-based solutions as a way of storing increasing volumes of data, combined with their expertise in AI to support medical actors with their research projects.[65] Project Nightingale, a partnership between the Ascension health system, Google, and numerous hospitals aimed for example to transfer the digitized information of millions of patients to Google Cloud.[66]

62. According to a French senior civil servant specializing in the digital sphere and health policy whom the authors interviewed in April 2021, the Blue Button initiative thus changed the philosophy of health data management by giving patients control over their data.
63. L. Determann, "Healthy Data Protection", *Michigan Technology Law Review*, Vol. 26, No. 2, 2020.
64. Institute of Medicine, *Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary*, Washington, D.C.: National Academies Press, 2010, available at: www.ncbi.nlm.nih.gov.
65. BearingPoint France, "Post COVID-19 : Comment la valorisation des données va-t-elle façonner la médecine de demain ?", 2020.
66. R. Copeland, "Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans", *The Wall Street Journal,* November 11, 2019.

In recent years, the GAFAM have also formed numerous partnerships with pharmaceutical companies including Novartis, Pfizer, and Sanofi,[67] enabling the latter to offer solutions that now go well beyond simply selling drugs (such as disease prevention, health care management, and post-treatment services), based on the collection and analysis of real-world data. The activities of the big tech companies in the sphere of health data also affect public actors: in 2019, instigated by Medicare, Apple, Google, and Microsoft joined a project to centralize US patient data. The GAFAM offered logistical support in creating a program interface into which all health care professionals can deposit their patient documents.[68]

In addition to these institutional partnerships, the ambition of the tech giants to gain a permanent foothold in the health data market has been facilitated by the rise of connected objects—such as smart watches and medical wristbands[69]—that can collect health data on a massive scale in real-time (along with any other personal data useful for matching purposes). With its acquisition of Fitbit, one of the world's leading companies in the sector, for €2.1 billion on January 14, 2021, Google has gained a foothold in this market, previously dominated by Apple (46.4% of the market) and Samsung (16% of the market).[70] A recent study based on an analysis of over 20,000 mobile apps showed that Google and Facebook are also the main data collectors through their intermediary, via their various publicity and tracking services directly integrated into these apps.[71]

67. Sanofi has developed the collaborative platform Darwin, which brings together a wide range of health data covering over 345 million patients, over 300 diseases, and 48 clinical trials.

68. A. Burgat, "Les GAFA s'immiscent dans les systèmes de santé publics", *Les Échos Entrepreneurs*, September 5, 2019.

69. The GAFAM are involved in many different projects in the health care sector. Alphabet, Google's parent company, has a subsidiary called Verily that works with various medical technology private companies and multiple pharmaceutical groups (including Novartis and Sanofi). Alphabet has set up various projects, including Project Baseline, which aims to "map human health"; Cityblock, which seeks to promote health prevention and education; and Calico, active in cancer prevention. Facebook has acquired Moves (specializing in physical activity monitoring) and Oculus, which operates in virtual reality. The platform also offers targeted advertising opportunities for pharmaceutical companies. Amazon, meanwhile, has launched Amazon Care, among other initiatives.

70. This acquisition raised concerns from the European data regulator, which stated on February 19, 2021: "There are concerns that the possible further combination and accumulation of sensitive personal data regarding people in Europe by a major tech company could entail a high level of risk to the fundamental rights to privacy and to the protection of personal data." (EDPB, "Statement on Privacy Implications of Mergers", February 19, 2020, available at: www.edpb.europa.eu). In relation to mobile data, although the EU initially supported the principle of regulation through a "Code of Conduct" developed by industry, rejected in 2018, the provisions of the GDPR concerning sensitive data now apply.

71. M. Ikram *et al.*, "Mobile Health and Privacy: Cross Sectional Study", *British Medical Journal*, Vol. 373, No. 1248, June 17, 2021. "For most of the 20,000 medical and health

Finally, the collection of unprecedented volumes of health data is enabling the big tech companies to position themselves in downstream segments with high added value. First, the new frontier of ambition for the GAFAM in relation to health data lies in their capacity to carry out high-level independent research and take a stake in the field of scientific knowledge: the "Research" app developed by Apple, for example, gives users the opportunity to take part in medical studies over several years by collecting data from their iPhone. Tim Cook, the company's CEO, has unhesitatingly claimed that "if you zoom out into the future, and you look back, and you ask the question, 'What was Apple's greatest contribution to mankind,' it will be about health."[72] On January 1, 2020, a study coauthored by Google (Alphabet) researchers and researchers from various US and UK cancer hospitals analyzed interpretation of a mammogram by an AI to screen for breast cancer.[73] This acceleration in the transformation of the health care landscape by the GAFAM, which are now making huge investment in health AI, is now provoking intense debate within international scientific bodies.[74]

Second, since 2015 the tech giants have significantly increased their investment in the insurance sector. This is particularly the case for Google, which invested $375 billion in the insurtech unicorn Oscar Health in August 2018 and further invested in 2019 in Clover Health, a health insurance solution based on predictive data analysis for offering health coverage targeting seniors. The other tech giants have followed suit: Apple has formed a partnership with Aetna, a US insurer that is developing personalized health insurance based on collection of Apple Watch data, and Amazon has invested in the Indian insurtech company Acko. These inroads made by the big tech actors into the insurance market, a cause for concern for the big companies in the sector,[75] is also a feature in China, where Ant Financial, a subsidiary of Alibaba and the largest fintech company in

and fitness apps analysed, we found that most can collect and potentially share data with third parties, including advertising and tracking services [...]. The analysis also revealed that mHealth apps were far from transparent when dealing with user data, with only about half being compliant with their declared privacy policies (if available at all)."

72. Interview on January 9, 2019 with Jim Cramer of CNBC: L. Feiner, "Apple CEO Tim Cook Speaks with CNBC's Jim Cramer: Full Transcript", January 8, 2019, available at: www.cnbc.com.

73. S. M. McKinney *et al.*, "International Evaluation of an AI System for Breast Cancer Screening", *Nature*, Vol. 577, 2020, pp. 89–94.

74. According to Pierre Corvol, a physician and biology researcher and former administrator of the Collège de France, "The use of AI in corollary with data collection is now a sufficiently major and evolving topic to require regular updates between the different science academies in the G7": cited in L. Belot, "Les données de santé, un trésor mondialement convoité", *Le Monde*, March 2, 2020.

75. D. Cuny, "Le digital et les Gafa, premier risque pour les assureurs", *La Tribune*, October 29, 2018.

the world, bought the insurer Cathay Insurance China in 2015 and has invested in the online insurance giant ZhongAn, valued at €10 billion.

China

Enhanced control over data in order to accelerate digitization of the medical system

China's earliest legislation concerning digital health dates back to 2014,[76] but it was the 2017 Cybersecurity Law[77] that first unified the legal regime applying to personal data, with the primary objective of securing the Chinese informational and digital space. Under this law, health data are considered sensitive data that cannot be stored outside the country and can be transferred abroad only with the consent of their owner, unless this is prohibited for a compelling reason related to security or Chinese economic interests. To ensure compliance with this requirement, the "Multi-Level Protection Scheme"[78] (the "MPLS") requires certain operators of vital interest to implement stricter protective norms if potential data violations represent a serious risk to national security. Under current regulation, platforms handling health data are classified as level 3 (on a scale of 1 to 5, from low risk to high risk), which requires them to prevent security incidents throughout the supply chain, from data production to data storage. Although participation in the MPLS is voluntary, implicit pressure on companies to opt in seems to have drastically increased since 2019.[79] App-based digital health services, which require huge volumes of data to operate, are further governed by two types of regulation: medical devices regulation, and general app regulation—neither of which is specific to telehealth companies.

Alongside this new regulation, since the mid-2000s the Chinese regime has pushed forward the development of a forced market in e-health, in particular with the desire to improve coverage of the country's vast rural areas, with significant involvement from the major tech companies in supporting the government's efforts. The "Healthy China 2030" plan, launched in October 2016 by the Central Committee of the Communist Party and the State Council and described by the World Health Organization as "the biggest health

76. Population Health Information Management Measures, May 2014.
77. Cybersecurity Law of the People's Republic of China, June 1, 2017. English translation available at: www.newamerica.org.
78. The Multi-Level Protection Scheme (MLPS) is discussed in H. Feldshuh and L. Yau, "The Growing Intersection of Digital Health and Data Processing in China", *China Business Review*, April 12, 2021.
79. *Ibid.*

system reform the world has seen"[80] aims among other things to significantly develop the e-health market, the interoperability of databases in a highly regionalized system, and to centralize public health and medical "big data," including through four dedicated national health "big data" centers in Fuzhou, Xiamen, Changzhou, and Nanjiang (where the National Health and Medicine Big Data Center is set to store genetic information for several million Chinese citizens in order to develop cutting-edge applications).

In 2016, China also launched its "National Precision Medicine Plan," investing 60 billion yen (€9.3 billion) in genetic sequencing projects and building dedicated databases. In April 2018,[81] the State Council published its opinions on the promotion of digital development in the health sector, requiring regional governments to increase their co-ordination in order to facilitate the implementation of the Joint National Health Information Platform. This will be gradually connected to the National Scientific Data Sharing Platform, which already includes data for 600 million people (half the Chinese population), derived from the national health insurance system. In the same vein, in July and September 2018 the National Health Commission announced a series of measures designed to ensure that all types of medical facilities at all levels are connected to the national regional health information platforms, transmit and safeguard the data generated during health procedures, and provide monitoring access to administrative health departments.[82]

Surveillance capitalism with an international outlook

For nearly fifteen years, the Chinese regime has pursued a strategy of "structured cohabitation" between the public and private sectors in the health care sphere, with the dual objectives of increasing access to basic care for all, and implementing a health care system that can compete with the best internationally.[83] The major tech companies, including BATX, thus work closely with the Party, local authorities, physicians, and private insurers. Since 2019, 450,000 Chinese physicians have for example signed up to Trusted Doctor, a start-up created in 2018 and bought by Tencent, which brings together physicians and patients, but also clinics and hospitals. Alibaba Health

80. World Health Organization, "Health Promotion", available at: www.who.int.
81. A. Zhou and C. Huang, "Cybersecurity and Data Protection in Chinese Healthcare Industry", *Global Law Office* and *Practical Law China*, November 2020.
82. Public Health and Medical Big Data Measures of 2018, articles 4 and 38, discussed in Zhou and Huang, "Cybersecurity and Data Protection."
83. J. D. Séval, "Santé et numérique: 'L'ambition de la Chine est de mettre en place une offre globale et intégrée'", *Le Monde*, November 26, 2019.

Information Technology has developed the country's largest online pharmacy service. LinkDoc, which was valued at $1 billion just four years after its creation,[84] uses databases produced by health actors in order to train algorithms in cancer treatment. Since 2016, WuXi NextCODE (derived from the acquisition of a US Company by a Chinese actor) and Huawei have positioned themselves to develop the cloud infrastructure required to store the vast quantities of data created by the Chinese system and to develop the corresponding computational power.

The large-scale investment from Alibaba, Baidu, Tencent, and Huawei in health technologies, particularly in analysis and "big data," has however exacerbated the divide in the Chinese health system between a poorly performing public sector and private actors who hold the critical masses of data to keep themselves at the cutting edge of technology. It also raises the issue of the growing hybridization between public health and police uses of the databases that have been created, particularly in view of campaigns to collect genetic material that target ethnic minorities or allow for increased surveillance of political opponents.[85]

Since 2014, the Chinese health care system's hunger for data has also resulted in an exponential increase in investment by Chinese companies and parapublic actors in the foreign health technology sector. According to a 2019 report by the US-China Economic and Security Review Commission[86]—created by the US Congress to assess the national security implications of trade and economic relations between the US and China—Chinese foreign direct investment in biotechnology grew from $100 million in 2014 to $1.5 billion in 2015, then to just over $3.5 billion in 2017. That same year, venture capital funding totaled $3.8 billion. The report highlights that since 2018, the health technology and biotechnology sector has become the leading area of investment for Chinese companies in the US. With twenty-three companies linked to China having access to databases containing health data of the most sensitive nature (including genetic sequences), the report's authors state that "China's efforts to acquire US health data combined with limited data protections by the US raise questions about national security."[87] The GDPR is explicitly

84. F. Le Deu, "8 Reasons Why China is the Most Exciting Healthcare Story in the World Right Now", McKinsey & Company, November 16, 2018, cited in "L'Industrie pharmaceutique en Chine, Étude de l'évolution des acteurs privés et publics pour faire face aux nouveaux défis de la Chine du XXIème siècle", *Mines ParisTech*, 2018/2019.
85. S.-L. Wee, "China Is Collecting DNA from Tens of Millions of Men and Boys, Using U.S. Equipment", *The New York Times,* July 30, 2020.
86 . U.S.-China Economic and Security Review Commission, "China's Biotechnology Development: The Role of U.S. and Other Foreign Engagement", February 14, 2019.
87. *Ibid*.

cited in the report as providing European citizens with greater protection from the potentially predatory designs of Chinese actors.

In support of the internationalization of Chinese actors, the authorities now view digital diplomacy as a key issue, particularly in terms of standardization, so much so that "co-operation on harmonizing data protection rules has become one of the main topics of discussion for Chinese diplomats in international organizations."[88] The harmonization of technical standards in relation to making medical products and services secure is also one of the strands of its Digital Silk Roads initiative.[89]

88. R. Creemers, "Comment la Chine projette de devenir une cyber-puissance", *Hérodote,* Vol. 177–178, No. 2–3, 2020, pp. 297–311.
89. J. Seaman, "China and the New Geopolitics of Technical Standardization", *Notes de l'Ifri*, Ifri, January 2020.

Lessons learned from the public health crisis: Health data as a battleground for power struggles in the COVID-19 era

The European Union

The failure to develop a pan-European contact tracing app

On the background of the public health crisis, the issue of health data coalesced at the European level around the difficulties experienced by EU Member States in co-operating on joint deployment of a contact tracing app: an episode that revealed the political sensitivity of the issue of health data and the differences in approach between the Member States.

On April 21, 2020, the European Data Protection Board (EDPB) published a set of guidelines on the use of location data and contact tracing tools setting out a harmonized European vision: use based on individual consent, Bluetooth technology, and the use of pseudonymized personal data.[90] There appeared to be broad agreement among Member States regarding the deployment of contact tracing apps and the use of Bluetooth, without using geolocation tools. However, the EU rapidly came up against the problem of how to store the data of "contact cases" collected by the apps.

Two alternative data storage methods quickly emerged: a "centralized" approach in which data would be stored on a third-party server controlled by the state, and a "decentralized" approach in which data would be stored directly on the app user's phone. With the announcement of an unprecedented partnership between Apple and Google to develop contact tracing technologies, deciding between

90. European Data Protection Board, "Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak", April 21, 2020.

these alternatives became a strategic issue for the Member States. On April 10, 2020, Apple and Google announced the joint creation of the "Exposure Notification" application programming interface (API), offering a technological basis to develop contact tracing apps for all mobile phones run on Apple or Google software.

This decentralized software solution, based on Bluetooth technology, accelerated the collapse of the Pan-European approach. France and the main French body for digital sovereignty, the Institut national de recherche en informatique et en automatique (INRIA) (French National Institute for Research in Digital Science and Technology) supported a centralized approach in conjunction with Germany,[91] which had a two-month head start on development, and had agreed to a joint testing approach with its neighbor.[92] The German government initially favored a centralized app developed by a consortium of European and national actors,[93] including the prestigious Fraunhofer Institute (specializing in basic research) and Robert Koch Institute (specializing in disease control and prevention). However, this centralized solution provoked fierce opposition in political circles, from a number of NGOs, and from some academics.[94] Their criticism centered on the storage of data on a central server, which in their view represented a major threat to public freedoms, by creating the conditions for mass state surveillance of the German population. In reaction to this criticism, which risked compromising public support for the very principle of a digital app to combat the COVID-19 pandemic, the German government abandoned the project and followed the majority of EU Member States in opting for the decentralized solution jointly developed by Apple and Google.

The debate provoked in Germany by the development of a centralized tracing app reveals the conceptual divisions between European countries on the issue of health data: focused on the risks of state surveillance, it sidelined the debate about the risks of developing such apps based on a technological platform developed by non-European private actors, which was widely held in France. By opposing a system based on central servers, controlled by their national governments, the project's opponents thus paradoxically

91. The basis for the ROBERT (ROBust and privacy-presERving proximity Tracing) protocol, ultimately used in France.
92. Interview by the authors with Claude Castelluccia, Director of Research in Science and Digital Technologies at INRIA, April 2021.
93. The "Pan-European Privacy-Preserving Proximity Tracing" (PEPP-PT) program.
94. An open letter was sent by 300 researchers from 26 countries asking governments to opt for the decentralized solution developed by Apple and Google in order to "increase trust": see A. Hern, "Digital Contact Tracing Will Fail Unless Privacy Is Respected, Experts Warn", *The Guardian,* April 20, 2020.

strengthened the monopoly of the US tech giants over digital tracing in over twenty countries around the world. This situation reflects the lack of a European tech actor of critical size able to play on even terms with the GAFAM, which the EU cannot compensate for solely through the size of its market or the influence of its normative power.

A French debate on a European issue: the storage of health data in France

The public health crisis has also revealed the shortcomings of the European industrial model in relation to the storage of health data. In France, this debate has centered around the issue of the "Health Data Hub" (HDH) and its approved storage provider and "health data host," the US company Microsoft Azure. [95] The pandemic has considerably accelerated the implementation of the HDH project, with a decree on April 21, 2020 permitting it to process numerous categories of data "for the sole purposes of facilitating the use of health data for the needs of managing the public health emergency and improving knowledge of the COVID-19 virus."[96] As such, the HDH was able to centralize and match data from mobile health apps, telemedicine, the SNDS, pharmaceutical companies, and pharmacies.

The decision to use a US storage provider provoked a fierce public debate in France, in particular due to the fact that Microsoft, as a US company, might be subject to US legislation such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act. This federal law, which came into effect on March 23, 2018, allows the US government to requisition access to data held by US cloud storage providers, including when these data are physically stored outside the US. Concern grew with the "Schrems II" ruling of July 16, 2020 from the Court of Justice of the European Union (CJEU),[97] which declared Privacy Shield, the data transfer agreement between the EU and US, invalid on the grounds that the surveillance exercised by the US intelligence services on the personal data of European citizens was excessive, with insufficient oversight, and no real actionable rights in opposition. The Court thus ruled that transfers of personal data from the EU to the US contravened the GDPR and the EU Charter of Fundamental Rights, unless additional measures had recently been

95. Interviews conducted by the authors with a senior civil servant from the Ministry of Health and a lawyer specializing in life sciences highlighted that Microsoft was the only entity to offer all the functionality required for the deployment of the HDH.
96. *Arrêté du 21 avril 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire*.
97. Judgement of the Court of Justice of the European Union, in the proceedings of Data Protection Commissioner/Maximillian Schrems and Facebook Ireland, July 16, 2020.

implemented or the transfers were justified on the grounds of article 49 of the GDPR, which allows for exceptions in specific situations.

Due to the sensitivity and volume of the data to be hosted by the HDH, requiring the highest level of technical but also legal protection, including from direct access by the authorities of a third country, the CNIL expressed a desire for its hosting and management services to be restricted to companies based exclusively in EU jurisdictions.[98] Asked to rule on the issue by several online public liberties organizations, the Conseil d'État published a ruling on October 13, 2020 recognizing the existence of a risk of data derived from the HDH being transferred to the US due to Microsoft being subject to US law, and asking for additional guarantees to be put in place.[99] The health minister committed to use of a technological solution that would mean the data hosted by the HDH were not exposed to any access requests of an illegal nature under the GDPR, within a period of 12 to 18 months. On the basis of this information, the CNIL approved four new pilot HDH projects.

The HDH, whose development has been accelerated by the public health crisis, has therefore revealed the vulnerabilities of the French and European approach to health technologies, including the challenges to producing an alternative to US cloud actors in order to ensure a level of service that meets the expectations of governments, professionals, and patients. It also exposes the flaws of the normative European model, based on the GDPR, due to the continent's lack of its own industrial powerhouse, and its dependency on actors subject to the US CLOUD Act: in France, the recent dispute about the hosting by Amazon Web Services of data collected by Doctolib during the public health crisis has again raised the question of the relationship between the two normative systems.[100]

The European "trusted cloud" project Gaia-X,[101] launched on June 4, 2020 by the French and German economic ministers, does however demonstrate a real ambition to better secure health data, with the objective of bringing together the twenty-six national digital

98. CNIL, "La Plateforme des données de santé (Health Data Hub)", February 9, 2021.
99. Conseil d'État, ruling of October 13, 2020, "Association Le conseil national du logiciel libre et autres", No. 444937.
100. The Conseil d'État judge in chambers ruled that personal data hosted by Doctolib in relation to COVID-19 vaccination are sufficiently protected despite the choice of Amazon to host them. This decision was based in particular on the implementation of an encryption procedure based on a trusted third party located in France, and the fact that the two companies have signed a contract addendum making it possible to oppose US government control over French patient information (Conseil d'État, ruling of March 12, 2021, "Société Interhop et autres", No. 450163).
101. This project, based on collaboration between over twenty French and German companies, including OVHcloud and T-Systems, seeks to build a reliable and secure European data infrastructure.

health spaces involved at the European level.[102] In France, the National Cloud Strategy, unveiled on May 17, 2021,[103] sets out new ambitions to combine competitiveness and sovereignty, by advocating the use of US technologies, under license, by EU companies, in order to avoid the application of US law; by strengthening ANSSI "SecNumCloud" certification (held for example by OVHcloud and 3DS Outscale); and by investing €107 million through the Plan France Relance in innovative French cloud-based projects. Following these announcements, Capgemini and Orange launched "Bleu," a trusted cloud solution based on a license agreement with Microsoft, in order to meet the dual requirements of high level of service and the security of data hosted by the HDH. Microsoft, meanwhile, has committed to the data of European companies and public services remaining in Europe.[104]

Prospects for greater European co-operation on health data

In its Communication of February 2020 on a European data strategy, the European Commission made a commitment to supporting the creation of a Common European Health Data Space, one of nine "data spaces" defined by the strategy. The COVID-19 pandemic has revealed the desperate need for co-operation and productive discussions about data in the EU in order to develop an effective political response to this type of immediate global threat.[105]

In response to the heterogeneity and lack of interoperability of health databases in Europe, which have limited the opportunities for truly co-ordinated action at the European level, the project of creating a European Health Data Space has been accelerated by the crisis. On November 11, 2020, the European Commission declared its desire for greater co-operation in terms of health care, research, and health policy development in Europe.[106] In its view, the first pillar of this consists of a solid system of data governance and sharing rules: in the eyes of the Commission, the COVID-19 crisis has legitimized the

102. C. Treilles, "Gaia-X: Le hub français invite les volontaires à rejoindre ses rangs", ZDNet, January 25, 2021, available at: www.zdnet.fr. See A. Pannier, "The Changing Landscape of European Cloud Computing: Gaia-X, the French National Strategy, and EU Plans", Ifri, *Briefings de l'Ifri*, July 2021.
103. "Stratégie nationale pour le cloud" press release, May 17, 2021, available at: www.numerique.gouv.fr.
104. L. Barthélémy, "Où sont les données? Microsoft tente de répondre aux inquiétudes européennes", AFP, May 27, 2021.
105. N. Iacob and F. Simonelli, "Towards a European Health Data Ecosystem", *European Journal of Risk Regulation*, Vol. 11, No. 4, 2020, pp. 884–893.
106. European Commission, "Building a European Health Union: Stronger Crisis Preparedness and Response for Europe", November 11, 2020.

European approach to health data, which must be collected and analyzed in a responsible manner to effectively combat the pandemic, at the risk of undermining privacy and public trust. In relation to this latter, the Commission seems to have taken the public debate provoked by contact tracing apps very seriously, and wants to build an atmosphere of trust, even if it means putting the brakes on the creation of a European health space.

The Commission also believes that in order to fully exploit the potential of health data exchanges, it is essential to ensure their quality and to ensure that the various sources of health data (such as electronic medical records, different registries, various computing and digital tools) can "talk" to one another. This requires technical and semantic interoperability between the different IT systems, and new infrastructure allowing for links between the databases, the eHealth Digital Service Infrastructure (eHDSI) for the portability of patient medical records, set to be deployed from 2025 in EU countries, and Cross Border eHealth Information Services (CBeHIS) for data exchanges between public institutions. [107] Finally, the Commission has set out the criteria for its protocol for data concerning health, which must be "findable, accessible, interoperable, and reusable" (FAIR).

In addition to the gradual establishment of a European Health Data Space, the next challenge for Europe lies in the effective introduction of an EU health passport, approved on April 29, 2021 and adopted on June 9, 2021 by the European Parliament in the form of an "EU Digital COVID Certificate," facilitating movement within the Union. This document, in paper or digital form, will constitute proof that an individual has been vaccinated against coronavirus or has recently received a negative test result or recovered from the infection.[108] Regarding the technical infrastructure, a "gateway" to verify certificates "in a secure and privacy-friendly way"[109] has been set up by the Commission at the EU level. As of June 21, 2021, sixteen EU countries had opted to connect to the gateway.[110]

107. European Commission, "European Health Data Space", available at: https://ec.europa.eu.
108. European Parliament, "EU COVID-19 Certificate Must Facilitate Free Movement Without Discrimination", April 29, 2021.
109. European Commission, "EU Digital COVID Certificate: EU Gateway Goes Live with seven Countries One Month Ahead of Deadline", available at: https://ec.europa.eu.
110. Further information and the list of connected countries is available from a dedicated website: European Commission, "EU Digital COVID Certificate", available at: https://ec.europa.eu.

United States

The failings of technological management of the public health crisis

The pandemic has revealed the failings of the US public health data collection and processing system. The US Centers for Disease Control and Prevention (CDC) have typically used a monitoring system with data flowing from a local level up to the federal level to monitor the spread of epidemics. This method is effective in smaller scale epidemics such as salmonellosis, which periodically affects US states, but in the context of the pandemic encountered numerous difficulties with gaps in the data being fed upward and a pace of analysis too slow to keep up with the spread of the virus.[111]

In response to these failings, the Trump administration decided to sideline the CDC in processing data on COVID cases and hospitalizations, in favor of an ad hoc system under direct control of the Department of Health and Human Services. The infrastructure for this system was operated by two companies with close ties to the president, TeleTracking and Palantir, based on over 200 datasets from three-quarters of the country's 8,000 hospitals. According to Georges Benjamin, director of the American Public Health Association in Washington, DC, rather than rationalizing the collection of health data during the crisis, this change disrupted collection still further, as many hospital administrators no longer knew which agencies they should contact, and due to difficulties linked to obsolete methods of data sharing (such as by fax).[112] In a report published back on September 25, 2019,[113] the Council of State and Territorial Epidemiologists noted the slow and fragmented nature of the US health data system as primarily manual and paper-based: although the federal government spent several billion dollars in the early 2010s to encourage private physicians to replace their fax machines with electronic records,[114] the HITECH Act included no such funding for public hospitals and clinics. The lack of a tool for rapid collection and sharing of health data with the public health

111. In addition to these technical problems, the slowness of the system can also be partly attributed to information being withheld by figures in the Trump administration as the November elections approached. See for example N. Weixel, "Clyburn: Documents Show Trump Officials Helped Suppress Coronavirus CDC Reports", *The Hill,* April 9, 2021.
112. "Editorial: The Trump Administration Must Stop Sidelining the CDC", *Nature* Vol. 583, No. 660, 2020.
113. Beaumont Foundation, "White Paper: Driving Public Health in the Fast Lane", CSTE, September 25, 2019.
114. S. Kliff and M. Sanger-Katz, "Bottleneck for U.S. Coronavirus Response: The Fax Machine", *The New York Times,* July 13, 2020.

authorities thus created difficulties for steering handling of the pandemic and the early vaccination campaign.

In terms of contact tracing apps, the federal government has remained relatively quiet about the development of a national app, and has largely relied on the solution developed by Apple and Google. Some states capitalized on this and moved to local solutions prior to the release of the API by the two tech companies in mid-May, with scattered results. With the help of local companies, North Dakota, South Dakota, and Utah thus developed their own contact tracing apps that were centralized, based on GPS and Bluetooth, and used to support manual contact tracing.[115] In general terms, the reluctance about contact tracing apps expressed by Americans in surveys (around 3 in 5 Americans reported that they could not or would not want to use one)[116] and the lack of impetus at the federal level has resulted in the states turning to sometimes huge human resources (California has relied on 10,000 volunteers) as a more effective and politically less costly solution.

With the involvement of Google and Apple in contact tracing, and Palantir in developing health databases, the US tech giants have succeeded in imposing the image of their responsive online services compared to slow or lacking public systems. They have thus seized the opportunity of the pandemic to "change the way they are perceived by the general public and by political leaders," in the view of William Kovacic, a former commissioner of the US Federal Trade Commission and a law professor at Georgetown, in Washington, D.C.[117] These new public–private partnerships have however raised several concerns about the desire of tech companies to present themselves as the default partners for governments that want to digitize access to health services for their citizens, and to do so on their own terms.[118]

Moves toward convergence with the European model under President Biden

Due to his strong and long-standing commitment to cancer research, first via the Cancer Moonshot initiative and then the Biden Cancer Initiative (see above), the new US president has long had a very clear view of his country's health data problem. In a key opinion piece

115. E. Setzer, "Contact-Tracing Apps in the United States", Lawfare blog, May 6, 2020.
116. C. Timberg, D. Harwell, and A. Safarpour, "Most Americans Are Not Willing or Able to Use an App Tracking Coronavirus Infections: That's a Problem for Big Tech's Plan to Slow the Pandemic", *The Washington Post,* April 29, 2020.
117. A. Piquard, "La crise du coronavirus va-t-elle améliorer l'image des GAFA?" *Le Monde,* April 10, 2020.
118. F. Guerrini, "The Dark Side of the Apple and Google Collaboration Against COVID-19", Forbes.com, April 13, 2020.

published on March 19, 2018,[119] Joe Biden set out his view of the obstacles and required reforms in this area. In this article, he notes that in the wake of the measures adopted under Obama's terms in office, the medical industry did not seize the opportunity to encourage database interoperability and give patients control over their data. From this, he deduces the need for the government to intervene in the health data sphere. He thus proposes the idea of requiring health care providers to provide patients with their full up-to-date medical records within 24 hours of a request, or be subject to criminal sanctions; of creating a single portal under the leadership of the Center for Medicare and Medicaid Innovation making it possible to store, read, and exchange the data of insured patients in a uniform manner; and to strengthen the Sync for Science (S4S) partnership between the Department of Health and Human Services and private health database aggregators (electronic health record (EHR) vendors)[120] in order to improve research access to these resources.

On January 21, 2021—his first day in office as president—Joe Biden sought to build on the lessons learned from the Trump administration's management of the pandemic by signing an executive order designed to ensure a "data-driven" response to COVID-19 and to future high-consequence threats to public health.[121] Among other measures, the executive order emphasizes making the data held by the federal government open to the public in usable and readable formats. The order also makes the Secretary of Health, in consultation with the agencies concerned, responsible for assessing the effectiveness, interoperability, and connectivity of the federal public health data systems, bringing an end to the overlapping mandates cultivated by the Trump administration. Finally, the order puts in place the foundations for advancing innovation in public health data in the US, which is set to receive huge funding as part of the relief plan.[122] President Biden has proposed injecting $8.7 billion in funding into the CDC in order to modernize the collection of public health data at the national level, and support the improvement of core public health capacity in the states.

Finally, the Biden presidency is likely to be characterized by renewed debate about a major federal law regarding personal data protection, following the European model. Vice President Kamala Harris took an interest in this during her term as Californian senator,

119. J. Biden, "Joe Biden: To Save and Improve Lives Using Data, Details Matter", Forbes.com, March 19, 2018.
120. Such as Allscripts, Cerner, eClinicalWorks, Epic, and others.
121. "Executive Order on Ensuring a Data-Driven Response to COVID-19 and Future High-Consequence Public Health Threats", The White House, January 21, 2021.
122. For further information, see Letter to the Honorable Patrick Leahy, April 9, 2021, www.whitehouse.gov.

and supported a bill proposed by Elizabeth Warren to amend the HIPAA in order to increase protection of health data in the context of the COVID-19 pandemic. She was backed in this by the left wing of the Democratic party, which has also produced several proposals in this area. In 2020, two bills were also introduced, one by the Republicans in the Senate[123] and the other by the Democrats in the House,[124] designed to improve data protection, based on broad bipartisan consensus, particularly in relation to making health data a sensitive data category to receive special protection, with the exception of notable disagreement on the role of local state regulations. This domestic debate has diplomatic implications for transatlantic relations: with the CJEU's invalidation of the Privacy Shield (see above), even a slight shift in US law toward the European GDPR, in particular by modification of some of its most intrusive provisions,[125] might enable the new US administration to give assurances to its European allies, burned by four years of the Trump presidency.

China

The management of the public health crisis strengthened the influence of BATX in Chinese surveillance capitalism

The COVID-19 pandemic has strengthened the control of the Chinese Center for Disease Control and Prevention (CCDC), a government institution responsible for technical management of disease control and public health, over health actors. By connecting the CCDC's monitoring and early warning system to the hospital electronic medical records management system, the CCDC was able to monitor in real-time the computers of front-line physicians to prompt them to check the accuracy of the information provided by patients.[126] The CCDC monitoring system was thus able to reduce the mean time required for physicians to report a case of COVID-19 from 5 to 8 minutes to 40 seconds, and the time required to submit a report through the CDC infectious diseases reporting system from 2 to 3 minutes to a few seconds.[127]

123. S.3663 – COVID-19 Consumer Data Protection Act of 2020.
124. H.R.6866 – Public Health Emergency Privacy Act.
125. Article 702 of the Foreign Intelligence Surveillance Act and Executive Order no. 12333.
126. J. Wu *et al.*, "Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations", *Journal of Medical Internet Research*, Vol. 22, No. 10, 2020.
127. J. Y. Shuangshuo Technology, cited in Wu *et al.*, "Application of Big Data Technology."

The Chinese regime has also made extensive use of public and private databases in the fight against COVID-19. Most notably, China monitored population movements and applied strict restrictions to cases of infection. Wu Zunyou, an official expert in epidemiology at the National Center for Epidemic Prevention and Control, reports having had access to and using numerous data sources to monitor movements—with the help of China Railway, the Chinese rail company—and to locate sick people: "With big data, we know where the five million people who left Wuhan and Hubei province went. We can capture precise location data and track these people."[128]

The Chinese tech giants have worked alongside the regime to process the vast quantities of information available. A digital epidemic prevention system, for example, jointly developed by Alipay, Dingding, and Alibaba Cloud,[129] made it possible to analyze the medical data for cases diagnosed in every hospital in the country, and to identify patients who had bought drugs to treat fever from a pharmacy in the previous month. Using the data gathered, these companies were able to model the spread of the epidemic by geographic region and to identify the main sources of outbreaks, such as the Baodi and Tulong shopping malls, and the hospital in Tianjin. BATX have also been involved in setting up the various public health QR code systems used by the majority of Chinese provinces and cities, operated by Alibaba (Alipay), Tencent (WeChat), and Baidu, among others. Since late February 2020, Alibaba has hosted the apps for over 200 large communities, compared to over 300 hosted by Tencent.[130] Most of these apps required users to provide biometric data, if not facial recognition registration (for example in Beijing). They all worked in a similar way, displaying a color code (green, yellow, or red) that could be read using an individual QR code, based on information including the individual's travel history and health status. This code determined whether the user had to self-isolate for fourteen or seven days, and whether they had access to certain sectors or services.

While the central government initially allowed these local initiatives to develop, the incompatibility between certain apps caused issues as the country gradually opened back up. Rather than develop a national app, in spring 2020 the authorities therefore embarked on the creation of a national database enabling sharing of the data gathered by local apps, thus favoring their interoperability and the

128. D. André, "La Chine utilise les données personnelles pour lutter contre le coronavirus", Interview with France Inter, January 31, 2020.
129. Wu *et al.*, "Application of Big Data Technology."
130. N. Gan and D. Culver, "China is Fighting the Coronavirus with a Digital QR Code: Here's How it Works", CNN, April 16, 2020.

regaining of control by central government. While this tracking system has been at the heart of the Chinese crisis management "narrative," analysts have widely questioned its true effectiveness,[131] and the reality appears to be closer to the European tracing systems, based on a huge number of human agents in order to contact suspected cases by phone and obtain robust data, in order to compensate for the lack of granular data in health QR codes.

Signs of the regime regaining control over BATX

In response to the omnipresence of BATX in the management of the pandemic, the relationship between the government and the big tech companies seems to have shifted toward restricting the latter's room for maneuver. This renewal of tensions in the wake of the COVID-19 crisis was notably visible in the hardening of antitrust regulation in late 2020, which required Alibaba to pay a fine of $2.3 billion in November 2020, and of stock market regulation, which led to the blocking of the $34 billion flotation of Ant Group, Alibaba's online payment subsidiary.[132] Similarly, the Chinese digital regulator, the Cyberspace Administration of China (CAC), recently cracked down on thirty-three mobile apps, including several run by Alibaba, Baidu, and Tencent, for having collected more data on their users than it judged to be necessary to provide their service. On May 10, 2021, a further eighty-four apps were targeted.[133]

The desire of the Chinese government to restrict the latitude of the big tech companies was also reflected in October 2020 by the introduction of a new bill on the protection of personal information (PIPL), with a new version published in late April 2021,[134] which seeks to unify data regulation in a stricter manner than the Cybersecurity Law of 2017.[135] Partly inspired by the GDPR, with which it shares certain extraterritorial effects (on the protection of the data of Chinese citizens held abroad), the PIPL classifies personal health data as sensitive data (article 29 of the latest version of the bill) and should in theory give patients greater protection from private actors than they have under US law. In reaction to the major role played by big tech companies in managing the pandemic, and a certain form of

131. Interview by the authors with a political science and sinology researcher, April 2021.
132. Bloomberg Business, "What Is Behind China's Crackdown on Its Tech Giants: QuickTake", November 13, 2020, available at: www.bloomberg.com.
133. S. Sharwood, "Beijing Twirls Ban-Hammer at 84 More Apps it Says Need to Stop Slurping Excess Data", *The Register*, May 12, 2021, available at: www.theregister.com.
134. "Translation: Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft)", DigiChina, available at: https://digichina.stanford.edu.
135. X. Fu-Bourgne, "Un nouveau projet de loi publié en Chine", *Expertise*, No. 467, April 2021.

social demand for giving citizens greater power of consent in relation to their data, the Chinese government seems bent on increased oversight of the country's digital economy, and regaining control over its main actors.[136]

136. AFP, "La Chine met au pas ses géants du numérique", March 22, 2021.

Conclusion: The need to make Europe a power in digital health following the public health crisis

The geopolitics of health data, which have been deeply reconfigured by the COVID-19 pandemic, complicate the observation in February 2018 by the French Cyberdefense Strategic Review of a "fundamental opposition" between the Western conception of cyberspace and those of Russia and China. This study has attempted to show that within the West itself, the models of governance and set of values concerning the issue of health data are subject to friction and power relations, due to the specific characteristics of such data in the typology of the digital world.

Conversely, mutual influences and greater alignment in future between the different models analyzed by this study cannot be ruled out. As such, while the reconfiguration of the US model on the one hand, and the Chinese data protection model on the other, appears to indicate convergence toward a European-style model, the major difference remains that the US and China already have a powerful "tech-health" complex that has been strengthened by the public health crisis, even if the pandemic has also illustrated its shortcomings and limitations.

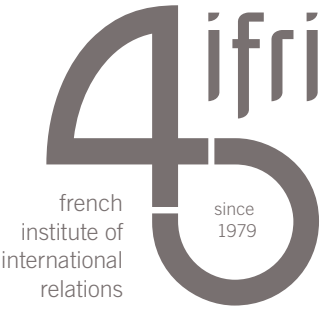
Far from confirming the triumph of European normative power, without resolute action from Europe in the industrial and scientific sphere, this reconfiguration could therefore have the effect of confirming the US–Chinese duopoly on digital health apps: a major source of value and power in the twenty-first century. As Stéphane Grumbach, research director at INRIA, highlights: "We are moving inexorably toward a model of ever-increasing use of health data since, in an ideal world, this holds extraordinary potential for the common good, the good of individuals and populations. But this now raises questions of sovereignty that go beyond simple public and private

interests. Dependency on foreign platforms in areas such as health care or education inhibits the very ability to govern."[137]

With contact tracing apps and the "health passport," the public health crisis has begun a major European public debate on the issue of health data, the outcome of which will influence the future of European co-operation in the health sphere and the capacity of Member States to develop an industry model consistent with their interests, values, and conception of care. While the current European normative model has genuine influence, it is in competition with the Chinese surveillance model and the capitalistic vision of the tech giants, who are propagating a narrative of total appropriation of data by patients and their free use, acting as a gateway to their de facto commoditization. In an interview published on May 12, 2021, prior to his taking up the role of chair of a medical research body in June 2021, former Google CEO Eric Schmidt recommended "that the confidentiality rules [in relation to health data] be modified so that consent for medical research is given by default."[138]

After the work of the German presidency on digital sovereignty at the end of 2020, the "Conference on the Future of Europe" launched in May 2021 and set to culminate in spring 2022 under the French presidency of the Council of the European Union could become the site for a collective debate on the issue of health data that brings together the democratic, economic, and political issues that lie at the heart of the continent's digital sovereignty in the COVID-19 era.

137. Belot, "Les données de santé."
138. Stat+, "Former Google CEO Schmidt Opens Up on Health Data Privacy and the Future of Tech in Medicine", May 12, 2021, available at: www.statnews.com.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org