CERNA
Commission de réflexion
sur l'Ethique de la Recherche
en sciences et technologies
du Numérique d'
ALLISTENE

Sovereignty in the Digital Age

Keeping control over our choices and values

CERNA

Writers: Jean-Gabriel Ganascia, Eric Germain, Claude Kirchner

2018, October

Contents

ABSTRACT

The digital revolution currently underway raises new ethical questions that each of us needs to consider. Originating in political philosophy, where it is restricted to the idea of national sovereignty, sovereignty can be defined as the capacity of an entity to set itself its own rules or, more trivially, as "the power to be able". This concept of sovereignty remains relevant to understanding and analysing the impact of digital sciences, technologies and uses. However, it needs to be revisited, so far do the problems raised by digital technology overturn the classical concept of sovereignty, in particular that of national sovereignty. These problems alter the conditions of the expression of sovereignty and facilitate opposition to it by outside interests. Far from leading us to abandon any idea of national sovereignty, digital technology offers new perspectives on the concept and prompts us to introduce different forms of sovereignty, which include in particular question of sovereignty over infrastructures, the digital sovereignties of states, organisations or citizens, scientific sovereignties, or supranational sovereignties such as European sovereignty, all of which clearly appear today as both desirable and necessary.

Against this background, the ethical issues that emerge and that we develop are of two kinds:

1. In the absence of sovereignty, the choices that arise from rational reflection and from the expression of free will cannot be implemented, so sovereignty is essential to applied ethics;
2. In addition, digital technology changes, but does not eradicate, the classical expression of the sovereignty of peoples. The global age, despite its globalisation effects, erases neither the expression of cultural diversities nor the need and the rights of human communities to govern themselves and forge their own destiny around shared values, aesthetics and political choices.

However, the coexistence of these different forms of sovereignties inevitably leads to conflict between sovereignties of different orders, which will have to be overcome. This will undoubtedly lead us in the future to devise new conflict resolution procedures. This report is not about those procedures, which will be a matter of political choices, but is primarily concerned with characterising these new forms of sovereignty and with the challenges they bring as we look forward to a digital society.

After an introduction that situates the problem, the first part of this report recalls the historical foundations of the notion of sovereignty. The second part develops conceptual aspects of sovereignty, highlighting the points on which the digital age presents a challenge to traditional notions, which we will develop in the third part. In the fourth part, we cover first digital sovereignties, and then scientific sovereignties. Finally, we conclude by relating the challenges of ethics and sovereignty to contemporary geopolitical thinking, the education of citizens and scientific ethics.

In the course of the text, we identify the principal issues associated with the concept of sovereignty, we advance recommendations and make several suggestions. Though strictly speaking the latter lie outside the remit of CERNA, they form a coherent whole with the seven issues raised and eight recommendations formulated. All these elements are summed up at the end of the document.

INTRODUCTION

Addressing the 72nd General Assembly of the United Nations on 19 September 2017, the President of the United States employed the words "*sovereign*" and "*sovereignty*" no less than twenty-one times.[1] It is difficult not to see this insistence as a response to the Russiagate controversy, in which digital technologies are suspected to have been used in a Russian attempt to interfere in his favour in the US elections. Donald Trump was keen to emphasise that "*in America, the people govern, the people rule, and the people are sovereign*".

On the same day and before the same audience, Emmanuel Macron spoke of wishing to respond to the restrictive vision of sovereignty of "*those who appeal for our help means believing that we are protected by walls and borders*",[2]advocating for a sovereignty that does not set up an opposition between security and openness to the world. The President of the Republic asserted: "*It is our will to act, and to influence the course of history. It is our refusal to accept that history will be written without us, while we believe we are safe. What protects us is our sovereignty and the sovereign exercise of our strength in support of progress. That is the independence of nations in the context of our interdependence.*"

These words have a particular resonance when related to the sovereignty issues raised by the development of digital technologies in a space where it is difficult to imagine building walls and borders, although certain attempts are emerging, such as "Runet", which describes itself as the Russian segment of the Internet.

The consequences of the upheavals caused by digital sciences, technologies, practices and innovations are everywhere. Global digitisation is changing our experience of the world that surrounds us, and placing tremendous pressure on numerous aspects of the human relationship to the world.

Sovereignty and ethics are fundamentally connected, since without sovereignty it is difficult to develop ethical reflection, which requires freedom of thought, of action and of access to knowledge and, above all, it is impossible to implement clearly and responsibly the choices to which that reflection leads.

CERNA began this work when France's Digital Republic Act of 7 October 2016 was considering the creation of a Commission for Digital Sovereignty.[3] We therefore thought it essential to reflect on what this "digital sovereignty" really represents, and on the ethical issues inherent in this topic.

[1] https://www.whitehouse.gov/the-press-office/2017/09/19/remarks-president-trump-72nd-session-united-nations-general-assembly

[2] https://www.diplomatie.gouv.fr/en/french-foreign-policy/united-nations/united-nations-general-assembly-sessions/unga-s-72nd-session/article/united-nations-general-assembly-speech-by-m-emmanuel-macron-president-of-the

[3] Art. 29: *The Government shall submit to Parliament, within three months of the enactment of the present law, a report on the possibility of creating a Commission for Digital Sovereignty attached to the Prime Minister's Office, tasked with contributing to the exercise, in cyberspace, of national sovereignty and the individual and collective rights and freedoms that the Republic protects. This report shall specify the resources and organisation necessary to the functioning of the Commission for Digital Sovereignty.* https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=F5935AFABF3AE72BDB108134B84C9F8F.tpdila08v_2?idArticle=JORFARTI000033203122&categorieLien=id&cidTexte=JORFTEXT000033202746&dateTexte= Our translation.

It is interesting to note that the recent report on artificial intelligence, produced by the MP and mathematician Cédric Villani and his task force,[4] never refers to "digital sovereignty", but embeds it in a wider problem of "technological and economic sovereignty". At the public release of this report, on 28 March 2018, President Emmanuel Macron described national sovereignty as the capacity of a nation to define its own standards and not to have those standards imposed from outside. To assert that "artificial intelligence is an imperative of sovereignty"[5] immediately elicits the question of whether sovereignty in the digital age still has the same meaning, which is precisely the subject that we tackle here.

If we take the simplest definition of sovereignty as the capacity for self-governance, does a nation, a corporation, a scientific community still have the capacity to conceive and to implement the ethical choices that it defines for itself? At the individual scale, the problem is similar, although in this case we would speak of autonomy rather than sovereignty.

Sovereignty, a pivotal and defining notion of the relationship of legitimate authority between human beings under the rule of law, is particularly affected by this rapid and global technological change. The notion appeared at the dawn of the modern age, with political theorists such as Jean Bodin in the sixteenth century, then John Locke in the seventeenth and Jean-Jacques Rousseau in the eighteenth. Its transposition into today's hypermodern society, with our generalised use of digital technologies, raises a number of questions, notably:

- How can the notion of sovereignty in general, a political or philosophical concept foreign to digital sciences, be applied to digital technology? In other words, can one imagine the ascendancy of a **digital sovereignty** that either overturns traditional national political sovereignty and national borders, or coexists with them?
- How can the concepts and practices of **national sovereignty** be harmonised with planetary flows of digital data that seem to prefigure the obsolescence of territoriality?

Should sovereignties, whether national or digital, rely on digital tools and services or on dedicated systems of governance? Does the notion of a sovereign operating system or a sovereign "cloud" mean anything? To what extent does the governance of the Internet (ICANN, W3C, …) challenge national sovereignty? We believe that we need first to emphasise three points, to set limits on the scope of our reflection.

This report should not be expected to attribute an ethical value, positive or negative, to sovereignty, which we see above all as a concept. It is a concept whose heuristic value we were able to appreciate in writing this report, finding it particularly relevant to understanding the political, societal and of course ethical issues raised by the mass spread of digital technologies.

Nor should our words be read as an argument in favour of national sovereignty. The ethical value that we might associate with this type of sovereignty greatly depends on other parameters, such as the type of political regime in the country concerned: the sovereignty of an open and pluralistic liberal democracy, with different checks and balances on power, is obviously not the same as the sovereignty of an authoritarian and dictatorial regime. Moreover, it should be noted that we speak in this report of sovereignties in the plural. In this plurality, it is the quest for the common good that defines the ethical value of a sovereignty, whether national, scientific or corporate.[6]

Finally, the subject of our report is not "democracy and the challenges of digital technology", though

[4] "Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne"; http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/184000159.pdf

[5] https://www.la-croix.com/Economie/France/Cedric-Villani-Lintelligence-artificielle-imperatif-souverainete-2018-03-29-1200927629

[6] Article 1833 of the French Civil Code states that "*every corporation must* (…) *be constituted for the common interest of its members*"; http://codes.droit.org/CodV3/civil.pdf, cf. p. 349, our translation. "Corporate social responsibility" (CSR) can be seen as a form of extension of this principle of common interest beyond the members or shareholders alone.

there are obvious links with our theme and it is raised several times, without lengthy discussion. There is, for example, the question of net neutrality set against the issues of cybersecurity. In France, on the government side, the answer to this question is envisaged today through the establishment of "effective and reasonable"[7] oversight of the National Agency for Information System Security (ANSSI) by the Authority for the Regulation of Electronic and Postal Communications (ARCEP).

We therefore propose to contribute to the debate on these questions by first recalling the historical background (Part I) and conceptual background (Part II) of the notion of sovereignty and then by highlighting the areas in which the digital age raises questions about the traditional notions (Part III).

We then propose to examine in practical terms the ethical and political issues raised when nation-states assert their sovereignty in digital space (Part IV).

We conclude by formulating recommendations to help citizens, scientists and political or business leaders to advance in their thinking about digital technologies and the ethical issues associated with them, so that they can act in a way commensurate with their beliefs and responsibilities.

[7] Expression employed by Guillaume Poupard, Director-General of ANSSI, in his appearance on 8 March 2018 before the Defence Committee of the National Assembly; http://www.assemblee-nationale.fr/15/cr-cdef/17-18/c1718053.asp

PART 1: A look at the historical and classical definition of sovereignty

Before seeing how digital technology challenges the classical idea of sovereignty as the foundation of the social, cultural and political identity of a human community, let us recall how this notion emerged in our history. Already present in theology or in political and moral philosophies, it was introduced very early on as the basis of international law.

In the etymological sense, sovereign refers to supremacy over all others. Hence, God in a theocracy, the king in an absolute monarchy, or the people in a democracy, can be the entity that holds the supreme and autonomous authority described as sovereign power.

1.1. From sovereignty of divine essence…

The adjective "sovereign" originally described a spiritual power, before it came to be applied to temporal authority. In the theological sense, the sovereign is that entity which, from a metaphysical point of view, is self-sufficient, which draws its essence from itself. It is autonomous, total, and closed, since there is nothing beyond. Thus from Augustinian thought to scholastic theology, we see the existence of a sovereign God defined as being the totality of the real, since nothing is outside him. In his *Ethics*, Spinoza describes God, who is "his own cause" as a being possessed of sovereign intelligence and sovereign power.[8] As we will see later, this concept of closedness can be useful in tackling the paradox of digital sovereignty, which can be understood in two different ways. One way is as national sovereignty over digital infrastructures, which would result in states maintaining total control over the governance of the Internet, leading to a process of closure, of censorship, of digital border controls, etc. The other way is as the sovereignty of the digital domain over the other forms of local sovereignty, in particular national sovereignty, which would lead to openness and the embeddedness of the national in the global.

Finally, in yet another domain, moral philosophy speaks of a "Sovereign Good" to describe a good greater than any other. Likewise, a duty is said to be sovereign if it cannot be weighed against other reasons for acting, since it has its own overriding rationality.

In Western Europe, the modern era was marked by the desire of monarchs to break free of the spiritual authority of the Pope. In the sixteenth century, one of the first acts in the construction of the nation-state was to assert the autonomy of national temporal power over the transnational power of the Church.[9] In France, in 1539, the sovereign Francis I issued the Ordinance of Villers-Cotterêts which imposed the use of French rather than Latin as the language of law and administration. This policy went hand-in-hand with the Gallican movement which, in the religious sphere, sought to impose national political control over the "ultramontane" authority of the sovereign pontiff.[10] Note that the primary Latin etymology of "pontiff" refers to the first bridge in Rome and that @pontifex is the name of the Pope's Twitter account, a choice that suggests a desire to "build bridges".[11] This choice

[8] Baruch Spinoza, *Ethics*, Part I.

[9] The term nation-state refers to the juxtaposition of a state, as a political organisation, and a nation, i.e. individuals who consider themselves to be linked and members of the same group; https://fr.wikipedia.org/wiki/%C3%89tat-nation

[10] In the kingdom of Britain, this movement would be even more radical with the creation in 1534 of a Church independent of the papacy.

[11] https://fr.wiktionary.org/wiki/pontifex

illustrates the similarity of the universal and "deterritorialised"[12] sovereignty of the Catholic Church with what today might be characterised as the "fluid and all-pervasive"[13] sovereignty of the digital domain.

1.2. … to the sovereignty of the nation

The sovereignty claimed in the religious sphere is different from the model attached to the idea of the nation-state, which gained ascendancy in the seventeenth century with the Treaties of Westphalia.[14] These treaties brought into being an international order in which each state is sovereign in its choice of religious policy (*cujus regio, ejus religio*).[15] The state is seen as an entity that imposes a single religion within its borders and exercises a "monopoly of legitimate physical violence" over its subjects.[16] This monopoly is imposed within the borders against the feudal order and defended outside them with an increasingly "national" army.

The sovereignty of the nation-state would take the form of a royal absolutism (theorised by Jean Bodin in France in the sixteenth century, then by the Englishman Thomas Hobbes the following century), before evolving into a sovereignty of the nation that would be embodied in British parliamentarianism or in a more radical form in revolutionary France.

With the genesis of the centralised state at the beginning of the modern age, the notion of "sovereign" was used to refer to the prince, the king or the Republic (Genoa, Venice, Geneva, etc.), embodying the abstract collective entity in whose name political decisions were taken. In the course of the eighteenth century, the establishment of a state apparatus, with its institutions and its civil servants, led to the autonomisation of the state, its separation from the person of the monarch. The notion developed and bloomed through the ideas of Bodin, Hobbes and Locke, among others, before playing a central role in Rousseau's pre-Republican thinking. It was Rousseau in particular, in *The Social Contract*, who developed this structuring idea of "sovereign" as the collective person from which the "general will" emanates. He contrasted the "sovereign people" with individuals or entities that each pursue their particular interests.

Thus, Article 3 of the 1789 Declaration of the Rights of Man and of the Citizen stipulates that : "*The principle of any sovereignty resides essentially in the Nation. No body, no individual can exert authority which does not emanate expressly from it.*"[17] In this very French conception, authority

[12] The sovereignty of the Catholic Church resides more in the state apparatus of the Holy See than in the Vatican micro-state (fewer than 1000 inhabitants over half a square kilometre), with the world's smallest army (110 Swiss Guards) and without a currency of its own.

[13] Regarding the digital revolution, French MP Laure de la Raudière refers very accurately to "a dimension of temporal, spatial and social pervasiveness"; https://www.youtube.com/watch?v=Q_V9V3gpzXk&t=9s; cf. 8:26'

[14] The Treaties of Westphalia in 1648 put an end to the Thirty Years War. The expression "Westphalian system" would subsequently come to refer to the international system that emerged from these treaties.

[15] A concise way of expressing the fact that a ruler's religion determines the religion of his or her subjects.

[16] Concept developed by Max Weber in two essays, *Science as a Vocation* and *Politics as a Vocation* (1919).

[17] https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789
https://en.wikisource.org/wiki/Translation:Declaration_of_the_Rights_of_Man_and_of_the_Citizen

derives neither from groups, which as intermediate bodies act only as factions,[18] nor from individuals, understood as being subservient to their particular needs. This article thus understands national law as the expression of the general will, itself a manifestation of the sovereignty of the people.

Expressing its affiliation with the revolutionary legacy, the preamble to the Constitution of 4 October 1958 begins with the stipulation: "*The French people solemnly proclaim their attachment to the Rights of Man and the principles of national sovereignty as defined by the Declaration of 1789, confirmed and complemented by the preamble to the Constitution of 1946, and to the rights and duties as defined in the Charter for the Environment of 2004.*"[19] Then, in Article 3 "*National sovereignty shall vest in the people, who shall exercise it through their representatives and by means of referendum.*" This clause thus unites the notions of the sovereignty of the people and of national sovereignty, which is expressed within the political framework of a "state" (a cardinal principle of the United Nations Organisation at its creation in 1945).

1.3. A triumphant – but doubly disputed – national sovereignty

According to some political currents, the system of representative democracy betrays the "pure" expression of the people's sovereignty. Usually found at the margins of the political chessboard, this latter conception – described by its detractors as "populist" – is presented by its adherents by the label "sovereignist".

Whether termed populist or sovereignist, this current is at present enjoying a revival, especially in Europe. It claims to support the model of the nation-state in a centuries-old movement that has seen a transition from sovereignty "by divine right", to the sovereignty "of the nation", then to the sovereignty "of the people", the latter taking on a mystique that is somewhat reminiscent of the initial formulation.

On the other hand, the "nation-state" is also being challenged by other actors, who do not see it as the only possible framework for the expression of sovereignty. They argue for the transition from a rigid and centralised model towards a more fluid framework more characterised by the principle of subsidiarity.

While the Westphalian model of the "nation-state" became dominant in Europe, then around the world, it has never been exclusive. It has coexisted with religious or economic powers, acting as quasi-states, which have made the transition to a deterritorialised exercise of their sovereignty.

In the religious sphere, the Order of Malta is an example of a quasi-state that today is completely "deterritorialised", yet possesses an official diplomatic presence which has enjoyed a certain revival in recent years. In 2017, for example, an embassy of the "Sovereign Order of Malta" opened in Germany. In the economic sphere, it may be recalled that, in seventeenth and eighteenth century Europe, the East India and West India Companies were "sovereign" in their authority over the overseas trading posts and territories placed under their control. The Dutch and British East India Companies in particular provided perfect models.[20]

[18] It was the spirit of the Le Chapelier law of 1791 that prohibited professional corporations and associations.

[19] https://www.legifrance.gouv.fr/Droit-francais/Constitution/Constitution-du-4-octobre-1958; text updated on 3 March 2017.http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/constitution_anglais.pdf

[20] One might also mention other, more "underground" models of transnational organisations in rivalry with state sovereignties, such as the triads and other criminal organisations, for which digital technologies now offer new resources (e.g. cryptocurrencies that facilitate money laundering).

These two examples correspond to what the historian Fernand Braudel called a “world-economy”: the Order of Malta (like the seagoing republics of Venice or Genoa) developed in Mediterranean space, and the India Companies in transoceanic space. **The commercial space of the “digital world-economy” is reminiscent in some respects of these historical examples**. They can help us better define the concept of sovereignty which, today, is primarily characterised by its domains and the means of its exercise.

PART 2: How to think differently about sovereignty?

2.1. Defining the term "sovereignty" by its domains…

Challenged today by digital technology and globalisation, the idea of national sovereignty remains fundamentally attached to the old notion of political sovereignty theorised by Locke, Voltaire, Rousseau and others. There are still prerogatives that are recognised as falling naturally within the competence of the state. The first of these are the so-called regalian functions: internal security, defence, education, diplomacy, justice, finance, in particular monetary policy and the collection of taxes and duties.

Some countries like France consider that "national education" is also a sovereign function of the state, because it enables future citizens to develop critical thinking and to acquire the methodological tools for access to knowledge and culture. This probably reflects the influence, accepted at the highest level of the state, of an "*Enlightenment spirit which means that our goal* (…) *is the autonomy of the free, aware and critical individual"*.[21] The problem of a state commitment to the "public instruction" of the new generations is revived today by the development of digital technologies. Likewise, some countries – including those of the EU and in particular France – think that the organisation of the health system also falls within the purview of national sovereignty.

France's broader conception of state functions is expressed through more extensive prerogatives: official language, health, environment, transport and transport infrastructure, solidarity (social insurance, pensions, unemployment benefit, etc.)..

Not only can the range of domains perceived as the core of the sovereignty of a human community vary, but also the hierarchy between them. Catalonia, for example, illustrates a political orientation that prioritises language, culture and education over issues of monetary policy or border control, and which also corresponds to the European federalist project.

This approach to sovereignty through its domains prompts us to review the classical concept of sovereignty **by focusing on the capacity of the sovereign, as a collective entity, to fully control the attributes over which it claims control**: territories (borders), army, police, currency, language, civil code, etc.

The term "control" is used here to express the fact that the entity concerned is both independent and recognised as such by its conspecifics, and that it also possesses the resources to effectively exercise its authority.

The coexistence of these different orders of sovereignty can spark rivalries and generate conflicts. This happens, for example, when a supranational entity supplants a national entity in certain prerogatives.

2.2. Being pragmatically aware of the means of exercising it in a globalised world

Sovereignty only means anything if its holder's capacities are commensurate with its holder's ambitions. In the case of national sovereignty, this depends on control over the regalian functions of national defence, internal security, diplomacy and justice,[22] as well as over the market economy, including tax collection and to a certain extent the currency. Typically, a state will only be sovereign if it possesses credible means to defend its borders (diplomatically or by force), to maintain social order and to levy taxes.

[21] Speech by Emmanuel Macron before a joint session of Parliament on 3 July 2017; http://www.elysee.fr/declarations/article/discours-du-president-de-la-republique-devant-le-parlement-reuni-en-congres/ Our translation.

[22] With regard to justice, there is a double level of sovereignty: a national jurisdiction can be sovereign, but judges can also be vested with "sovereign authority to judge".

The control over these regalian functions has motivated the acquisition and control of data, information and knowledge, and has given rise, for example, to the development of national doctrines regarding domination of the informational sphere ("*information dominance"* or, more diplomatically, "*information superiority*"). Intelligence services, communication protocols and cryptology have, throughout history, formed the underpinnings of national sovereignty. From Caesar's cipher to modern encryption techniques, methods of keeping secrets and acquiring information have been (and still largely are) controlled by states. However, with the arrival of the information and communication technologies, in particular with the development of the Internet, then what we call the digital society, in other words an entire society penetrated by these technologies, the control, production and processing of information take on much greater importance, since they becomes the key to all exchanges and social activities. For this reason, the state has not been able to maintain encryption as solely a state prerogative. In France, it was not until 1998, when it became necessary to allow the banks to offer online services, that it became legal for citizens and companies to employ cryptography with no limits on resistance. Today, we see that control over communications and information processing is potentially accessible, in democracies, to multiple entities, from big corporations to ordinary citizens.[23]

In these circumstances, sovereignty is simultaneously emphasised, disputed and confronted with its own limits. There are *doctrinal* limits, *pragmatic* limits (notably linked to globalisation), and *technological* limits.

The *doctrinal* limit essentially reflects an opposition between two traditions that originated in the Enlightenment: a more liberal tradition, which seeks to reduce the reach of the state to a minimum, though without eliminating it; and a more statist tradition that grants greater scope to state sovereignty, while nevertheless retaining an area of privacy. The French tradition is markedly statist. However, even in the more liberal tradition, the state continues to assume the regalian functions of defence, internal security, justice, finance and diplomacy. Thus, in 2008, at the time of the so-called sub-prime crisis, the British government intervened to save the banks from bankruptcy. Conversely, a liberal government can delegate some of its prerogatives, such as health and education, to other entities, and sometimes even security and defence roles (e.g. the private US military firm Blackwater, renamed Academi in 2011).

The second, *pragmatic* limit arises because states do not exist in isolation: they maintain multiple relations with each other which necessarily limit their power. In this respect, states have never been able to be totally sovereign and are even less so today. National sovereignty is limited by international agreements and treaties, by international law and the law of war, as well as by the voluntary renunciation of sovereignty by a country's citizens in order to be part of a larger supranational entity. This is notably what France has done in relation to Europe. Thus, in the very particular context of the aftermath of the Second World War, the preamble to the 1946 Constitution stated that, "On condition of reciprocal terms, France shall accept the limitations of sovereignty necessary to the organization and defence of peace". And the Constitution also accepted the rule that "Treaties or agreements regularly ratified or approved have, from the time of publication, an authority superior to that of laws" (Article 55 of the Constitution). European integration would subsequently lead to the abandonment of certain regalian prerogatives of the nation, such as "minting money".

The third limit is *technological* in origin and arises from the multiple dependencies of national technological systems on international systems. Digital technology is clearly among them, probably the most important, but not the only one. There are, for example, international systems of standardisation such as driving on the right or on the left, the gauge of railway tracks or the voltages of electrical systems, or indeed the RFC (Requests For Comments) of the IETF or of the W3C.[24]

[23] For example by using secure message services like Protonmail or Telegraph, encryption utilities like PGP or Veracrypt.

[24] IETF is the Internet Engineering Task Force, an informal international task force which, since 1986, has been developing Internet standards. The World Wide Web Consortium or W3C was set up in 1994 to promote the compatibility of World Wide Web technologies.

Technological frontiers are not, so to speak, the same as national frontiers.

2.3. Sovereignty or autonomy?

Sovereignty is the opposite of interference, just as autonomy is the opposite of heteronomy ("Agents are heteronomous if their will is under the control of another").[25] Sovereignty and autonomy are related notions but, paradoxically, national sovereignty today is often challenged on the grounds of regional or community "autonomy".

The term "irredentism" is a more accurate expression of the old idea of a territory that wishes to escape the sovereignty of a state to which it belongs in order to acquire its own sovereignty. The example of Catalonia is once again interesting, because it represents the demand for a sovereignty that is partial (rejection of Spanish sovereignty but acceptance of a very significant delegation of sovereignty to Europe) and selective, focused on the most central elements of a collective identity (language of everyday use and education, school textbooks, conception of secularism, etc.).

The examples of "autonomist" claims from within a nation can help us to pinpoint and better understand the differences between autonomy and sovereignty.

While the two notions are obviously linked, sovereignty implies the capacity to recognise independence and, reciprocally, the capacity to be recognised by other sovereign entities as the holder of an acknowledged and independent power.[26] From the transcendent properties associated with the early uses of the word sovereignty, the concept has retained something of a sacred aura. Once defined, the borders of modern states have therefore taken on a certain character of inalienability.[27] Until recently, independence was essentially exercised in an identified geographical space. Today, data and computational capacity create their own space, which extends the notions of territories as examined here.

The word autonomy can be ascribed to a collectivity or to an individual, or indeed to an object or a set of objects (e.g. autonomous vehicles or drone swarms), whereas in its historical meaning, sovereignty is in essence collective.

Strictly speaking, the notion of autonomy should be restricted to the scale of the individual ("free will"), and sovereignty reserved for the expression of collective will. However, we are in a situation where the autonomous individual also aspires to be independent, notably thanks to the new digital tools. We therefore find ourselves in the position of sanctioning a new notion (for some an oxymoron) of "individual sovereignty", a notion that already exists, notably in political rhetoric, but on which the writers of this report have differing views.

[25]http://www.oxfordreference.com/view/10.1093/oi/authority.20110803095436286

[26]"*Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State*." Max Huber. Permanent Court of Arbitration, arbitral ruling, p.8, in https://pcacases.com/web/sendAttach/714

[27]In France, the principle of the irrevocable and absolute inalienability of the royal domain was affirmed by the Edict of Moulins in 1566.

PART 3: The digital challenge to the classical notion of the sovereignty of the nation-state

The term "digital" here refers to the sciences, technologies, practices and innovations rendered possible by the identification, study, storage, processing, reception or transmission of information. Indeed, information is at the heart of this scientific, technological and human revolution, in the same way as matter, energy or life were fundamental in the last century.[28] The impacts of digital technology on our philosophical, scientific, technological and societal thinking are profoundly changing our contemporary societies. What does this mean for the notion of sovereignty?

3.1. From the libertarian utopia of the early days of the Internet…

The origins of the digital era were marked by a certain notion of the popular will. From the emergence of the first concepts of computerisation and the Internet between the 1950s and the 1980s, and more so with the first version of the World Wide Web in the 1990s, digital technology was seen as opening the way to a sort of political, social and even spiritual utopia. Some saw digital technology as potentially offering a space in which the ideal of the popular will would be expressed instantly, leading to an authentic democracy in which all citizens would participate directly, from the comfort of home. The idea of a "planetary *agora*" – in reference to the *agora* of the Ancient Greek city, a public place of political debate – was a common theme. In his famous manifesto, "*Declaration of Independence of Cyberspace*"[29] (1996), for example, John Perry Barlow declared a new form of sovereignty,[30] a "new home of the mind", in which the governments of the industrial world would have no power.[31] Barlow describes a world in which the users of digital data will possess their own autonomy by virtue of their position in digital space and not because of the political norms or rules of democratic institutions. Several institutions of governance were subsequently created along such lines, such as the W3C or the Internet Engineering Task Force (IETF), although digital space quickly proved to be hard to govern, especially as the United States, currently the leader of this new economic sector, was not willing to renounce such a precious capacity for influence.

As we have just noted, and as Michel Serres very clearly explains, the digital sphere relates to the production, reception, storage and processing of information. The domain of information, hence the digital domain, is a major sector for the exercise of sovereignty, because whoever controls information outdoes their competitors in their capacity to know, to decide and to communicate. This advantage is very explicitly the objective sought through the doctrine of information dominance pursued in particular by the United States. It is summed up in this 1999 statement by Barbara McNamara, Deputy Director of the *National Security Agency*: "The ability to understand the secret communications of our foreign adversaries while protecting our own communications, a capability in which the United States leads the world, gives our nation a unique advantage." However, while information has long been used

[28] "*Information is information, not matter or energy. No materialism which does not admit this can survive at the present day.*" N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine* (1st. ed. 1948). Cambridge, MA: MIT Press, cf. p. 132.

[29] https://www.eff.org/cyberspace-independence

[30] John Perry Barlow (1947-2018), founder of the Electronic Frontier Foundation.

[31] "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather*." John Perry Barlow. https://www.eff.org/fr/cyberspace-independence https://www.eff.org/fr/cyberspace-independence

for intelligence purposes, to gain an advantage over one's rivals, today it has taken on an even more important role, since it is becoming the medium and the condition of all social life, for exchanges between people, between banks, between hospital IT systems, between government departments, etc.

The entire US state apparatus has been recruited to this policy, as evidenced by Executive Order No. 12333 of 4 December 1981, which begins with the following statement of intent: "The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal." [32]

The information used by states to monitor their territory and the activities of their citizens differs from that which the information and communication technologies make available for use by the public as a whole. While controlling information has always been a major priority of national sovereignty, the new factor is the use of processing and communication technologies, hence its crucial importance at all levels of the economy, of social life, of the media. It concerns not only nations, but corporations, organisations and citizens who, from the comfort of their homes, can participate in the life of the state.

3.2 … to experiments in direct democracy

Digital platforms provide new *agoras* for discussion that seek to give citizens a free and direct voice, They are in competition with the traditional structures of representation: trade unions, political parties, civil society organisations of various kinds. It is worth listening attentively to Google-France's Director of Communication when she chooses to illustrate her company's "corporate social responsibility" policy with three examples: its support for the Egyptian revolution of 2011 (the Voice-to-tweet software developed by Google with Twitter to help Egyptian citizens to bypass Internet censorship), the support for whistleblowers (with no other details) and the activities of the firm Change.org.[33]

Of course, there are legitimate questions to be asked about the future of these so-called "citizen" initiatives (Internet users often labelled as "citizens of the world") in the event that they should prove to threaten the geopolitical interests of certain states or corporations (e.g. the case of whistleblowers). More importantly, however, we believe that it is worth looking more closely at the example of Change.org which, as a "for-profit" philanthropic enterprise, constitutes a new model.[34] In fact, its business model consists in mobilising the moral sentiments of the population in order to build reputational capital which, in the digital economy, is an exploitable resource. The company nevertheless presents itself as the perfect example of the type of generous initiative that "e-democracy" can produce. The online petitions platform has built its success on popular issues such as the protection of the environment, human rights and health. However, it also engages with political subjects, such as the petition in 2013 demanding the resignation of the Spanish government. Since Change.org is a commercial organisation, its valuation relies on its capacity to mobilise public opinion, a capacity realised by supporting causes deemed to be "moral".

From an ethical perspective, there are questions to be asked when a commercial entity poses as a

[32] https://www.archives.gov/federal-register/codification/executive-order/12333.html

[33] Talk by Anne-Gabrielle Dauba-Pantanacce, Director of Communication for Google-France at the symposium on "L'héroïsme à l'ère de l'IA" [Heroism in the AI age], at the École militaire, on 18/12/2017. It is interesting to see this online petition platform highlighted by Google's communication, when to our knowledge there is no formal link between the two firms (apart from Jennifer Dulski who left Google in 2013 to become CEO of Change.org).

[34] Tomio Geron, "The Business Behind Change.org's Activist Petitions", 5/11/2012; https://www.forbes.com/sites/tomiogeron/2012/10/17/activism-for-profit-change-org-makes-an-impact-and-makes-money/#6c1ce7e67ffa

model of alternative sovereignty. Indeed, the director of Change.org in France presents his company as "the insurgence of the citizen into the public debate, a desire to impose change through citizens".[35] Drawing on the idea that "the digital revolution gives us a stronger voice", he claims that the "primary objective [of his company] is "empowerment". All this cannot be done by an algorithm… There is human input."

In hosting the "*Loi travail : c'est toujours non, merci !*" petition against France's new labour law, this company (in collaboration with Twitter and Facebook) explicitly entered the political arena as a full participant, claiming to offer a "modern" alternative to political parties, trade unions and other kinds of civil society organisation. Change.org today claims to have 9 million users and 2 million individual visitors a month. Does Change.org's hosting function include a human presence? Perhaps. Multiple algorithms? Undoubtedly. Digital tools like those supplied by the firm NationBuilder?[36] That, too, is a possibility.

For the moment, the profit principle of the companies that operate in the "social influence" business is presented as the best guarantee of nonpartisan access to their services. It is true that, in France, NationBuilder's software, for example, is bought and used equally by political parties as disparate as The Republicans, La République En Marche or the French Communist Party. However, things are changing and some of the big digital players are now overtly beginning to move towards a more partisan political engagement.

When work on this report began, it was still a matter of speculation to wonder about the potential problem of the founder and president of Facebook standing as a candidate for the US presidency in 2020s,[37] given that the company holds personal information on 200 million users in the United States.[38] The Cambridge Analytica scandal has shown that we already need to consider the risks posed to democracies, from the United States to India,[39] by a candidate's asymmetrical access to the personal data of a significant proportion of the electorate. This is without question a major ethical and political challenge.[40]

More generally, the ideal of direct digital democracy raises the question of legitimacy, whether ethical or political. Public digital expressions may be numerous without being representative – organised

[35] Olivier Pirot, "Change.org : les pétitions en ligne qui veulent changer le monde", *La Nouvelle République.fr*, 10/06/2017; https://www.lanouvellerepublique.fr/actu/change-org-les-petitions-en-ligne-qui-veulent-changer-le-monde Our translation.

[36] http://nationbuilder.com/software

[37] Xavier de La Porte, chronique "Si Mark Zuckerberg devenait vraiment Président des États-Unis", *France Culture*, 17/01/2017; https://www.franceculture.fr/emissions/la-vie-numerique/si-mark-zuckerberg-devenait-vraiment-president-des-etats-unis

[38] https://www.statista.com/statistics/408971/number-of-us-facebook-users

[39] Barkha Dutt, "Even before Cambridge Analytica, India had already lost the data wars", *Washington Post*, 30/03/2018; https://www.washingtonpost.com/news/global-opinions/wp/2018/03/30/even-before-cambridge-analytica-india-had-already-lost-the-data-wars/?utm_term=.98a41d9037b4

[40] Indeed, this singular moment, which Claude Lefort describes as a "test of a dissolution of the landmarks of certainty", can be seen as the source of a life in community that allows the greatest freedom of opinion; Philip Knee, "Claude Lefort, Montaigne et l'écriture de l'incertitude", *Revue d'histoire littéraire de la France* 2008/1 (Vol. 108), p. .21-36. DOI 10.3917/rhlf.081.0021

groups with a good command of social networks have the capacity to elicit slanted outcomes. Moreover, access to digital public expression remains marked by both technical and sociocultural inequalities. In light of this, it is important to consider the procedural conditions for the construction of consensus between groups with conflicts of interest, as emphasised in the philosophy of "deliberative democracy" initiated, among others, by John Rawls and Jürgen Habermas.[41]

3.3. Can digital sovereignty be reduced to an issue of encryption?[42]

The production, reception, storage and processing of information are less and less controlled by sovereign states, a fact that – beyond the question of the sovereignty of states – raises ethical and legal questions that are both new and complex.

Thus, according to Pierre Bellanger, "*digital sovereignty is control over our present and our future as manifested and guided by the use of information technologies and networks.*"[43] But also: "*By technical and material separation after the Chinese or Iranian model, by means of national level coordination of the encryption of data of national interest for a new form of "encrypted" border control, by a networked operating system that acts as a constitution, or by an insistence that sovereign applications and systems – servers – be located on French territory and the prohibition on the export of data.*"[44]

What is this idea of a new "encrypted" form of border control? Technically, the communication of information, protecting the integrity or confidentiality of data, relies on two essential factors: first, the capacity of an information system (IS) to guarantee that the information it contains and the processes it performs are uncorrupted and confidential; second, the capacity to guarantee that the communications produced by the IS are in fact transmitted, both confidentially and uncorrupted. The guarantee of an information system's qualities relies in particular on its operating system (OS) and the quality of its material components. Today, there are multiple OS, the best-known being Unix, Linux, Windows, MacOSX, ios, Android, VMS, Multics, CP/M, DOS and their many variants. Others are being developed, in particular to manage industrial facilities, household appliances, cars, the components of the Internet of Things, etc., for example RIOT, Contiki, TinyOS.

Designing a "cybersecure" operating system is a particularly complex challenge. As of now (2018), there is no such OS that is proven, robust and has sufficiently extensive functions to be widely usable. However, technology moves fast and extensive functionalities are currently available, with security based on robust and effective encryption capacities.

But the OS is not everything: leaks can also occur at the level of the BIOS (Basic Input Output System) or even the processor. In consequence, the OS and the BIOS need firstly to be redesigned together, in order to make "cybersecure" machines, and secondly the processor itself needs to be armoured.

In this scientific and technical context, the question can therefore be analysed in two different ways.

First possibility, citizens accept that the state has a pre-eminent position that, for reasons of internal security and national defence, guarantees the availability of an OS with the capacity to maintain national sovereignty. This would mean, for example, that state agencies would be able to decipher all communications, while ensuring that they are not decipherable by other entities. Today, however, this security imperative is counterbalanced by the imperative of maximising privacy. In this event, therefore, legislative guarantees and procedures would have to be found to limit state intrusion into

[41] https://en.wikipedia.org/wiki/Deliberative_democracy

[42] This section includes contributions by Didier Rémy, Deputy Scientific Director of Inria.

[43] http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm Our translation.

[44] Pierre Bellanger, hearing of 19 October 2016. Our translation.

communications between individuals, organisations or groups. This first possibility faces several difficulties, which have in fact already come up in the current debate on the use of cryptology and are reflected in the 2017 rulings and reports of CNIL[45] and CNNum,[46] respectively France's data protection and digital transition authorities. Indeed, it means maintaining a sovereign OS (with BIOS and processor), which is very difficult from a technical point of view. Moreover, this solution would mean all IT systems using the same sovereign OS, which again is technically very complex with very practical difficulties. For example, how do you ensure that this OS takes over in the population by replacing OS that are more or less specific to each brand ("native" systems) of computer or telephone? How could a sovereign OS replace all the OS needed for the Internet of Things? Past and recent experiences with open-source word processing software raise doubts. Despite a stated readiness to shift to open-source software, the administration has often sent mixed signals, which have undermined every effort. For example, the French National Research Agency (ANR) required applicants responding to national calls for projects to use macros that were programmed using the *Suite Office*, thereby obliging them all to buy Microsoft software. Another example is the partnership agreement signed on 28 November 2015 between the national education service and Microsoft, giving the company responsibility for training teachers and administrators in digital technology.

This takes us towards a second possibility in which "top-down" national digital sovereignty is replaced by "bottom-up" digital sovereignty, whereby individual users remain in control of and take full personal responsibility for their data and communications. This could be based on the availability of operating systems with the capacity to implement such local digital sovereignty, all maintained by communications encrypted by public protocols with open, verifiable and verified codes. In this context, the notion of "Sovereign Operating Systems" comes into play, in the form of open-source operating systems that guarantee public security and digital sovereignty, while protecting privacy. Apart from the technical difficulties of resolving this very tough problem, the solution obviously raises the question of access to private information by the intelligence services, police or military for security purposes (e.g. antiterrorism, cybercrime, etc.).[47]

Encryption is undoubtedly a very important factor in the sovereignty of a state, but the sharing of this capacity with other entities (scientific communities, businesses, not to say the "fourth estate" of the press and media) may be seen as a recent democratic advance,[48] which it would be a pity to roll back. Moreover, digital sovereignty cannot be reduced to this single question of encryption.

3.4. What attributes of classical sovereignty can still be protected in the digital world?[49]

What happens to the attributes of national sovereignty in a digital – and therefore largely globalised – world?

[45] https://www.cnil.fr/en/node/23701; the French *Commission nationale de l'informatique et des libertés* (CNIL) analyses the consequences of new technologies on citizens' private life with an advisory power, an onsite and offsite investigatory power as well as an administrative sanctioning power.

[46] https://cnnumerique.fr/wp-content/uploads/2015/04/2306_Rapport-CNNum-Ambition-numerique_sircom_print.pdf ; the French *Conseil national du numérique* (CNNum) is an independent advisory commission created in 2011 to hold a national debate on issues raised by digital transformation.

[47] See, for example, the banning of Telegram in Russia or in Iran.

[48] In France, the use of encryption methods was only authorised from 2004, with the Law Regarding Confidence in the Digital Economy.

[49] This section includes contributions by Didier Rémy, Deputy Scientific Director of Inria.

One of the pragmatic limits on national security comes from international law and the treaties between sovereign states. Digital technology requires international standards, with a free and secure flow of information. On these principles, there are large private entities which increasingly aspire to compete with states and assume functions that until recently were a monopoly of states:[50]

- **Maintaining internal security**: facial recognition requires access to a large number of photographs that, for legal and technical reasons, most states do not have. On the other hand, social networks can easily undertake this function. Moreover, some states today export their technological security know-how, for example China to Ecuador or France in particular to African countries.
- **Authenticating individuals**: social media provide authentication services that can certify an individual's identity. At one stage, for example, the United Kingdom considered using people's "Facebook identity" as a national ID. Other Internet companies also provide this type of identity checking and certification service (cf. https://www.civic.com).
- **Minting money**: with cryptocurrencies like Bitcoin,[51] but also with local currencies restricted to a community of interest or a geographical community, national currencies are losing their exclusivity.
- **Land registry**: Google, for example, can help with the collection of land tax in certain countries, such as Greece or a number of African nations, where there is no land registry. Establishing internationally used maps, not necessarily recognised by the UN or the countries concerned, can significantly encroach on the national sovereignty of states in situations of territorial conflict.[52]
- **Air traffic control**: at the end of April 2018, Örnsköldsvik airport in Sweden became the first airport to be controlled from a distance, in this case 150 km, a technology that opens up the possibility of relocating air-traffic controllers (who have civil servant status in France) not only outside airports, but perhaps even outside the country.
- **Handling health data**: the handling of health data originating either in the health system, in social networks, in connected health appliances, in genetic tests from abroad (forbidden in France without a medical prescription) or in the use of data from search engines, is – in numerous countries including France – part of the state's regalian role in the sphere of health.[53]
- **Health research**: the company Calico, for example, wants to decode the human genome in order to find the genes responsible for ageing processes.
- **Attacking and defending**: companies like Zerodium acquire and sell "zero-day exploits"– potential software vulnerabilities that are unknown and consequently not detected by existing

[50] Jean-Gabriel Ganascia, *Le mythe de la Singularité : faut-il craindre l'intelligence artificielle ?*, éditions du Seuil, 2017, pp.107-126.

[51] Blockchain allows bitcoin holders to be sure that the money they have in their possession is authentic and above all that it is actually theirs, in the sense that it has not been transferred to others and cannot be without their consent; see J.-G. Ganascia, "L'État peut-il rester tiers garant à l'heure de la blockchain ?", published in the magazine "L'ENA hors les murs": https://www.aaeena.fr/group/l-ena-hors-les-murs/169/articles/l-etat-face-au-choc-numerique-mars-2018-n-478/23/04/2018/259

[52] Jean-Christophe Victor, *Le dessous des cartes, Asie itinéraires géopolitiques*, Tallandier et Arte éditions.

[53] This is framed in France in particular by the Touraine Act and the laws on bioethics.

countermeasures "– to clients potentially exposed to these risks. Others provide digital defence services for IT sites.

- **Encryption**: specialist firms like ProtonMail or Telegram offer high-quality encryption services, capable of rivalling most encryption (or decryption) methods, including those developed by states.
- **Establishing and preserving legal deeds**: systems based on blockchain technology provide OTC (Over-the-counter) contracts which are currently considered unfalsifiable and could ultimately replace certain legal deeds.[54] Another example, Creative Commons is testing the use of blockchain technologies to register a work and the author's name, specify the licence conditions and track alterations to the work on the Internet.
- **Heritage protection**: in 2009, Google proposed an agreement to digitise all the works in France's National Library, a controversial offer that was ultimately rejected.
- **Deciding on official language(s)**: the language of communication, in particular government communication, is one of the regalian prerogatives. Today, more and more private organisations implicitly require knowledge of English, which is becoming a key factor of integration, since without it, communication becomes very difficult to control.

Each of these attributes of sovereignty is associated with moral values and therefore ethical questions, choices that will differ from one country to another. For example, the definition of cultural heritage and sensitivity to its preservation are not the same in Paris, Santiago or Beijing.[55] Similarly, medical ethics vary according to the balance between individual freedoms and the collective interest, a balance that varies to a certain degree from one culture to another.

It is only once we have established the perimeter of protection of these attributes of sovereignty, that we can tackle acceptable methods and conditions for protecting them.

3.5. Defending digital sovereignty alone or together: war by other means

If there is agreement on the conclusion we have just proposed, should a state respond to it alone? With regard to defence, long considered the very essence of the sovereign prerogatives of regalian power, the change has been remarkable. In France, for example, the last White Paper on defence and national security in 2013, asserts (our emphasis):

"*At the European level, in clarifying the direction that France has decided to take in order to safeguard its security, the White Paper seeks to establish an in-depth dialogue with the EU Member States, calling for a new ambition. This dialogue aims to* ***replace de facto interdependencies with organised interdependencies, thus reconciling sovereignty and mutual dependence****. At the global level, it seeks to explain how the French strategy fits into the broader perspective of its contribution to an international order based on peace, justice and the rule of law.*"[56]

This broader understanding of the political concept of sovereignty, which seeks to "replace de facto interdependencies with organised interdependencies, thus reconciling sovereignty and mutual dependence" seems particularly interesting in approaching the question of digital sovereignty, but is far from universally accepted.[57]

[54] Note that at the time of writing of this report, the properties of the blockchain algorithms have not yet been scientifically analysed. Nobody therefore can currently guarantee their robustness to attack..

[55] F. Koller, "Pékin rase son patrimoine pour les JO", *Le Temps, 4/12/2001; https://www.letemps.ch/culture/2001/12/04/pekin-rase-patrimoine-j-o*

[56] White Paper on Defence and National Security, 2013, p. 12 (emphasis by the writers of the present report); http://www.defense.gouv.fr/portail/enjeux2/politique-de-defense/le-livre-blanc-sur-la-defense-et-la-securite-nationale-2013/livre-blanc-2013

[57] China, for example, remains marked by the memory of the nineteenth century, described as a "century of

Whatever the perimeter chosen (European, Franco-German, or strictly national), we are facing a new question of how to protect digital borders from foreign incursion in a "permanent war". Thus, soldiers now draw up doctrines for the defence of "national digital space" which was, until recently, a *terra incognita* in the law of war.

In 2013, NATO's Estonia-based Cooperative Cyber Defence Centre of Excellence published the first edition of a *Manual on the International Law Applicable to Cyber Warfare* (called "*Tallinn Manual"*). Again supervised by the US lawyer Michael Schmitt (colonel and professor at the *Naval War College*), the second edition of February 2017 includes problems that arise in peacetime, and notably covers the application of sovereignty to cyberspace. It is significant that the question of sovereignty constitutes the very first chapter of the book, which defines it in terms of five rules.[58] The manual also tackles the subject of cyber-espionage in peacetime (rule 32).

A question such as that of intelligence, the epitome of state sovereignty, enables us to measure the "cultural" differences that exist today with regard to the readiness to outsource certain state prerogatives to private commercial firms. Thus in the eminently regalian sphere of intelligence, while openness to the private sector is highly developed in the Anglo-Saxon countries[59] (e.g. *US Cyber Command* or the new British *National Cyber Security Centre*) and in Israel, the attitudes in France (DGSE) and Germany (BND) clearly show the contrast between two attitudes to national sovereignty.

On this subject of intelligence, it is also worth noting that big private sector companies have in the last few years sought to create their own intelligence services. This illustrates how some multinationals now operate like quasi-states.[60]

The example of intelligence shows that the GAFAMI[61] – because of their privileged and massive access to confidential information with "high nuisance value" – represent a very specific category. It is obvious that, despite their equivalent financial muscle, Alphabet-Google or Microsoft moving into intelligence is more of a problem than it would be if an industrial firm like Toyota Motor or a bank like Wells Fargo were to do the same.

humiliation" because of the division of its national territory into zones of influence by foreign powers. It remains attached to a strict conception of the notion of sovereignty and to the principle of non-interference. Likewise, in its international relations, China does not agree to participate in a UN military intervention unless the government of the country concerned gives its prior assent.

[58] Cf. "*Sovereignty*" (p. 11-29), "*Rule 1: Sovereignty (general principle) / Rule 2: Internal sovereignty / Rule 3: External sovereignty / Rule 4: Violation of sovereignty / Rule 5: Sovereign immunity and inviolability*"; http://assets.cambridge.org/97811071/77222/toc/9781107177222_toc.pdf

[59] Even in these countries with a largely "liberal" tradition, confidence in the public/private partnership can be disputed contested. For example, the Swedish Minister of Defence, Peter Hultqvist, who is currently in hot water following an accusation of disseminating confidential information – some relating to defence – after the outsourcing to IBM of the technical maintenance of a public database (https://www.ttu.fr/suede-laffaire-derange).

[60] On this subject, see controversy about certain public-private partnerships agreed by the International Criminal Police Organisation (Interpol) and the very enlightening documentary entitled "*Interpol, une police sous influence ?*"; https://www.arte.tv/fr/videos/061744-000-A/interpol-une-police-sous-influence

[61] GAFAMI for "Google, Apple, Facebook, Amazon, Microsoft, IBM", the Chinese equivalent of which is BATX (Baidu, Alibaba, Tencent, Xiaomi). These companies are not the only ones to collect highly private individual data and there are reasons for concern over the security of the information collected by "social networking" apps. See the article by Judith Duportail, "I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets", *The Guardian*, 26/09/2017;
https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

In his hearing on 8 March 2018 before the deputies on the Defence Committee, the head of the military intelligence directorate noted: "*These days, even states have been overtaken by the financial muscle of certain companies, like Microsoft or Google, which can allocate much greater resources to these developments*."[62]

However, even the French position, where the tendency is to maintain all offensive capacities with regard to cybersecurity within the state, is changing. The text of the draft military planning act, receiving its first parliamentary reading, stated that telecommunications operators could, "*for purposes of security and defence of their information systems*", install devices to detect attacks on their networks.

Digital technology today is pushing us to broaden the paradigm of sovereignty by extending the number of those who possess it, in particular to corporations, in particular to corporations.

[62] http://www.assemblee-nationale.fr/15/pdf/cr-cdef/17-18/c1718052.pdf Our translation.

PART 4: Towards new sovereignties and new actors

As we have shown above, the historical notion of sovereignty is now contested by both individuals and legal entities, speaking on behalf of singular or collective ideas and interests. As we have seen, we find clear expression of the notions of collective sovereignty (national, European,[63] or in the scientific, well-being and health and digital domains),[64] but also sovereignty that is more restricted (to the scale of a company), or even individual.[65] This inversion of the traditional vision of sovereignty – previously conceived exclusively at the scale of a human collectivity – is undoubtedly a change of paradigm. It is a direct consequence of the way that the ontology of notions is being rewritten by digital technology.

In this section, we examine what might be the formalisation and the relevance of notions of digital sovereignty, on the one hand, and of scientific sovereignty, on the other.

4.1. Digital sovereignties, in the plural!

Apart from national sovereignty in the classical/historical sense of the term, we also now speak of European sovereignty, scientific sovereignty, technological sovereignty, economic sovereignty, individual sovereignty,[65] and of course, of digital sovereignty. Thus, in the summary of the fourth *Assises de la Souveraineté Numérique : "Souveraineté numérique et cyber-sécurité"*[66] we see "*three circles of sovereignty"* presented:

"(...) What meaning should we assign to sovereignty? Information is the heart of digital space. It needs to be protected. The spaces of sovereignty are different:

1. *individual sovereignty: what are we prepared to give? To the state? To corporations? What are we not willing to give: protection of our privacy, of our movements, etc. Sovereignty needs to be reinvented.*
2. *Sovereignty of the corporation: its entire wealth is built on data. The exchange of data across the world generates the wealth of trade.*
3. *Sovereignty of the state, our state. It must absolutely be protected."*

Digital technology and the explicit recognition that the role of information is as fundamental as that of matter or energy have revealed a new "digital continent", often also called the "digital ocean", because they share the characteristic of all-pervasiveness and because the legalities relating to the seas and oceans seem analogous to those pertaining to the digital world.[67] We have therefore seen the

[63] "*So if today we must re-forge our Europe,* […] *the goal must be to reforge it around a* ***shared sovereignty****, in other words a Europe that protects our fellow citizens* […]". http://www.elysee.fr/declarations/article/discours-du-president-de-la-republique-emmanuel-macron-lors-de-l-inauguration-de-l-historial-franco-allemand-de-la-guerre-14-18-du-hartmannswillerkopf-en-presence-de-frank-walter-steinmeier-president-de-la-republique-federale-d-allemagne Our translation.

[64] With the emergence of patient communities or communities that form around connected objects.

[65] "[We must] *include the notion of individual sovereignty in our thinking. The citizen or the enterprise must be able to control their data, be fully aware of their values, of the issues, and also ensure dissemination that can be consented and sought.*", in *Synthèse des 4èmes Assises de la Souveraineté Numérique : "Souveraineté numérique et cybersécurité";* http://aromates.fr/public/Synthese%20ASN%202017.pdf. Our translation.

[66] These 4èmes Assises de la Souveraineté Numérique took place in Paris, on 29 March 2017, in the presence of numerous parliamentarians; http://aromates.fr/public/Synthese%20ASN%202017.pdf. Our translation.

[67] The parallel with the maritime metaphor could even be pursued by comparing the Net with the surface waters,

emergence of numerous proposals for the definition and establishment of digital sovereignty.

In France, the issue and the term *digital sovereignty* were explicitly introduced by Pierre Bellanger, first in a text published online in 2011,[68] reproduced in the journal *Le Débat*, then further developed in particular in his book *La Souveraineté Numérique* published in 2014.[69] In it, he sharply condemns the loss of national sovereignty resulting from the appropriation of digital data by state or business entities. Pierre Bellanger's action led to the introduction of an amendment,[70] accepted during the vote on the Digital Republic Act promulgated on 7 October 2016, proposing research into the creation of a Commission for Digital Sovereignty. We would note that here, the concept of sovereignty is understood in the sense of national sovereignty, i.e. sovereignty exercised by the state over the digital domain.

However, the concept of digital sovereignty can be understood in a different way and refer to the possibility, for a given entity (a nation, a corporation, an individual), to control digital attributes (data, information, knowledge, algorithms) of objects that it claims to be entitled to observe, or even to monitor.

The term "control" used here (and elsewhere in this document) does not necessarily mean that the entity possesses (in the sense of full ownership) the objects in question, let alone the digital attributes, in this case the data, of those objects.

For countries like Russia or China, control of data is clearly associated with the requirement that their fellow citizens' data be stored exclusively on national territory. This is not not the case in France or in Europe, where a significant volume of personal data is transferred and stored abroad. When the place of storage is the United States, the Privacy Shield mechanism in place since 1 August 2016 does not protect European citizens from large-scale and indiscriminate data surveillance,[71] which is a source of difficulty in respect to European law, but is permitted by American legislation (e.g. the Patriot Act).

We can see that in this definition, digital sovereignty, understood as "**national digital sovereignty**", i.e. as national sovereignty over digital data, comes into conflict with the entanglement of a globalised world governed by multiple international agreements and norms. As mentioned above, international data law resembles the problem of international maritime law. More prosaically, since the operation of our democracies increasingly relies on public expression via digital media, the capacity for censorship in some societies raises questions (e.g. the debate in Germany on the application of a law obliging Twitter, Facebook or YouTube to delete messages whose content is punishable under criminal law).

At both infranational and supranational level, digital sovereignty can also take the form of "**corporate digital sovereignty**". Here, the corporation should be understood in a broad sense, like that employed by INSEE,[72] which includes non-governmental organisations and foundations. We saw previously

and the Darknet with the depths…. It is interesting that the command of cybernetic operations in the military is very often assigned to admirals, whether in the United Kingdom, France or the US!

[68] "De la souveraineté en général et de la souveraineté numérique en particulier", les Echos;

http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm

[69] Pierre Bellanger, *La souveraineté numérique,* Éditions Stock, 2014, 264 p.ISBN978-2918866213

[70] http://www.assemblee-nationale.fr/14/amendements/3318/CION_LOIS/CL129.asp

[71] https://www.cnil.fr/fr/le-privacy-shield

[72] According to INSSE, France's national institute of statistics and economic studies: "*he company is the smallest combination of legal units that constitutes an organisational unit of production of goods and services*

(section 3.4) that in particular the GAFAMI (or BATX) could claim to control the data that the companies possess, as well as to control the algorithms that they employ to collect and exploit those data. However, we are also seeing the emergence of corporate claims of sovereignty over data that describe or originate in their know-how and their activity as multinationals, as illustrated by certain contents of GTC,[73] or code of conduct initiatives. It is worth noting on this subject that the objective of Europe's General Data Protection Regulation (GDPR)[74] is to create an obstacle to the pursuit for corporate digital sovereignty by the Internet's big players. In the light of previous experience, it is important to be vigilant regarding the implementation of the GDPR: for example, a recently published Code of Conduct for Cloud Infrastructure Service Providers only provides "non-binding recommendations" for its application.[75]

Finally, the notion of "**individual digital sovereignty**" describes the capacity of individuals to control their personal, medical, educational (e.g. school, lifelong learning, etc.), sentimental (photos, letters, etc.) information, in a context where individual views of privacy protection often depend on cultural factors and computer literacy.[76] Awareness of the volume of data concerned often comes only with reports of data theft, such as that which affected 3 billion Yahoo account users in 2013 and, in 2016, the Uber ridesourcing company's 57 million users. Individual autonomy comes into conflict both with national sovereignty, as has always been the case in representative democracies, and with corporate sovereignty, which could be a source of conflict in the future (OpenAccess can thus be seen as a way of rebelling against the sovereignty of corporations, just as the Dark Web is also a form of opposition to the sovereign control of states). However, while in democratic regimes the legal structures are generally able to settle conflicts between the individual and the state, especially in Europe which also has a legal entity arbitrating at the supranational European scale, it is much more difficult to settle conflicts between the individual and the big international corporate players, which lie outside national control.

The claim of sovereignty in these three categories raises difficult questions of law, of legitimacy and ultimately of application. By way of illustration, there is the "non-realisation" so far (at least to our knowledge, in May 2018) of the study commissioned under France's Digital Republic Act of 7 October 2016 on the possibility of establishing a Commission for Digital Sovereignty.

We thus identify the following issues:

I-1 digital sovereignty is not simply a political and economic issue, but incorporates questions that are eminently ethical;

I-2 this ethical issue notably concerns the right of every individual to privacy. The assumption made by some digital corporations that the alienation of this privacy is today tacitly accepted (on the principle that the user's silence signals acceptance of any subsequent use of the data collected) is unacceptable, both from an ethical point of view, and in terms of national or individual

that enjoys a certain decision-making autonomy, notably in the allocation of its available resources."; https://www.insee.fr/fr/metadonnees/definition/c1496

[73] GTC: general terms and conditions of use

[74] This regulation, adopted in 2016, is applicable from 25 May 2018.

[75] Lettr sent by Isabelle Falque-Pierrotin (on behalf of the Article 29 Working Party) to Alban Schmutz (Chairman of CISPE, Cloud Infrastructure Services Providers in Europe) on 23 February 2018; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615033

[76] Jean-Marc Manach, La vie privée, un problème de vieux cons?, Limoges, Ed. Fyp, coll. Présence, 2010, 224 p.

sovereignty;

I-3 the Privacy Shield mechanism or the entry into force, on 25 May 2018, of the General Data Protection Regulation, illustrate the difficult balance of power in particular with corporations established under US law (and the extra-territoriality associated with it). This may mean that the radical measure of requiring the data of European citizens to be stored exclusively on European Union territory should not be ruled out;

I-4 What is true on the individual scale is equally true on the collective scale; whether our vision of collective sovereignty is primarily national or European, there are good reasons to be concerned about the threat that the digital sovereignty of the big Internet players may pose to the democratic functioning of our institutions or in terms of interference in society's choices.

4.2. The case of scientific sovereignty

"Corporate digital sovereignty" is not the only kind that operates within a framework that is both infranational and supranational. Digital sovereignty can also exist in forms of "scientific sovereignty", which are of particular interest to CERNA, whose remit is to bring ethical scrutiny to the research community. We therefore tackle this issue as a subject in its own right.

The scientific community of today values a certain independence and aspires both to autonomy in its institutions and freedom in its research.[77] As Caroline Wagner explains in her book *The New Invisible College*,[78] this situation is recent: the history of science and science funding has been characterised by very different phases. At the beginning of the twentieth century, and in particular after the Second World War, national science was funded by states, with objectives that were both economic and military. Since the mid-1980s, with European projects, science funding has become increasingly supranational, with the result that scientific communities now have their own agendas, independent of those of state actors. Digital further reinforces the autonomy of scientific communities, which are in constant communication on the networks and pursue collective initiatives. Moreover, today, the big private economic players, particularly those in the digital economy, also have the capacity to set up their own research laboratories, some of which can be at least as well funded as the big public research centres, since they have significantly different ways of remunerating and organising research. As a result, in disrupting traditional scientific approaches and practices, the arrival of digital technology contributes to the emergence of a notion of "scientific sovereignty" and raises the question of what it means.

What we understand by "**scientific sovereignty"** here is the control by scientists, in different collective forms (e.g. research laboratory or scientific discipline), of all the information they need to develop knowledge, replicate research, to freely access and freely publish all data, information and knowledge based on their work, within the norms of scientific deontology and integrity.

Digital technology originates directly from scientific and technological advances underway since ancient times, though significantly faster in the last 70 years or so. It is, however, remarkable to see how these digital advances are altering the scientific method itself, as well as the environment of scientific research, without scientists necessarily being aware of it themselves. We are witnessing a scientific revolution that affects practically all scientific disciplines: whereas the classical experimental approach, since the beginnings of the modern age, entailed the design of an experiment to confirm or invalidate a theory, today data can be systematically recorded and subsequently processed by digital techniques, without any *a priori* idea of theory. The term sometimes used for this is e-science or *in silico* experiment, in other words experimentation on data using silicon chips.

Two new paradigms have thus entered the scientific method: in addition to observation, developing theory and designing experiments, scientists now have the capacity to simulate and analyse massive quantities of data at scales that are completely transforming every field of scientific activity. We can,

[77] See COMETS report No. 2018-35 entitled *Liberté et responsabilités dans la recherche académique* and approved on 31 January 2018; http://www.cnrs.fr/comets/spip.php?article255

[78] Caroline Wagner, *The New Invisible College*, Brookings Institution Press, Washington D.C., 2008, 157 p.

for example, make a galaxy evolve before our eyes, reconstruct sparse fragments of manuscripts, simulate a quantum computer before we are able to build one physically, check and in some cases compute the proof of a new theorem, etc. Not a single discipline is untouched by this revolution.

Science is fed by and generates vast masses of data: the knowledge generated, the protocols used, the software, the data from experiments or simulations, the scientific exchanges arising out of the development or validation of knowledge. These masses of data take very different forms. In addition to the traditional texts that document knowledge (dissertations, theses, articles and scientific papers), there are now the terabytes of data generated from astronomical observatories or nuclear physics experiments, but also from the analysis of texts, video and sounds for sociological analysis, or from formal proofs of protocols or programs. Moreover, the data from scientific exchanges itself comes from discussions on online scientific networks. In consequence, the ethics and integrity of the data sharing processes have become a significant issue.[79]

The publication of knowledge constructed by scientists and of their discoveries is emblematic of the challenges of scientific sovereignty. The ongoing digital revolution raises questions of professional and individual ethics and of integrity.

Publishing – in other words making a method, discussions and the results obtained through the scientific approach available to a particular audience[80] – is a fundamental aspect of the work of scientists. Publishing means both adding to the sum of scientific knowledge, construed as a common good,[81] and also enabling others to progress using the new knowledge thus made available. It means laying one's methods open for replication or refutation. It is also, within the context of contemporary scientific "coopetition",[82] about providing the opportunity to assess the quality of the scientific work done by an individual, a team, a laboratory, a research centre, a university, a discipline or a country. This has resulted in the emergence of notions such as "impact factor" applied to scientific journals or "h-index" to measure the influence of scientists. These new tools have been used to do research on the most appropriate ways of quantifying the impact of scientific results and their authors.

The first scientific journals in the Western world go back to the seventeenth century with the creation of the *Journal des Sçavans* in Paris in 1665,[83] a literary and scientific news periodical published at the state's expense. The same year saw the publication, in London, of the *Philosophical Transactions of the Royal Society of London*, the first scientific journal to establish the bases of the peer review mechanism. The service provided by publishing houses to scientists then developed to the benefit of researchers, as evidenced by the enthusiastic letter of thanks sent in 1923 by 23 scientists, including Hilbert and Einstein, to Ferdinand Springer.[84] However, this relationship has now shifted very significantly to the advantage of the publishing houses, which has elicited increasingly heated

[79] See the COMETS recommendation of 7 May 2015 entitled "Les enjeux éthiques du partage des données scientifiques" [ethical issues in the sharing scientific data]: http://www.cnrs.fr/comets/IMG/pdf/2015-05_avis-comets-partage-donnees-scientifiques-3.pdf

[80] Depending on the technicality or the confidentiality of the results, the audience concerned can be the scientific community or subsets of it, specific target communities (e.g. the heads of information systems security in cybersecurity) or else society as a whole (for example on climate change).

[81] See in particular UNESCO's 13 November 2017 revision of its *Recommendation on Science and Scientific Researchers*. In particular, it establishes "academic freedoms" and science as a "common good". Proceedings of the General Conference, 39th session, Paris, 30 October - 14 November 2017. Volume 1: Resolutions, pages 128-141. http://unesdoc.unesco.org/images/0026/002608/260889f.pdf#page=128

[82] A neologism, contraction of "cooperation" and "competition", which expresses the willingness of an entity, in particular a company, to share certain resources (cooperation), while maintaining its autonomy.

[83] https://fr.wikipedia.org/wiki/Journal_des_savants

reactions from the scientific communities (see the Budapest Open Access Declaration of 2002 and the Jussieu Call of 2017).[85]

Open access and more broadly open science are significant issues of scientific sovereignty, at a time when scientific data, information or knowledge are being appropriated by private profit-making entities (such as the GAFAMI or scientific publishers like Elsevier, Springer, IEEE or ACM) or state security agencies (like the NSA). **This appropriation prevents scientists or scientific communities accessing knowledge that enables them to do research at the highest international level.**

One such example is Text and Data Mining (TDM), which requires access to all the available data, information and knowledge on a subject in order to extract from it the content needed for scientific progress. If, for example, a scientist wishes to access all the information available on the interactions between electromagnetism and life, this information is at present primarily controlled by private publishing houses. The latter seek to resell access to the data despite the fact that, firstly, those data were developed and validated by the scientific community itself and, secondly, there is no certainty that their access will be consonant with scientific deontology (since at present the exhaustiveness or accuracy of the data supplied by a publisher in response to a TDM request are neither guaranteed nor verifiable).

A second subject of concern is data on use. Peer review processes, social media discussions, entries in search engines, generate valuable scientific information that today is not available to scientific communities, but here again is pre-empted by special interests.

A third example is the scientific job market, which until now was primarily controlled by the academic world but today is in competition with special interests which possess substantial financial resources and are able to monopolise the work of some of the most productive scientists on an unprecedented scale.

Finally, there is a fact that the resources available to the scientific communities (capacities for simulation, machine learning, experimental labs in biology, chemistry or physics) can today also be controlled by particular entities for economic or strategic purposes.

These factors provide a perspective on the ethical issues associated with the conflicts of values that arise from the implementation of scientific, national or economic sovereignties, each of which can also potentially interfere with the others.

We therefore identify the following issues:

I-5 Digital technology is profoundly changing the scientific method and its environment; the questions of scientific sovereignty that arise from this combine with ethical issues that are crucial in the development of all scientific disciplines;

I-6 The implications of these changes in the scientific framework have profound consequences for all societies across the world and for the future of humanity.

These issues prompt us to formulate the following recommendations:

R-1 In addition to the training in scientific ethics and integrity provided in graduate schools, training programmes in scientific ethics and responsibility should be established for all scientists;

R-2 A mechanism of scientific sovereignty should be established in the academic sector in France and Europe with an open science perspective.[86] In particular, the aim should be for all scientific

[84] See http://www.dam.brown.edu/people/mumford/images/MathAnn_FSpringer.jpg on the blog of David Mumford http://www.dam.brown.edu/people/mumford/blog/2015/WakeUp.html

[85] http://www.budapestopenaccessinitiative.org/read et http://jussieucall.org

[86] Open science (or open research) seeks to make scientific research, data, knowledge and their dissemination freely accessible at all levels of society.

output in which at least one author is affiliated to a French research structure to be deposited in HAL, and that a similar mechanism should be encouraged at European and international level;

R-3 Access should be provided to all the data necessary to the scientific activity of research institutions; in particular, access to Text and Data Mining (TDM) should be provided without restriction for scientific purposes, in all cases according to strict and audited norms of scientific ethics and integrity;

R-4 Specifications should be made for platforms that collect large masses of data (e.g. the GAFAMI and BATX companies) to give scientists access to those data for purposes of open science, according to strict and audited norms of scientific ethics and integrity;

R-5 In accordance with disciplinary specificities, an equitable, discipline-by-discipline open access policy on research data should be established, in concert with national institutions and the big Internet players;

R-6 The professional organisations of the different scientific disciplines should be invited to specify their contributions to the reinforcement of scientific sovereignty;

R-7 National, digital and scientific sovereignties depend on research in the field of cybersecurity, which should therefore be intensively developed;

R-8 With the sponsorship of the European Union and in collaboration with the professional scientific organisations, the Academy of Sciences and the Academy of Technologies, an international "ethics and scientific sovereignty" prize should be established.

4.3 Plenty of other examples!

What we have just explored with regard to the definition and consequences of digital or scientific sovereignties can be extended to other, equally fundamental, domains.

Industrial and technological sovereignty: this is the capacity of an industrial sector, of a company or indeed of a state, to fully control the technological attributes that it claims to control. Today, this sovereignty often intersects with the same entity's digital sovereignty, including not just data, but also the algorithms needed to control industrial processes. The example of Airbus's use of the algorithms developed by Palantir to manage the A350 production chain is typical of the questions that can arise in this domain.[87]

Sovereignty in the health sphere: refers to the capacity of individuals (healthy or not), of hospitals, of a state, of a medical speciality, to fully control the medical attributes they claim to control. Here again, this sovereignty intersects with the digital sovereignty of those same entities, in particular their data and procedures. It also intersects with national sovereignty and relies on the capacity to develop the ethical, normative and legislative foundations needed to establish and maintain this sovereignty.

Sovereignty over data: the analogy with oil has often been mentioned. The capacity to control all data is a fundamental issue of sovereignty, as was emphasised in particular in Cédric Villani's report: "*Data policy must finally be linked to an objective of sovereignty and capitalise on European standards of protection to make France and Europe the champions of an ethical and sustainable AI.*"[88] This sovereignty, which also includes the possibility of controlling the legal framework applicable to these data, represents a subset of digital sovereignty which can usefully be identified in its own right. Note that this sovereignty can be exercised at the level of individuals or of a company or of a state, or indeed of entities such as the European Union.

Sovereignty in the agricultural sphere: this refers to the capacity of an agricultural sector, of an

[87] https://www.palantir.com/build/images/media/Airbus-taps-Silicon-Valley-expertise-to-speed-production-of-A350.pdf

[88] Report by Cédric Villani, p. 25. Our translation.

http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/184000159.pdf individual farm or of the European Union to fully control the attributes that it claims to control. Here again, this sovereignty intersects with the digital sovereignty of those same entities, as is emphasised in particular by OPECST (France’s parliamentary office for the assessment of scientific and technological choices).[89]

We therefore identify the following issue:

I-7 In our modern societies, digital sovereignty intersects with most, if not all, the other sovereignties. This makes it a significant source of conflict.

[89] The role of big data in agriculture: situation and prospects. http://www.senat.fr/rap/r14-614/r14-6141.pdf

CONCLUSION: ethical issues and recommendations

5.1 Sovereignty and ethics at the heart of contemporary geopolitical thinking

There was much talk about sovereignty and ethics at the first Parliamentary Artificial Intelligence Forum, which was held in Paris on 14 November 2017. This event was co-sponsored by the MPs Cédric Villani and Laure de la Raudière, who defined three issues of sovereignty which, in her view, represent a major strategic and political question:

- ✓ The sovereignty of states in the light of the hegemonic temptations that some of them exhibit;
- ✓ The sovereignty of companies;
- ✓ The sovereignty of individuals, which entails their right to privacy.[90]

Concluding the business of the Forum, the Economics Minister declared that artificial intelligence would require us in the years to come to take on a European challenge, but also an "ethical challenge",[91] with "considerable ethical problems with regard to information, with regard to the control of data and (…) digital sovereignty".

It is interesting to note that the Economics Minister very explicitly linked this ethical challenge to the defence of a digital sovereignty that represents both a "national issue and an European issue".

The MP Laure de la Raudière emphasised the importance of this issue with the assertion that "the end of privacy (…) would signal the end of democracy".[92]

We share this view in so far as a human community that no longer had control of its personal data, nor control of the information that informs its judgement, nor the capacity for the digital processing of information, could no longer claim to form an autonomously acting "community of destiny".

In a way, digital technology will show in the rawest way whether or not Europe can claim to embody a project of digital sovereignty of absolutely essential political and strategic importance. If the European Union fails in this objective, **an intermediate Franco-German level could prove relevant**, pursuing around a pragmatic objective the cooperation that began a little more than half a century ago with the signature of the Élysée Treaty. As the French President declared in Davos on 24 January 2018: "Those [in Europe] who want to return to national sovereignty should not block the way for those with greater ambitions."

If European sovereignty cannot be defended at the European scale, or around a Franco-German axis, we would have to return to a national solution which, for a country like France, seems ill-suited to the balance of power currently in place in the world.

Although we can observe hints of a desire for the re-establishment of a Westphalian order, a return to the balances of power between nations, there are also other possible pathways for the governance of the digital world. In this respect, the model of the Geneva Conventions offers one interesting avenue for consideration.

During the Second World War, France experienced the occupation of its territory and the incapacity of its state apparatus to perform its primary regalian function of protecting its citizens. This experience stimulated reflection on the protection of civilian populations that would no longer fall exclusively

[90] https://www.youtube.com/watch?v=Q_V9V3gpzXk&t=9s; cf. 10:36'. Our translation.

[91] https://www.youtube.com/watch?v=j5DIwcne85A ; cf. 09:51' to 10:15'. Our translation.

[92] https://www.youtube.com/watch?v=Q_V9V3gpzXk&t=9s: cf. 10:21'. Our translation.

within the competence of the nation-state.

Drawing on the Roman law tradition of *jus gentium* (law of peoples), this reflection led to the signature, on 12 August 1949, of the Geneva Convention relative to the Protection of Civilian Persons in Time of War. Commonly referred to as the “Fourth Geneva Convention”, it illustrates a form of reversal of the classical vision of sovereignty, with states anticipating their possible impotence (here in wartime) to protect their civilian populations. Protection is transferred to the scale of the person, an “individual sovereignty” attributed to an individual who possesses rights of universal value that can be exercised regardless of his or her citizenship of any given country.

Today, it is significant to note that it is not a state of a group of states, but a private multinational corporation, Microsoft, which has adopted the principle of the Geneva conventions and wishes to see it applied to the digital domain.[93]

Without necessarily going as far as planning a “Digital Geneva Convention”, it would seem wise to **launch an international initiative aiming to extend the principle of “freedom of thought and belief” to a right, for each individual, to monitor uses of technology that might undermine their privacy. More specifically, the aim is to preserve the individual’s capacity to develop their own thinking in a private sphere that goes beyond the legal concept of “private life”.**

“We have entered a new propaganda age”, in the words of the French Minister for Europe and Foreign Affairs.[94] The “orchestration of digital strategies of interference” condemned by Jean-Yves Le Drian is already no longer simply limited to the field of “informational destabilisation” (including the now famous fake news). It will increasingly affect the digital citizen’s very capacity to formulate any thought in a reasonably autonomous manner.

It is therefore time to give a new meaning to the principle that “every individual has the right to freedom of thought” set out in Article 18 of the Universal Declaration of Human Rights of 10 December 1948 (reproduced in Article 9 of the European Convention on Human Rights of 1950 and in Article 10 of the Charter of Fundamental Rights of the European Union, adopted on 7 December 2000). The authors of these texts could not imagine that technology would one day make it possible to know the thought processes, the sensibilities, the most intimate convictions not only of a single individual, but of tens or hundreds of millions of people, or even entire populations.

The latest figures in the Cambridge Analytica affair, which now speak of data being “siphoned” from some 87 million accounts,[95] show that there is a real danger for a democracy in failing to control access to the most private personal data of its citizens. This scandal also illustrates the unprecedented risks created by tools that draw on the knowledge of the psychological and cognitive characteristics of millions of individuals to influence both their shopping habits and their votes. In this year that we celebrate 70 years of the Universal Declaration of Human Rights, an initiative inviting the signatory states to broaden the principle of “freedom of thought and belief” would seem particularly relevant as a reminder that freedom of thought today can no longer be conceived without a digital sovereignty that is capable of ensuring that all individuals are autonomous in their thinking and sovereign in their choices.

This challenge of emancipation at the scale of every individual is linked with the capacity at collective

[93] See the speech on “*The Need for a Digital Geneva Convention*” by the CEO of Microsoft, Transcript of Keynote Address at the RSA Conference 2017, Brad Smith, at the *RSA Conference 2017* held in San Francisco on 14 February 2017; https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf

[94] Speech by Mr. Jean-Yves Le Drian closing the international conference on news manipulation which took place in Paris on 4 April 2018; https://www.diplomatie.gouv.fr/fr/les-ministres/jean-yves-le-drian/discours/article/conference-internationale-societes-civiles-medias-et-pouvoirs-publics-les?xtor=RSS-1 Our translation.

[95] Figure provided by Facebook’s technical director, Mike Schroepfer, in a post published on 4 April 2018; https://newsroom.fb.com/news/2018/04/restricting-data-access

level to be able both to "share and protect", the very project of the "new global contract" promoted by the French president at the Davos Forum. It should prevent the threat, according to the worry expressed by the German Chancellor on the same occasion, that "the disruptive development of digital technology may break societies, bringing the risk of the twentieth century repeating itself".

The digital age will perhaps lead us to reinvent a new *Habeas Corpus* that no longer focuses solely on freedom of the body, but also on freedom of the mind.

Since the freedom to think individually is relative, it needs to be combined with a recognition of the freedom of groups to freely develop collective thinking or, through argument, to strengthen individual thinking. This was particularly the function of academic freedom (*libertas academica*) which opened up a space of freedom in universities where thought developed through confrontation with different objections in the course of private argument. With digital, there is a risk that the total transparency of all debate could eliminate this protection, which would have deleterious effects. Spaces of liberty before publication must therefore absolutely be preserved in order that ideas can develop.

In a world where digital technologies play an ever-growing role, their potential to contribute positively to the common good can only be realised if we clearly set the rules guaranteeing the natural and inalienable human rights defined in 1789: liberty, property, security, and resistance to oppression. These four notions have a particular meaning in the digital age, and specify the nonnegotiable aspects of uses of technology that undermine privacy.

We therefore suggest:

S-1 the launch of an international initiative with the aim of explicitly extending to the digital domain the principle laid down in Article 18 of the 1948 Universal Declaration of Human Rights, which states that "Everyone shall have the right to freedom of thought", a principal reproduced in Article 9 of the 1950 European Convention on Human Rights and by Article 10 of the Charter of Fundamental Rights of the European Union in 2000;[96]

S-2 the launch of a European initiative, or more pragmatically a Franco-German initiative, in parallel with this international initiative, which – on the basis of increased research on cybersecurity and its applications – will provide the means to guarantee the integrity and confidentiality of digital data, in order to guarantee the expression of all sovereignties, whether national, digital, scientific or individual;

S-3 encouragement for the online organisations operating in the political field of "citizen action" and "social influence" (e.g. organisations specialising in the launch of online petitions, such as Avaaz.org, Change.org, SumOfUs, etc.) to make the conditions for the use of personal data transparent easily accessible and intelligible and, in particular, to develop a single, uniform heading for this information (covering the different terms such as *data policy*, *privacy policy*, *confidentiality policy* and *information policy*).

5.2 Educating citizens and raising awareness on digital sovereignty issues

Thinking about digital sovereignty should prompt us to study ways of increasing the resilience of our societies. On 12 March 2018, Mariya Gabriel, European Commissioner for Digital Economy and Society, received the report on fake news and digital disinformation that she had commissioned from a group of some forty experts.[97] This report invites the European Union Member States to make

[96] While Art. 18 of the 1948 text does not place any legal obligation on signatory states, this is not the case for the Charter of Fundamental Rights which, since the signing of the Lisbon Treaty in 2007, is legally binding on European Union Member States. It should be noted that this charter already refers to everyone's "right to respect for his or her private and family life, home and communications" (Art. 7) and a "right to the protection of personal data concerning him or her" (Art. 8).

[97] Report entitled *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*, 44 p.; http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271

knowledge of the media and information environment part of their national education programmes.[98]

We also believe that there is a major issue of citizen education that could take different forms:

- ✓ From primary school,[99] then in secondary school, design a curriculum that raises awareness of the issues of cybersecurity and familiarises students with the tools needed to protect their privacy and to recognise the different forms of manipulation or indoctrination facilitated by digital media.

  This proposal is close to that formulated in the new national plan for the prevention of radicalisation announced by the French President of the Republic, which calls for "*Students to be protected against the risk of online radicalisation and against conspiracy theories, by making education in media and information a standard part of the curriculum, while at the same time developing their critical thinking and the culture of debate".*[100] However, we have some concerns about the invitation to "*involve Internet companies in the protection of citizens*" (p. 10 of the press file) in this national "Prevent to Protect" programme, if this involvement does not include in-depth reflection on the ethical and political implications. This is particularly true when in a "*fight against algorithmic confinement* ", this collaboration includes a call for the Internet companies to contribute to "*promoting an effective counter-discourse*" (measure No. 14). If the problem of the lack of differentiation and hierarchy of information is not tackled – and without an effort to establish a truth based on rational thinking – any counter-discourse seems destined to fail, or even to become counter-productive.

- ✓ Continue the effort of education within the framework of a future French "universal national service" which seems well-suited to talk about cybersecurity, but which needs to be re-situated within a broader concept of resilience. The objective would indeed be to talk about the societal issues of sovereignty in the digital age (taking into account the problems noted in the previous point).

- ✓ As well as educating young people, ways also need to be found to reach the whole population (which gives a particular role to the media but also necessarily to the scientific community). Alongside civil society and media initiatives,[101] there is also a new kind of state role here in reinforcing the resilience of our fellow citizens with respect to fake news or other forms of manipulation that exploit digital media. The pioneering initiatives of certain European countries in this respect[102] are worth studying.[103]

[98] *Ibid*., p. 37.

[99] Drawing on feedback from local initiatives such as that led by Rose-Marie Farinella with CM2 (final year primary) classes:

http://www.cafepedagogique.net/lexpresso/Pages/2016/12/14122016Article636172963871740159.aspx

[100] Press pack, Measure No. 9 p. 10, available at:

http://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2018/02/2018-02-23-cipdr-radicalisation.pdf Our translation.

[101] Such as, in France, the Décodex of the *Monde* newspaper (http://www.lemonde.fr/verification/), the "Journalism Trust Initiative" (JTI) launched at the beginning of April 2018 by the Reporters without Borders organisation or the podcast prepared jointly by *France Info* and *France Culture* to combat fake news in the scientific domain, accessible from the end of April 2018;

http://www.lemonde.fr/economie/article/2018/03/19/franceinfo-et-france-culture-s-allient-contre-les-fake-news_5273020_3234.html

[102] See the documentary "Prague face à la propagande de Poutine" broadcast on Arte on 14/11/2017 or the article by Pauline Moullot "Contre les "fake news", le tacle tchèque" published in *Libération* on 21/08/2017.

Several companies have also announced that they are working on the subject of "*affective computing*" in order to better understand the mechanisms of empathy and, thereby, "to be able to combat fake news".[104] Others claim to be able to detect fake news with so-called "fact checking" software. In this respect, it is noteworthy that the report on disinformation that the CONNECTED division of the European Community has just published is based entirely on technological solutions to which representatives of the big Internet players, in particular Google, Facebook and Twitter, have contributed.[105] It would perhaps be naive to rely on digital companies alone to defend the public interest, the law and liberal democratic values. The fiscal behaviour of these companies should encourage us to look critically at the sincerity of such promises. Not to mention that they too often elude their responsibilities in the dissemination of fake news, since its proliferation depends in part on a business model founded on "clickbait", which rewards a piece of news on the basis of the number of clicks it receives.

Research into the mechanisms of empathy is a way to sell commercial products and services or to combat hostile propaganda. The markets associated with opinion shaping activities are quite disparate in scale, according to whether their purpose is commercial or political. It is doubtful whether a company will prioritise a public interest service, even a paying service, over a more lucrative economic activity.

More fundamentally, it should be remembered that the strategic objective of the "fake news" disseminated in liberal democracies is not so much to shape opinion as to generate doubt. Governments cannot confine their responses to the emotional register alone and abandon all attempts to recapture the field of education and rational and scientific argument.

<u>We therefore suggest</u>:

S-4 from primary school, then in secondary school, design a curriculum that raises awareness of the issues of cybersecurity and familiarises students with the tools needed to protect their privacy and to recognise the different forms of manipulation or indoctrination facilitated by digital media;

S-5 within the framework of a future "universal national service" specify the societal issues of sovereignties in the digital age;

S-6 with the support of the media and the involvement of the scientific community, raise awareness in the whole population in order to reinforce the resilience of our citizens with regard to fake news and attempts at manipulation via digital media.

5.3 Digital sovereignties, ethics, science and technology

As we have seen, national, digital and scientific sovereignties give rise to ethical challenges and fundamental responsibilities.

Paraphrasing the op-ed published in the digital version of *Le Monde* in December 2017,[106] we find ourselves today in a situation similar to that which in 1983 prompted France to play a pioneering role

[103] On this subject, see COMETS report No. 2018-37 published in April 2018, entitled *Quelles responsabilités pour les chercheurs à l'heure des débats sur la "post-vérité"* [What responsibilities for researchers in the era of debate on the "post-truth" world].

[104] According to Philippe Bournhonsque, technical director of IBM-France, speaking at the symposium on "L'héroïsme à l'ère de l'IA" [heroism in the AI age] held at the École militaire on 18/12/2017.

[105] *A multi-dimensional approach to disinformation — Report of the independent High level Group on fake news and online disinformation*, Directorate-General for Communication Networks, Content and Technology, March 2018, ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271

[106] "Il faut créer un comité national d'éthique du numérique", *Le Monde*, 14/12/2017; LE MONDE | 14.12.2017 à 11h22 • Mis à jour le 15.12.2017 à 09h35. http://www.lemonde.fr/idees/article/2017/12/14/il-faut-creer-un-comite-national-d-ethique-du-numerique_5229661_3232.html

with the introduction in 1983 of a national ethical consultative committee (CCNE) for the life sciences and health, tasked with reflecting on the ethical implications arising from our increased scientific and technical capacities in these domains. This committee organises the public debate in a transparent and structured way, within the framework of the law. As a result, though advisory, its opinions are treated seriously by society and by the legislature.

It is therefore essential to move quickly to create a national ethical consultative committee for digital sciences, technologies, practices and innovations. To quote the op-ed: "*The priority now is to connect the short term, the timeframe of industrial and economic competitiveness, with the long term, the timescale of human beings and of a "desirable future". Thus the independent and consultative CCNE for the digital domain would coordinate with the sectoral industrial committees. The management of these issues is, for France and Europe, a question of sovereignty and democracy, without which our continent will depend on decisions that will be taken elsewhere, based on cultures or ethical, economic, industrial and social considerations beyond our control.*

France needs to be a pioneer in the domain, as it was in the regulation of personal data and in the ethics of the life sciences and health. It needs to create, immediately and under the aegis of the President of the Republic, a national ethical consultative committee for digital sciences, technologies, practices and innovations."

This recommendation is also made in the previously cited report by Cédric Villani.

As we noted in the description of scientific sovereignty, significant conflicts can arise from different visions of the notion of progress and of the values underlying scientific development. Different cultural or political conditions can lead to the implementation of scientific developments whose ethics do not necessarily attract international consensus. One example might be genetic manipulations made possible by progress in genomics and bioinformatics that significantly modify the physiological or intellectual capacities of humans or animals. This is primarily a matter of ethics and national and scientific sovereignties, but it also affects all our societies.

We therefore suggest:

S-7 the creation of a national ethical consultative committee for digital sciences, technologies, practices and innovations;

S-8 the development of a doctrine and a strategy of French and European influence and of the resources to argue for them in all the relevant national and international organisations (EC, Unesco, WHO, standardisation bodies (ISO, AFNOR, IEEE,…)).

5.3 Summary of issues, recommendations and suggestions

We have identified in particular the following **issues**:

I-1 Digital sovereignty is not simply a political and economic issue, but carries within it questions that are eminently ethical;

I-2 This ethical issue notably concerns the right of every individual to privacy. The assumption made by some digital corporations that the alienation of this privacy is today tacitly accepted (on the principle that the user's silence signals acceptance of any subsequent use of the data collected) is unacceptable, both from an ethical point of view, and in terms of national or individual sovereignty;

I-3 The Privacy Shield mechanism or the entry into force, on 25 May 2018, of the General Data Protection Regulation, illustrate the difficult balance of power in particular with corporations established under US law (and the extra-territoriality associated with it). This may mean that the radical measure of requiring the data of European citizens to be stored exclusively on European Union territory should not be ruled out;

I-4 What is true on the individual scale is equally true on the collective scale; whether our vision of collective sovereignty focuses on the national or European scale, one cannot but worry about the threat that the digital sovereignty of the big Internet players may pose to the democratic functioning of our institutions or in terms of interference in society's choices;

I-5 Digital technology is profoundly changing the scientific approach and the scientific environment; the questions of scientific sovereignty that arise from this combine with ethical issues that are crucial in the development of all scientific disciplines;

I-6 The implications of these changes to the scientific framework have profound consequences for all societies across the world and for the future of humanity;

I-7 In our modern societies, digital sovereignty intersects with most, if not all, the other sovereignties. This makes it a significant source of conflict

These issues prompt us to formulate the following **recommendations**:

R-1 In addition to the training in scientific ethics and integrity provided in graduate schools, training programmes in scientific ethics and responsibility should be established for all scientists;

R-2 A mechanism of scientific sovereignty should be established in the academic sector in France and Europe with an open science perspective. In particular, the aim should be for all scientific output in which at least one author is affiliated to a French research structure to be deposited in HAL, and that a similar mechanism should be encouraged at European and international level;

R-3 Access should be provided to all the data necessary to the scientific activity of research institutions; in particular, access to Text and Data Mining (TDM) should be provided without restriction for scientific purposes, in all cases according to strict and audited norms of scientific ethics and integrity;

R-4 Specifications should be made for platforms that collect large masses of data (e.g. the GAFAMI and BATX companies) to give scientists access to those data for purposes of open science, according to strict and audited norms of scientific ethics and integrity;

R-5 In accordance with disciplinary specificities, an equitable, discipline-by-discipline open access policy on research data should be established, in concert with national institutions and the big Internet players;

R-6 The professional organisations of the different scientific disciplines should be invited to specify their contributions to the reinforcement of scientific sovereignty;

R-7 National, digital and scientific sovereignties depend on research in the field of cybersecurity, which should therefore be intensively developed;

R-8 With the sponsorship of the European Union and in collaboration with the professional scientific organisations, the Academy of Sciences and the Academy of Technologies, an international "ethics and scientific sovereignty" prize should be established.

Moving outside the primary framework of CERNA's role, which is to address the French scientific community, we believe it useful to formulate the following **suggestions**, which are more political in nature and international in scope:

S-1 Launch of an international initiative with the aim of explicitly extending to the digital domain the principle laid down in Article 18 of the 1948 Universal Declaration of Human Rights under which "Everyone shall have the right to freedom of thought", reproduced in Article 9 of the 1950 European Convention on Human Rights Convention and by Article 10 of the Charter of Fundamental Rights of the European Union in 2000;

S-2 Launch of an European initiative, or more pragmatically a Franco-German initiative, in parallel with this international initiative, which – on the basis of increased research on cybersecurity and its applications – will provide the means to guarantee the integrity and confidentiality of digital data, in order to guarantee the expression of all sovereignties, whether national, digital, scientific or individual;

S-3 Encouragement for the online organisations operating in the political field of "citizen action" and "social influence" (e.g. organisations specialising in the launch of online petitions, such as Avaaz.org, Change.org, SumOfUs, etc.) to make the conditions for the use of personal data transparent easily accessible and intelligible and, in particular, to develop a single, uniform heading for this information (covering the different terms such as *data policy*, *privacy policy*, *confidentiality policy* and *information policy*);

S-4 From primary school, then in secondary school, design a curriculum that raises awareness of the issues of cybersecurity and familiarises students with the tools needed to protect their privacy and to recognise the different forms of manipulation or indoctrination facilitated by digital media;

S-5 Within the framework of a future "universal national service", specify the societal issues of sovereignties in the digital age;

S-6 With the support of the media and the involvement of the scientific community, raise awareness in the whole population in order to reinforce the resilience of our citizens with regard to fake news and attempts at manipulation via digital media;

S-7 The creation of a national ethical consultative committee for digital sciences, technologies, practices and innovations;

S-8 The development of a doctrine and a strategy of French and European influence and of the resources to argue for them in all the relevant national and international organisations (EC, Unesco, WHO, standardisation bodies (ISO, AFNOR, IEEE,…)).

ACKNOWLEDGEMENTS AND INDIVIDUALS CONSULTED

We are very grateful to the following individuals, whom we consulted on these subjects:

- *Pierre Bellanger*, CEO of SkyRock;
- *Bernard Benhamou*, General Secretary of Ithe nstitute of Digital Sovereignty;[107]
- *Peter Burgess* Chairman of the Ethics Advisory Group (group set up by the European Data Protection Supervisor, Giovanni Buttarelli) ;
- *Guillaume Poupard* General Director of the National Information Systems Security Agency;
- *Henri Verdier* Chief State Data Officer, France.

Apart from these hearings, on Monday 3 July 2017, zt the Mines-Télécom Institute, we organised a CERNA day entitled "sovereignties and digital sovereignty". We would like to thank those who spoke at that event:

- Vice-Admiral *Arnaud Coustillère*, who at the time held the post of general cyberdefence officer in the Defence Department (currently director general of information and communication systems in the same Department)
- *Tristan Nitot*, former Chairman of Mozilla Europe and at that time Chief Product Officer at Cozy Cloud;
- *Pauline Türk,* Professor of public law at Nice Sophia Antipolis University.

We would also like to thank the people who attended the event on 3 July 2017 who were asked to take part in four workshops to debate several themes central to this report. These debates continued at the synthesis meeting held at Inria in Paris on the afternoon of 20 November 2017.

[107] https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany/