1

Healthcare Applications

France is slowly perishing in the face of the explosion of medical deserts. This observation is not new. The newspaper *Le Monde* recently published a leading article to this effect. These deserts are real political emergencies, especially considering that desertification currently affects peri-urban and urban areas. There are multiple clear warnings in the face of the growing risk of potentially violating the Hippocratic oath. The private sector offers opportunities such as "patient care via telemedicine tools, making it possible to reduce the inequalities caused by medical deserts"[1].

Brought about by Simone Veil in 1971, the challenge of the *numerus clausus* in medicine was an urgent one. Back in 2018, Michel Canévet raised the issue of the dangers of medical deserts to the senate. Their impact was particularly severe in Brittany, on the Côtes-d'Armor, concluding that "42% of Bretons lived in areas of tension regarding the access to healthcare" (Canevet 2018a, 2018b). It was by means of a simple decree issued on September 13, 2021 (Journal officiel de la République française 2021) that the *numerus clausus* was abolished, partially halting the exodus of medical students to Romania.

The French National Council of the Order of Physicians applied a code of professional conduct based on Article 32, making reference to Article R. 4127-32 from the Public Health Code, according to which "once having agreed to meet a demand, the doctor undertakes to personally ensure conscientious and dedicated care to the patient, relying on scientifically

Chapter written by Anne CAMMILLERI.

1 For example, the case of the company CISCO.

acquired data, and if necessary, calling on the assistance of competent third parties". The duties towards the patient are clearly defined in Articles 32–55 of said code. This shows the extent to which, after the global crisis of the Covid-19 pandemic, it became necessary to strengthen intergenerational bonds. In all areas, multiple initiatives thrived to make technologies available and improve the quality of life of people and animals.

However, cybercrime continues to be a fast-growing phenomenon. WannaCry has left its mark in our collective memory, as a highly virulent cyberattack against the British healthcare system in 2017 and 2020, which resulted in the lucrative theft of medical data of over 2,300 people. In 2021, it was France's turn to suffer a brutal data theft, affecting over 1.4 million patients from the AP–HP (*Assistance Publique–Hôpitaux de Paris*), including "the identity, social security number and contact details of the patients tested, as well as the identity and contact details of the health professionals treating them, the characteristics and results of the tests carried out" (Le Parisien 2021).

While the use of applications such as Stop Covid can fulfill this role in the event of a serious threat to public health (Journal officiel de la République française 2020), they can only do so in a limited way due to the fact that using the application is not compulsory. On the other hand, the use of Stop Covid quickly showed its limitations, particularly in regards to the fundamental requirement of privacy protection. The modernity of our era is paving the way for an increasingly greater reliance on digital technology, making room to a variety of healthcare applications.

1.1. The uses of a healthcare application

The Larousse dictionary defines an application as "a limited processing domain for which software is written" or as "software or set of programs intended to assist a computer user for processing a specific task".

The use of digital applications in the field of healthcare constitutes an immense physical and moral contribution, enabling patients to regain autonomy and improve their health through effective self-monitoring. The number of healthcare applications of all kinds has exploded. For example, among the top 50 best healthcare applications, the American search engine Google returns results for "AllergoBox, the anti-allergy health app", which

helps people with food allergies or intolerances and contact allergies, It also helps people to identify everyday products compatible with their dietary requirements. The application Health For You is only available on the AppStore. The healthcare application Gluci Check helps to monitor diabetes. Also, at the top of the list, there is the Santé.fr application, the official public service application!

It is clear that, above all, healthcare applications enable a collection of sensitive data. This implies the consent of the person who downloads the application on a mobile device or another computer medium and accepts its installation, fully aware that consent will lead to a processing of their personal data. The most classical and popular application in France is *Mon espace Santé*. This safely stores health documents, including "analysis results, prescriptions, medical certificates, which can be exchanged with healthcare professionals through secure messaging and protect health-related data"[2]. With the patient's consent, healthcare professionals have access to sensitive information. Data cannot be collected without the informed consent of the person involved and must have been completely anonymized. The contents of the results stored in the application may be of interest both to healthcare professionals who will analyze the recorded results and to the patient.

The digitization of the public and private spheres has enabled the development of applications in all fields, and depends on the uses envisaged. In this sense, the healthcare field is particularly sensitive. At the European Union level, the subsection XIV TFEU on public health is ambivalent. Article 168, TFEU states that a high level of human health protection is ensured by the definition and implementation of all EU policies and actions. However, the role of the EU remains legally complementary, insofar as this action only "completes" national policies on the improvement of public health, the prevention of human diseases and illnesses, and the causes of danger to physical and mental health.

The European Union is also held competent for monitoring and combatting serious cross-border threats to health. Therefore, this sphere of action is only limited to cooperation competences, in particular, to improve the complementarity of health services in cross-border regions (Article 168, paragraph 2 TFEU). Complementarity is also related to the adoption of standards on the quality and safety for medicinal products and devices for

2 A health insurance website.

medical use (Article 168, paragraph 4.c TFEU). EU action shall respect the responsibilities of the Member States for the definition of their health policy and for the organization and delivery of health services, medical care or the donation of organs. Medicine is experiencing spectacular progress in all fields. The dematerialization of our activities is a digital revolution and has opened up new fields of action to help those suffering, particularly in the medicine field, thanks to AI. Individuals are gaining autonomy through the remote access to healthcare and innovative technologies. This is how the popularization of healthcare applications for individuals contributes to strengthening their autonomy and feeds their hopes of regaining freedom and independence. If used properly, these applications promote the well-being of individuals and the correct functioning of public and private hospital structures (section 1.2). On the other hand, as regards the sensitivity of processed health data, guaranteeing their integrity requires building powerful cybersecurity strategies to ensure the resilience of applications (section 1.3).

1.2. Applications at the service of hospitals (HR dimension)

We immediately note the exponential development of healthcare applications with the assistance of a web search engine. While the anxiety-provoking context of the pandemic could be somehow related to this, in circumstances where a health crisis is not involved, applications continue to develop widely in all fields.

1.2.1. *Internal staff and patient management applications in public and private hospitals*

The hospital workload is particularly heavy. When it is possible to provide remote healthcare, the use of applications can lighten up the workload in public and private hospitals (section 1.2.1.1). The effective sharing of health data necessarily requires the ability to develop actions to ensure healthcare continuity, mutability and equality (section 1.2.1.2).

1.2.1.1. *Applications to assist human resources in hospitals*

MyGHT is a human resource application for hospital workers. It is a complete modular e-health offer to meet the needs of healthcare institutions, nursing staff and patients. It is also used for patients at French residential care facilities for senior citizens (Ehpad, *Établissements d'hébergement pour*

personnes âgées dépendantes). MyGHT Agent was the winner of the 6th edition of the Human Resources Innovation Prize awarded by the French Hospital Federation (FHF), MNH GROUP and the Association for the Development of Human Resources in Health and Social Institutions (Adrhess, *Association pour le développement des ressources humaines dans les établissements sanitaires et sociaux*) on the occasion of the HR Health Meetings back in 2018. This was a successful testimony of the impact of digitization for improving the administrative functioning of the public hospital.

The different solution modules for this application aim to strengthen the link between patients, residents, hospital agents and health institutions through the use of innovative applications, to be used across all media (computers, tablets and smartphones).

The application "comprehensively acknowledges the needs of healthcare institutions by facilitating medical care, patient remote monitoring, care coordination, the analysis or exchange of information between patients and medical or medico-social professionals". MyGHT centralizes all of the information an agent needs (payslips, hour counters, etc.), and provides access to documents and messages from the administration. The agent can easily submit administrative forms online (applications for leave, travel requests) through the application. Information management is facilitated because the administrative staff can manage the information made available to them via the application and centralize every procedure. Following their own initiative, agents can access their account, retrieve professional records and manage the administrative follow-up. As well as from accessing information, MyGHT enables staff to validate their "well-being" at work, from their first login, every day. The data collected and recorded provides the HR department with access to sensitive information. The HR Department can consult statistics on the well-being of agents, and monitor the quality of life at work in hospitals. However, the piece of information relating to the effectiveness of the agent's well-being, collected anonymously, has not been clearly determined. This is likely to truncate the expected information and constitute a serious breach of the GDPR (General Data Protection Regulation). In the search for balance in the French national health policy, the state relies on the classic rules of public law, namely Rolland's laws (section 1.2.1.2).

1.2.1.2. *The effective sharing of health data, scrutinized by Rolland's laws: continuity, mutability, equality*

For any public law specialist, Rolland's laws constitute a reference that is still the cornerstone of the public service: the principles of continuity, mutability and equality can contribute to framing the sharing of health data. How can applications contribute to scientific progress in aid of vulnerable people?

1.2.1.2.1. The continuity of care

This is taken into account thanks to the use of the digital shared medical record (DMP, *dossier médical partagé*). The Minister of Health supports the adoption of the shared medical record, which should enable all patients to access their medical data via the mon-dmp.fr website. With the patient's consent, the consulted doctor can gain access to it, making it easier to reach medical data. By its very nature (intended as the receptacle of all results from health examinations), it contains sensitive data, which justifies cybersecurity concerns and the protection of medical information. In principle, the access to the medical record should be based on the patient's consent, although the latter is not required in the exceptional case of a medical emergency. In fact, the continuity of care offered by the shared medical record favors a secured exchange of patient health data, regardless of the healthcare facility hosting it. Although not exactly an application, the updating of health information on the shared medical record either by the patient or by health professionals works similarly to one: sensitive data are collected, with the patient's consent, in order to ensure the mutability of care based on updated health data.

1.2.1.2.2. The mutability of care

At present, mutability is achieved through connected platforms destined to the health professionals. For illustration, Enovacom, a subsidiary of Orange Business Service, enables teams to share data in order to ensure the continuity and coordination of care. Above all, "for the Orange subsidiary, the intention was to create a common communication channel across clinics, cities and hospitals so as to make the patient's path consistent". The platform should make it possible to enhance the patient's cure/support, ensuring appropriate care practices. Today, many connected health platforms work in this direction. Among the points to be improved upon, let us mention here the availability of medical staff, curbing the growth of the chronically ill and

the high cost of treatment. It is also necessary to counter the overcrowding of medical facilities and to compensate for the lack of access to healthcare in rural areas. It is in this sense that we must understand the arrival of connected health platforms, such as Comarch Healthcare. The goal is to offer the patient teleconsultation solutions.

1.2.1.2.3. The equality of care

Telemedicine makes it possible to fight against medical deserts and to bring not only physical, but also moral, comfort to the isolated patients. Equal access to care was enshrined by the preamble of the French Constitution of October 27, 1946. The Republic proclaimed that the Nation should guarantee the necessary conditions for the development of the individual and the family; and, on the basis of paragraph 11 of said preamble, guarantee health protection, material security, and rest and leisure to everyone (in particular, to children, mothers and elderly workers). Any human being unable to work – in virtue of their age, physical or mental state, or economic situation – has the right to obtain suitable means of existence from the community.

1.2.1.2.4. The ethical challenge regarding the use of applications

Although seemingly innovative, the ethical use of technology is an age-old question. In 1990, Jean-Marie Auby wrote:

> the category of contracts relating to human rights, ignored by traditional civil law, currently appears as an important and difficult element rgarding contractual techniques. Given the fact that it concerns a medical act, it is up to the doctor to implement these techniques in the name of the principle of therapeutic freedom, provided that they do not affect public order (Auby 1999).
>
> What is certain is that ethics does not satisfactorily compensate for the absence of legal rules (Auby 1999).

The European Union addressed the needs of vulnerable adults on the conclusions drawn by the Council in 2020 (“Access to justice – seizing the opportunities offered by digitization”), noting “that they should be given special attention to improve their digital skills and their access to

information, in order to protect their rights" (Journal officiel de l'Union européenne 2021a). It is in this context that obtaining the person's consent for the processing of sensitive information on a healthcare application is a requirement that has to comply with the GDPR, a legal binding that no practitioner can be exempt from. As sedentary lifestyles evolve, applications can be a useful resource to combat isolation and vulnerabilities (section 1.2.2).

1.2.2. *Helpful applications to counter isolation and other vulnerabilities*

The Hippocratic Oath reminds doctors that their "primary concern shall be to restore, preserve or promote health in all its elements, physical and mental, individual and social" and that the doctor "will inform patients of the decisions envisaged, their groundings and their consequences". Modern software applications are an extension of that oath. Without overriding the diagnosis and recommendations preliminarily determined by the doctor, the development of applications allows many people to recover their motor skills for achieving greater freedom and dignity (section 1.2.2.1), and to overcome isolation (section 1.2.2.2).

1.2.2.1. *Recovering motor skills for greater freedom and dignity*

1.2.2.1.1. Through the use of virtual hypnosis

There are several applications to support human and animal welfare. People do not react in the same way to illnesses, physical accidents or moral trauma.

While a few years ago paralysis could permanently immobilize a person, today several applications allow humans, as well as animals – sensitive beings – to regain hope and recover their independence through the mastery of their body. Applications can be extraordinary tools to stimulate atrophied body portions. It is as if the body was sculpted to encourage the brain to regain balance. The world of start-ups is fully invested in research areas for the development of virtual[3] reality therapies, based on applications that facilitate hypnosis.

3 The start-up HypnoVR develops virtual reality therapies.

1.2.2.1.2. Increasing the autonomy of the vulnerable person by mastering technology

The help provided by heart tracking applications

Recovered autonomy can also be achieved "with the help of connected sensors which measure and record muscular strength outputs. The purpose is to provide practitioners with quantified results assessing patient progression in less than a minute"[4]. Many applications help the dependent person to regain moral and physical independence, through health self-monitoring. For example, in the case of heart diseases, some applications enable the recording of an ECG signal, considered to be reliable and secure in the long term. The application Cardiovest, developed by Comarch[5], offers a solution for carrying out preventive examinations. Patients suffering from heart diseases can be diagnosed and monitored through the use of technology that enables a safe, reliable and long-term recording of the ECG signal.

The monitoring[6] bracelet

The monitoring bracelet can be a solution for people in need of constant care, eager to improve their quality of life, and wishing to feel safe. These are remote care services for seniors: each patient is provided with a bracelet[7] and benefits from 24-hour remote support. The implementation of remote care for seniors by local authorities and health institutions helps to improve the situation of the elderly, especially those living on their own, far from relatives. This service seems to cater for dependent patients requiring constant support. The interoperability of digital certificates also helps in the fight against the isolation of vulnerable persons, thanks to free movement rules (section 1.2.2.2).

1.2.2.2. *The critical aspect of protecting information, introduced to the application*

Even though the application *Tous anti Covid*, created in 2020, had a national spectrum of use, its acceptability was difficult to generalize. While many other applications play an essential social role, they are largely

4 Application presented by Comarch.

5 See: www.comarch.fr/solutions-it/plateforme-de-santeconnectee/telemedecine/comarch-cardiovest/.

6 Comarch Life Band Company.

7 Comarch Life Band Company.

outstripped by medical applications, which enable patients to partially recover their physical and mental autonomy.

1.2.2.2.1. Health protection, a national, technical and political goal

Amidst the Covid-19 pandemic, the EU Commission fully played its role as guardian of the treaties in terms of preventive health policy, releasing the sum of 100 million euros under the emergency aid instrument, in order to acquire antigen tests with rapid results. It initiated a joint procurement procedure for over half a billion tests (Berrod 2021; Journal officiel de l'Union européenne 2021b), adding up to the discussions on the multi-annual financial framework adapted to the crisis for the 2021–2027 period.

1.2.2.2.2. The monitoring of essential services by the National Agency for Information Systems Security

In France, the National Information Systems Security Agency (ANSSI, *Agence nationale de la sécurité des systèmes d'information*, set within the General Secretariat for Security and National Defense) plays a crucial role in the functioning of several essential services, including health. A long European process has made it possible to strengthen cybersecurity, particularly in terms of health. Following the exponential increase in cybercrime among the Member States of the European Union, the French government was a driving force for amending and deepening the NIS 1 and NIS 2 directives (Journal officiel de l'Union européenne 2022a). On June 22, 2022, in order to better protect our cyberspace, the Member States, mindful of their sovereign prerogatives, agreed to distinguish the lists of essential services from important sectors in terms of cybersecurity.

Healthcare provided by public and private institutions was qualified as an essential service. Other services and sectors were also deemed to be essential: the postal services; waste management; chemical products; the food sector; electronics; machinery; motor vehicles; digital infrastructure providers; drinking water; education and the entire catering chain; order management; supply and logistics. Although this list, adopted by the consensus of states, is probably not exhaustive, it has the merit of fostering a better protection of health in many ways, by focusing on the interoperability of services. The ANSSI ensured the security of digital vaccination certificates (section 1.2.2.2.3).

1.2.2.2.3. The interoperability of digital vaccination certificates

The ANSSI made it possible to maintain free movement rules, while respecting public order in terms of health and public safety. We should bear in mind that digital certificates stem from a medical act binding the doctor. Hence, health protection cannot be affected by the interoperability of services.

On the other hand, it is up to the European Union to promote "a high level of human health" (Article 168, paragraph 1 TFEU). In 2021, the balance sought between the protection of public health and the respect for the free movement of people enabled the European Union to lift restrictions on free movement, including with regards to Third States such as the Republic of North Macedonia (Journal officiel de l'Union européenne 2021c). Digital vaccination certificates against Covid-19 were interoperable, which led to an improvement in free movement during the pandemic, thanks to the application of the mutual trust principle (Journal officiel de l'Union européenne 2021d). From 2021, the same rule was extended to Ukraine (Journal officiel de l'Union européenne 2021e) and Turkey (Journal officiel de l'Union européenne 2021f). Interoperability can be targeted by various attacks, whose spread could be significant in cyberspace. Therefore, a cybersecurity policy must be clearly stated in an area as sensitive as health. It is thereby appropriate to combine a modern approach in the use of healthcare applications with cybersecurity measures (section 1.3).

1.3. Cybersecurity to reinforce the resilience of applications

Based on the French constitutional traditions and the Declaration of the Rights of Man and of the Citizen, the explosion in the number of applications now available to minors implies an increasing awareness of the need to set up an effective protection of youth against content that could potentially harm their health. In order to achieve this, the use of the regulatory instrument is a strong political signal, considering the urgent need to provide a legal framework for cyberspace, in view of protecting vulnerable people and, especially the health of minor children (section 1.3.1). More generally, the cybersecurity policy must make it possible to better assess the risks associated with the use of modern technologies (section 1.3.2).

1.3.1. *The obligation to protect the health of minor children against content that may harm their health*

A democratic society must promote the physical, mental and moral development of children (section 1.3.1.1) and be able to manage crises or pandemics (section 1.3.1.2).

1.3.1.1. *The substantial interest in the physical, mental and moral development of children*

In formal terms, the entry into force of Regulation 2022/2065 from October 19, 2022 on digital services (Journal officiel de l'Union européenne 2022b) enabled the representatives of the Member States to take into account the convergence of this regulation with the GDPR, placing the person at the center of digital space. The acceptability of technologies integrating AI is in line with the search for scientific progress so dear to Bachelard, and is reflected by the consideration of the substantial interests of the child.

This demand for the primacy of the protection of the children's well-being is a legal and moral requirement. The representatives of Member States ensure that the design and operation of the service are easy for minors to understand, but most importantly, seek to protect them from content that could harm their health, as well as their physical, mental and moral development. The Council particularly emphasizes the obligation to protect children because "such risks may arise, for example, in relation to the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behavior" (Journal officiel de l'Union européenne 2022b, paragraph 80).

It is also necessary to provide a legal framework for the uses of algorithmic systems: operators must take into account the risks of infringement of children's rights by algorithmic systems, which are extensively used on online platforms. European lawmakers attach considerable importance to "the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behavior" (Journal officiel de l'Union européenne 2022b, paragraph 80). Child health risk assessments aim to protect minors. Providers of very large online platforms and of the biggest online search engines have an obligation to ensure that no negative

consequences infringe the rights of children, including through an application.

The effective monitoring of the full integrity of minors' health, physical, mental and moral development (paragraph 81) is an essential moral and legal obligation, constantly recalled by the European Commission. It involves taking into account the risk of "serious negative consequences to a person's physical and mental well-being". Particular targets are gender-based violence and the "danger to the minor's health by stimulating behavioral addictions" (Journal officiel de l'Union européenne 2022b, paragraph 80).

1.3.1.2. *Crisis or pandemic management*

Contrary to the providers of very large platforms, there is an obligation to take specific measures in the event of a pandemic and to ensure the adaptation of online content intended for children. In this context, mastering time constitutes the nerve of digital and pandemic warfare.

There is an obligation to adopt specific measures at odds with providers of very large online platforms in the event of a crisis. This covers

> armed conflicts or acts of terrorism, including emerging conflicts or acts of terrorism, natural disasters such as earthquakes and hurricanes, as well as from pandemics and other serious cross-border threats to public health (Journal officiel de l'Union européenne 2022b, paragraph 90).

As guardian of the Treaties, the Commission should be able to require providers of very large online platforms and of very large search engines to initiate a crisis response as a matter of urgency (paragraph 91).

Obligations relating to the adaptation of online content for children are detailed in Regulation No. 2022-2065 on digital services, and specifically impose an adaptation of content and awareness-raising measures. The panoply of these obligations is far from negligible. In particular, it concerns:

– the adaptation of content moderation processes;

– the adaptation of the general conditions of algorithmic and advertising systems;

– the intensification of cooperation with trusted flaggers;

– awareness-raising measures;

– the promotion of trusted information;

– adapting the design of online interfaces.

This search for a balance between the proper functioning of the digital internal market and the effective protection of children's rights is at the heart of the European legislative system. The European Union firmly combats advertising targeted at people in vulnerable situations, in particular, minors (Journal officiel de l'Union européenne 2022b, paragraph 95).

Finally, the mastery of time constitutes the nerve of the digital and pandemic war: in this barely hidden economic war, taking time into account is essential when evaluating different reactions to crises. Those responsible for processing must be able to react within a very short time and in a proportionate manner to the breach of the obligations to protect health. The simplified ergonomics of an application can be a major asset in this sense.

This strategy of controlling time to prohibit practices that could jeopardize health is reminiscent of the method of adopting European acts of secondary law, which are the basis of the intergovernmental common security and defense policy. A community of values clearly emerges between defense actors and internal market "watchdogs", who ensure the proper functioning of the four fundamental freedoms of movement (goods, persons, services and capital) and the ethical behavior of platform managers. However, it is equally essential to be able to assess the risks of harm to health by digital services (section 1.3.2).

1.3.2. *Assessing health risks through digital services*

It is desirable for health actors to find a sustainable balance between the use of digital services and the national health, on the one hand (section 1.3.2.1), while seeking to reconcile the wide distribution of digital services with the security goal, on the other hand (section 1.3.2.2).

1.3.2.1. *The balance sought between health protection and the sustainable inclusion of digital services in the daily lives of European citizens*

1.3.2.1.1. The risks of harm to public health by digital services

On October 19, 2022, European lawmakers adopted Regulation (2022/2065) on digital services, which contemplates a crisis response mechanism (Article 36, Regulation 2022/2065). In the medical sector, health applications help both doctors and patients. These same applications are very popular terrains for cyber attackers, since corporate cybersecurity is sometimes very rudimentary – if not nonexistent – not to mention applications for which finding a hint of cybersecurity is still a challenge. Regarding the scale and intensity of attacks, mentalities are changing, but still often far too slowly! In many regions and cities – among which Rennes is particularly relevant – cybersecurity centers of excellence help ensure that a business ecosystem is firmly rooted in resilient territories to grant the cybersecurity of essential services, including health.

These risks must be "proportionate to systemic risks" and respect the EU Charter of Fundamental Rights. On the basis of Article 34 from Regulation (EU) 2022/2065 on digital services (DSA, Digital Services Act), European lawmakers implemented the use of analysis in compliance with the principle of human dignity, freedom, media pluralism and children's rights (Article 24, Charter of Fundamental Rights), a high level of consumer protection (Article 38, Charter of Fundamental Rights), and the prevention of negative (or foreseeable) health effects related to gender-based violence (Article 34d, Regulation 2022/2065).

A risk assessment is also based on the design of recommendation systems and any other "relevant" algorithmic systems (Journal officiel de l'Union européenne 2022b, Article 34, paragraph 1). In this context, the providers of very large online platforms and large search engines examine whether (and to what extent) certain factors influence systemic risks, and how these are acknowledged. On the basis of Article 34 from Regulation 2022/2065 (DSA), European lawmakers clearly seek to protect "public health and minors, preventing serious negative consequences to the person's physical and mental well-being" (Journal officiel de l'Union européenne 2022b, Article 34, paragraph 2).

In order to legally qualify (or not) a health crisis at the European Union level, European lawmakers rely on internal public law and Article 35 paragraph 2 from Regulation 2022/2065 (DSA), to assess the scope of such a crisis. This is the case when such extraordinary circumstances result in a serious threat to public security or public health (Article 35, paragraph 2 from Regulation 2022/2065-DSA). This reveals a certain community of spirit with the rules of operation of the internal market and the freedoms of movement inherent in it.

While the general rules on the operation of the internal market are similar to those of the operation of a unified digital market, in the name of free competition, there is a certain vigilance against the operation of contestable and fair digital markets for essential services.

1.3.2.1.2. The influence of health on contestable and fair digital markets for essential services

European lawmakers adopted another regulation 2022-1925 on contestable and fair markets on September 14, 2022. In this context, the access controller and the requesting supplier must ensure that interoperability does not compromise the protection of personal data (GDPR). This reflects the desire of European lawmakers to implement specific protective measures for children online, a goal deemed as "important for the EU" (Journal officiel de l'Union européenne 2022, paragraph 38).

The functioning of these markets is scrutinized by the Commission, because they essentially come under the rules of free competition: the freedom to provide services and goods within the internal market.

Moreover, the deepening of the digital internal market is particularly intense in the context of the crisis response mechanism with regards to digital services (Journal officiel de l'Union européenne 2022b, Article 36, paragraph 2). For that matter, in terms of health, the legal protection mechanism implemented is reminiscent of the European Capability Action Plan (ECAP)[8].

As regards crisis management mechanisms aimed at protecting digital services, European lawmakers strictly frame the notion of extraordinary

8 European capability action plan.

circumstances as “a serious threat to public security or public health in the Union or in significant parts of the Union”. Nowadays, the European Union still contemplates public health simply as an end, and not as an integration policy. This public health goal is understood as a horizon, an aim of the European Union in its economic, social and environmental dimension, but not as a European health policy (in the same way as the other policies of the unified market). Such an approach simply confirms the Europeans’ ‘right to health’, rather than calling into question the hospital system itself, a system which is still lacking in essential means for the dignified care of patients.

The glaring absence of a real European health policy persists in favor of an unambitious goal: the mere coordination of social protection mechanisms. The so-called European health policy does not exist. At best, there is a Berveridgean or Bismarckian mechanism for coordinating social protection systems (Cammilleri 1992).

Similarly, based on EU Regulation 2022/1925 (Journal officiel de l’Union européenne 2022c, pp. 1–66), lawmakers allow the European Commission to not have to impose an obligation on an essential platform service, for reasons of public order. Under exceptional circumstances – solely justified by reasons of public health or public safety, defined by European Union law and interpreted by the Court of Justice (Journal officiel de l’Union européenne 2022c, Article 10(3)) – the Commission should be able to decide that a given obligation does not apply to a specific essential platform service. It is in this framework that an exemption, for reasons of public health and public safety, can be decided upon.

This exemption is subject to an annual review by the Commission (Journal officiel de l’Union européenne 2022c, Article 10, paragraph 3). It can only be granted for reasons of public health or safety. Only an emergency measure by the Commission can temporarily suspend the application of a specific obligation at any time (Journal officiel de l’Union européenne 2022c, Article 10(4)).

1.3.2.2. *Three national and European entities to support health*

Cyberspace monitoring by two national and European agencies is a substantial guarantee of security.

1.3.2.2.1. Two agencies: a national (ANSSI) and a European entity (ENISA)

In its report published in 2022 on the Panorama of the computer threat in 2021, the French National Agency for the Security of Information Systems (ANSSI) announced that "the number of proven intrusions into reported information systems increased by 37% between 2020 and 2021 (786 in 2020 compared to 1,082 in 2021, that is, nearly three proven intrusions per day" (ANSSI 2022). Major events in France, such as the French presidency of the European Union, the presidential and legislative elections of 2022 and the Paris Olympics in 2024, are all contextual opportunities attackers could seek to exploit.

1.3.2.2.2. At the European level, the ENISA annual report (2021)

This highlights that the Covid-19 pandemic favored cyber-espionage activities and created opportunities for cybercriminals[9]. Covid-19 was an important lure in email attack campaigns. Healthcare-related data breaches multiplied. Regulation (EU) 2019/881 of the European Parliament and of the Council of April 17, 2019 relating to ENISA (Journal officiel de l'Union européenne 2019) provides a basis for legal standards that should allow for the implementation of a certification policy, whose outlines can help strengthen cooperation between all the actors, to increase confidence by seeking a high level of security and transparency vis-à-vis the consumer.

1.3.2.2.3. An independent administrative authority, the CNIL, to support health

On May 11, 2022, the CNIL published its 2021 annual activity report, which confirmed:

> the exponential trend in rule violations […]. In 2021, the CNIL received 14,143 complaints, 12,522 of which were closed down. It carried out 384 controls and the shortcomings noted during some of the investigations led to pronouncing 135 formal notices and 18 penalties, for an unprecedented cumulative amount of fines exceeding 214 million euros[10].

9 ENISA Annual Report, p. 12.

10 Sanctions and corrective measures: the CNIL presents the 2022 report of its repressive action on January 31, 2023. See: www.cnil.fr.

With the adoption of the NIS Directive 2 (Journal officiel de l'Union européenne 2022a, p. 80), specific rules are to protect so-called "important" sectors such as postal services, waste management, chemicals, food, medical device manufacturing, electronics, machinery, motor vehicles and digital suppliers.

1.4. Conclusion

Historically, within the UE, health corresponded to a simple and insufficient method for coordinating social protection mechanisms. These could reflect two social models: either the Beveridgian model (identifiable by its universality) or the Bismarckian type, based on an insurance model (Cammilleri 1992). Unfortunately, without really being able to speak of the existence of a European health policy, the Union limits its role to the promotion of public and private healthcare institutions and pharmaceuticals. However, in the event of cyberattacks, the protection of health must result in the use of specific protection tools, because this concern is at the heart of the human being!

1.5. References

ANSSI (2022). Panorama de la menace informatique. Report.

Auby, J.-M. (1999). L'autorité judiciaire gardienne du corps humain ? In *L'unité du droit. Mélanges en l'honneur de Rolland Drago*. Éditions Economica, Paris, 353–367.

Berrod, F. (2021). Le passe sanitaire français et l'enjeu des droits fondamentaux. Université de Strasbourg, Strasbourg.

Cammilleri, A. (1992). *La protection sociale en Europe*. G.L.N. Joly Editions, Paris.

Canevet, M. (2018a). Question orale n° 0441. *JORF Sénat*, 4646.

Canevet, M. (2018b). Réponse du secrétariat d'État auprès de la ministre des solidarités et de la santé. *JO Sénat*, 14043.

Journal officiel de l'Union européenne (2019). Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité JOUE). *JOUE*, L(151), 15–69.

Journal officiel de l'Union européenne (2021a). Conclusions du Conseil sur la protection des adultes vulnérables dans l'ensemble de l'UE. *JOUE*, C(330).

Journal officiel de l'Union européenne (2021b). Déclaration de la Commission. *JOUE*, L211(23).

Journal officiel de l'Union européenne (2021c). Décision d'exécution (UE) 2021/1381 de la Commission du 19 août 2021 établissant l'équivalence, aux fins de faciliter l'exercice du droit à la libre circulation au sein de l'Union, des certificats Covid-19 délivrés par la République de Macédoine du Nord avec les certificats délivrés conformément au règlement (UE) 2021/953 du Parlement européen et du Conseil. *JOUE*, L(297).

Journal officiel de l'Union européenne (2021d). Règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats Covid-19 interopérables de vaccination, de test et de rétablissement (certificat Covid numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de Covid-19. *JOUE*, L(211).

Journal officiel de l'Union européenne (2021e). Décision d'exécution (UE) 2021/1380 de la Commission du 19 août 2021 établissant l'équivalence, aux fins de faciliter l'exercice du droit à la libre circulation au sein de l'Union, des certificats Covid-19 délivrés par l'Ukraine avec les certificats délivrés conformément au règlement (UE) 2021/953 du Parlement européen et du Conseil. *JOUE*, L(297).

Journal officiel de l'Union européenne (2021f). Décision d'exécution (UE) 2021/1382 de la Commission du 19 août 2021 établissant l'équivalence, aux fins de faciliter l'exercice du droit à la libre circulation au sein de l'Union, des certificats Covid-19 délivrés par la République de Turquie avec les certificats délivrés conformément au règlement (UE) 2021/953 du Parlement européen et du Conseil. *JOUE*, L(297).

Journal officiel de l'Union européenne (2022a). Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne. *JOUE*, L(333).

Journal officiel de l'Union européenne (2022b). Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques). *JOUE*, L(277).

Journal officiel de l'Union européenne (2022c). Règlement (UE) 2022/1925 du Parlement et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives 2019/1937 et 2020/1828 (règlement sur les marchés numériques). *JOUE*, L(265).

Journal officiel de la République française (2020). Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé "StopCovid". *JORF*, 0131(17).

Journal officiel de la République française (2021). Arrêté du 13 septembre 2021 définissant les objectifs nationaux pluriannuels de professionnels de santé à former pour la période 2021-2025. *JORF*, 0217(27).

Le Parisien (2021). Diffusion de données piratées à la suite d'une cyberattaque : quels sont les risques et les précautions à prendre ? *Le Parisien*, September.