Summary

Digital technology and fundamental rights

Digital technology presents a problem for fundamental rights insofar as it increases the amount of data generated and results in a generally networked world; whilst it is not a negative phenomenon in itself, it raises issues around the content of fundamental rights and how they are implemented. It undoubtedly increases individuals' capacity to enjoy certain rights, such as freedom of expression and freedom to do business, but at the same time it undermines others, such as the right to privacy or the right to security.

The Conseil d'Etat's annual study comes at a time when the phenomenon has taken on a new dimension: a threefold upheaval is underway, in technical innovation, in the economy and in society's understanding of digital technology, and it is raising further questions on fundamental rights.

This study will first examine how the rise of digital technology has already prompted the recognition of new fundamental rights and freedoms and changed the conditions under which they are exercised (part 1) and then show how the ambivalence of digital technology is forcing a rethink of how such rights should be protected (part 2). Finally, it puts forward 50 recommendations to ensure that digital technology supports both individual rights and collective interests (part 3).

I. – The rise of digital technology has prompted the recognition of new fundamental rights and changed the conditions under which they are exercised

I.1. The rise of digital technology implies a technological, economic and social revolution

Digital technology is defined as the representation of information or physical elements (images and sounds) by a finite number of discrete values, most often represented in binary form by a series of 0s and 1s. Its transformative power is based on its capacity to express disparate realities (sounds, images, texts, human behaviours, industrial processes, etc.) in a common universal language, opening up the possibility of treating them systematically and relating them to each other. The result is a series of technical, economic and social changes.

Technical changes arise from the fact that machines are networked and that the world becomes a source of data generation. The development of networks of machines was made possible by the architectural decisions taken when the internet was being designed in the 1960s and 1970s, namely openness, which allows any local network to be connected to the internet without being controlled by a central authority, and neutrality, which means that the routers used in interconnection nodes are indifferent to the content of the message. These decisions have enabled the internet to expand globally, to the point where it now has three billion users. The world as a source of data generation is driven by the growth in the number of users, the processing power of computers and the increasingly diffuse presence of connected collection points.

Strictly defined, the **digital economy** is made up of a small number of specialist sectors such as telecommunications, software development and computer services and engineering companies; today, however, it has gone far beyond this and is now transforming almost all areas of activity, from cultural industries to the press, trade and distribution, the hotel industry, public transport, financial services, the automotive sector, the construction industry, etc. Digital technology is demonstrating its capacity to re-write the rules of the game and challenge the *status quo* in all these sectors. The business models of firms in the digital technology sector present specific characteristics: a focus on growth rather than short-term profitability, strategies to redefine the boundaries of the markets in which they operate, platform strategies that allow them to act as a gateway for consumers, and finally, intensive use of data, particularly personal data, to generate value.

The effects of digital technology are also transforming social relationships. Digital technology acts as a catalyst for collaboration, which is manifested in various forms, such as the development of data-sharing services, content-sharing platforms, social networks, etc. It fosters participation and transparency in the actions of public authorities. Its impact on social norms has stirred up a debate, particularly in relation to privacy. Those who advocate moving beyond the desire for privacy, in favour of a trend towards "self-publicity", find themselves in opposition to those who maintain that the desire for privacy has not disappeared but simply changed its substance: it is no longer a question of being "left in peace" and free from intrusion, but also of managing one's own image and reputation.

I.2. Digital technology has prompted the recognition of new fundamental rights: the right to protection of personal data and the right to internet access

The right to protection of personal data (a) and the right to internet access (b) have emerged in response to the questions posed by the rise of digital technology. Although there are often presented as being attached to the right to privacy and to freedom of expression respectively, in reality the issues involved are broader and can be seen as autonomous fundamental rights.

(a) Despite its short history, the right to the protection of personal data has seen a fundamental upheaval in the issues associated with it: the authors of the "Tricot Report" in June 1975, whose main concerns centred on the consequences of the creation of large databases of administrative information, could not have envisaged either the rise of the internet, the processing power of mobile devices or the economic value assigned to data. The legal framework that emerged from these reflections, however, has proved highly stable, giving rise to just one significant reform, which was required to transpose Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 into national law, and which notably shifted the emphasis from the public to the private sector.

The various standards applicable in respect of the protection of personal data (the French Constitution, Council of Europe Convention no. 108 of 28 January 1981, the Charter of Fundamental Rights of the European Union, Directive 95/46/EC and the French data protection act of 6 January 1978 as amended) now agree on the **principal safeguards for the protection of personal data**:

- principles related to data quality (fairness of collection, legitimate purposes, proportionality and retention period)

- requirement for the consent of the person concerned or another legitimate basis provided for in law;

- prohibition on collecting so-called sensitive data, except in particular circumstances as provided for in law;

- rights to information, access, correction and opposition;

- a security obligation on the data controller;

- the existence of an independent regulatory authority.

These principles form the basis of a European law on personal data, which is substantially different from US law.

(b) The United States Supreme Court was the first sovereign jurisdiction to be asked to examine the **issues of internet access** in relation to freedom of expression in the case of *Reno, Attorney General of the United States vs American Civil Liberties Union (ACLU)* of 26 June 1997. In France, the Constitutional Council has given judgment in a case challenging the law supporting the dissemination and protection of works on the internet; in this instance, it judged that the freedom of communication protected by article 11 of the Declaration of the Rights of Man and the Citizen "implied the freedom to access such services" (judgment no. 2009-580 DC of 10 June 2009, §12).

Recognition of internet access as a fundamental right imposes an obligation to guarantee equality of treatment for individuals and businesses in relation to such access: this is the issue underpinning the debates on "net neutrality", a concept formulated for the first time in 2003 by the American lawyer Tim Wu. Net neutrality implies that all communications operators treat all data streams on the internet equally, regardless of content. This reflects the original architecture of the

internet, which is based on the principle of "best effort": each operator must do its best to ensure the transmission of all packets of data passing through its network, with no guarantee of achieving a specific result and without discrimination. Several technical, economic and political factors, however, mean that operators do differentiate how packets are treated, based on their content. The purpose of the debates on net neutrality is to decide whether this principle should be incorporated into positive law in order to restrict the possibility of differentiation. These debates cover technical, economic and political issues.

I.3. Digital technology has brought about profound changes in the legal situation of several fundamental freedoms

The rise of digital technology has clearly had a positive impact on the exercise of certain rights, whilst raising doubts over some aspects of their legal situation: this is the case with freedom of expression (a) and the freedom to do business (b). For other rights, such as the right to security (c) and intellectual property rights (d), digital technology appears to present more of a risk, which legislators need to tackle.

(a) Whilst **freedom of expression** is the fundamental principle common to all means of communication, the legal system that defines how it can be exercised varies depending on the medium used. Until the emergence of the internet, there was a perfect match between the form of expression (press, phone calls and audiovisual communication), the technical medium used and the legal system applicable to it. The internet calls these distinctions into question insofar as it enables content ranging from private correspondence, the press and audiovisual sources to be disseminated via the same medium, a phenomenon often known as "convergence".

The legal system governing freedom of expression on the internet has been relatively stable in France since act no. 2004-575 of 21 June 2004, the so-called Act on Confidence in the Digital Economy (LCEN). Reflecting the architecture of the internet, it draws a clear distinction between the infrastructure layer and the content layer. The LCEN defined two major categories of actor for the latter: publishers on the one hand, who are subject to a very similar regime to the press, and hosting providers on the other, who are governed by less stringent requirements in terms of civil and criminal liability than publishers, since they are viewed as not having control of the content accessible via the sites they host.

The rules governing internet communications, either the requirements for publishers or *a fortiori* for hosting providers, are thus characterised by a degree of liberalism that distinguish them from those governing audiovisual communications; this, in turn, introduces a requirement for prior authorisation combined with various obligations for content providers. The increase in audiovisual consumption on the internet, in particular of films and television series, raises new questions over this distinction, which may constitute a distortion of competition and undermine the French policy of support for creating and producing cultural content.

The internet also raises new questions on limits to freedom of expression and combating illegal content. The constitutional and convention texts that guarantee freedom of expression all recognise the possibility of imposing certain limits on it and the internet does not in itself challenge either the existence of such limits or their impact. Nonetheless, the specific characteristics of the internet raise questions about the effectiveness of the measures taken by the public authorities to counter illegal content and about the role assigned to private-sector players in combating such content. Whilst the involvement of internet intermediaries may seem beneficial in terms of ensuring effective protection of public interests such as combating xenophobia or protecting minors, it raises issues about legitimacy.

(b) The economic upheavals caused by digital technology have an impact on the law of economic activities. **Freedom to do business** now implies the right to a digital existence. The law and case law now guarantee what could be classified as the "right to a digital existence" for a business, which comprises several elements: the right to a domain name, the right to provide services on the internet and the right to use certain instruments such as advertising, encryption or electronic contracts.

The changes associated with digital technology complicate the implementation of two forms of managing the freedom to do business, the general regulation of competition and the sector-specific regulations applicable to certain activities. Firstly, there is evidence in certain sectors of the digital economy of a gradual concentration of the market around one or more pre-eminent players, a phenomenon favoured by increasing economies of scale, network effects and the central role of platforms. Dominant players are prompted to constantly extend their activities to new services and take over emerging operators who may compete with them.

The digital economy is also causing an upheaval in numerous sector-specific regulations insofar as established players are being confronted with new participants, who dispute whether such rules apply or whose business model is based on a different approach. This is particularly relevant in the areas of telecommunications, books, hotels, taxis and legal assistance.

(c) Digital technology is enabling or driving new types of security attacks, which require legal responses. It is also giving the police new resources, which call for new safeguards to maintain the **balance between protecting public order** and **personal freedom.**

Digital technology may be the target of security attacks aimed at gaining access to confidential data, destroying or altering data, preventing the normal operation of the system or using computer resources without their owner's knowledge. France's act no. 88-19 of 5 January 1988 on computer fraud, known as the "Loi Godfrain", punishes acts of fraudulent access to an "automated data processing system", attempts to prevent their operation and fraudulent changes to or removal of data. Neither the state nor "operators of vital importance" (OIV) are immune from increasing dependence on information systems for their operations. In order to

deal with such attacks, they have supplemented the existing system of criminal sanctions by adapting their tangible resources (including the creation in 2009 of a specialist agency, ANSSI) and legal options (with power given to the Prime Minister by law to set the security rules for information systems that OIVs must comply with). Digital technology can also be used to undermine security: whilst it cannot be held responsible for types of crime such as counterfeiting, fraud or paedophilia, it makes them easier to perpetrate and is allowing new forms to emerge.

Conversely, digital technology increases the effectiveness of the police, the administrative authorities and the intelligence services. It also improves the effectiveness of their existing working methods, such as files, using biometric data or video surveillance. Digital technology also opens the door to new investigative methods, in particular monitoring electronic communications and the use of new ways of exploiting data associated with the concept of "Big Data".

The legislature has also introduced safeguards in order to set limits on the new resources available to the police and intelligence services, in particular for:

- the use of security files, which are specifically controlled by the law of 6 January 1978 as amended;

- video surveillance, which is subject to an authorisation system under the act of 21 January 1995;

- interception of communications: the act of 10 July 1991 drew a distinction between judicial interceptions and administrative interceptions for security purposes; the act of 23 January 2006 supplemented these rules on intercepting the content of communications with rules on retaining and accessing metadata (i.e. data about the people involved in a call, how long their conversation lasted and their location).

(d) **Intellectual property law** has been extended to elements derived from digital technologies, software and databases; it thus plays a fundamental role in the digital economy. The traditional prerogatives of copyright and rights to reproduction and representation have proved flexible in their application to digitisation and dissemination on the internet.

That said, the internet has a tendency to ignore intellectual property law, by making it significantly easier to reproduce and disseminate works with complete disregard for copyright and associated rights. The public authorities have reacted by combining prevention (through using and providing legal protection for "technical protection measures", preventing copying and notifying hosting providers about illicit content), suppression (with the introduction of a "graduated response" system under the acts of 12 June 2009 and 28 October 2009) and promoting lawful use.

I.4. The internet is not immune from the power of the state either under the law or in practice, but presents it with new challenges

Contrary to what its pioneers had hoped, the internet is not a space where the law does not apply. The two assumptions underlying such a libertarian approach –

states' lack of legitimacy for regulating the internet and their inability to do so – have not been confirmed. **States have no less legitimacy in legislating on digital networks** than they do in any other area of human activity. States' capacity to exercise their power over the internet is now well established. The most extreme illustration is found in the practices of non-democratic states, which manage to prevent their citizens' access to the internet to a significant extent. States where the rule of law prevails also exercise restrictive power over the internet, within the boundaries defined in law and under the control of the judiciary, for example when the courts order the withdrawal of a domain name or delisting of a site.

The fact that a state exercises power over the internet does not mean that it does not face **particular difficulties** in doing so. These are primarily related to the form of **governance of the internet**, defining the **applicable law** and the **effectiveness** of state interventions.

Whilst previous technological innovations (telecommunications, aviation, etc.) gave rise to the creation of specialist intergovernmental organisations, the governance of the internet is distinguished by the absence of a central authority and the role played by several private-sector bodies, acting primarily on the basis of soft law, and in which the United States plays a leading role: ICANN for domain-name management, IETF and W3C for defining technical standards, and the Internet Society and Forum for the governance of the internet and dealing with the political, economic and societal questions associated with it. States are simply one group of stakeholders amongst others in this "multi-actor" model.

By making content and services available all over the world accessible to internet users in all countries, the internet has created numerous conflicts between the legal systems of different countries and thus presented them with a twofold problem: on the one hand, the complexity of the rules of international private law, which determine the applicable law and competent court, is a source of uncertainty; on the other, these rules can designate foreign jurisdictions and laws. The state thus has to face the possibility that its laws on protecting personal data, freedom of expression or intellectual property are not necessarily applicable to all the situations it wishes to govern.

Finally, the internet poses three specific problems that can undermine the effectiveness of state interventions: the ease of recreating a website that has been found to be involved in illegal activity; the necessity of securing enforcement of administrative or court decisions by foreign states; and the discrepancy between the speed at which the digital world is changing and the time taken for institutional and court processes.

**

Two trends are emerging from these multiple changes in the law governing digital technology and determining how the protection of fundamental rights needs to be re-examined: the fact that digital technology is creating new spaces in which to exercise freedoms, in particular of expression, association and sociability; and the strategic issue of fierce competition between states and between economic actors.

II. – The ambivalence of digital technology requires a re-examination of the protection of fundamental rights

The law has already undergone a profound transformation in response to the digital explosion. It has not, however, reached a point of equilibrium. Questions on the relevance of the legal rules governing fundamental rights are being asked as fast as the innovations driven by digital technology are appearing. The difficulty in answering them comes from the **intrinsic ambivalence** of the digital phenomenon: the fact that it is opening up new spaces in which to exercise freedoms whilst at the same time posing risks to them. Heavy-handed intervention by the legislature intended to **prevent the negative aspects** of digital technology **risks hindering its positive potential** at the same time. To overcome this difficulty, we need to re-think how we protect fundamental rights in order to adapt them to the explosion of data, the unprecedented role of the major "platforms" and the transnational character of the internet.

II.1. The explosion in the use of personal data and the risks associated with it are forcing a re-examination of protection

➔ *Risks associated with the explosion of personal data*

Since the adoption of the act of 6 January 1978, the sources and types of personal data in circulation have diversified considerably. Data are no longer only collected by organised entities (such as administrative authorities, businesses and associations) but also published online by individuals themselves or by third parties, or gathered automatically. They no longer relate simply to the individual's objective characteristics (age, gender, profession, etc.) but can include information about their tastes, opinions, relationships, travel, biological traits or physical symptoms.

If all this information were simply disseminated to the people who gathered it, the risks to privacy would undoubtedly be limited. The dynamics of the digital economy, however, mean that they are combined with others. Digital technology has driven the emergence of new actors such as search engines or social networks, which function as repositories of whole swathes of our personal lives. Advertising plays a particular role in this: the greater the amount of information included in an individual's "**profile**", the more the advertising aimed at them will potentially be relevant. Major digital businesses have embarked on diversification strategies, one of the aims of which is to increase the amount of data held on each individual. There are also actors who specialise in collecting and reselling data, known as **data brokers**; the largest of these claims to hold data on 700 million people all over the world.

Such widespread dissemination of personal data and the tendency for economic actors to combine them present **risks** for individuals, which the study groups into **six categories**: dissemination of personal data outside the control of the individual

concerned; increasingly frequent receipt of increasingly targeted, personalised advertising; the development of abusive commercial practices, consisting of customer differentiation based on the use of their data; reputational risks, which can lead to restrictions on access to insurance, credit and employment; malicious use, causing direct harm to people or property; and the use of personal data by the public authorities for the purpose of safeguarding public order and national security, where such use is excessive.

➔ *A legal framework whose fundamental principles remain relevant but whose mechanisms require significant reform*

The new risks associated with digital technology raise questions over the relevance of the current legal framework for the protection of personal data. **The fundamental principles of data protection still resist these questions, however**:

- **A broad definition of personal data** (in particular, covering IP addresses and "profiles" used in relation to online advertising), as advocated by the G29, is needed to ensure protection for individuals but is the one used in French case law.

- **The principle of defined purposes** lies at the heart of the confidence people have in the services of a digital company. It is this principle that ensures that personal data are not simply treated as ordinary goods: they can be traded, but the purchaser's right of ownership is limited by the individual's rights over their own data, which implies that their use must be limited to the purposes for which they were initially collected.

- **The principles of proportionality and limitation on retention periods** arise from this first principle.

- Principles of fairness in collection and the accuracy of data processing are simply an expression of general principles of responsibility.

- **The role of the consent** of the individual must be neither overestimated (under current legislation, it is neither a necessary nor a sufficient condition for the lawfulness of data processing) nor disregarded, since it embodies the individual's freedom in terms of how their personal data are used.

These principles are **not a barrier to the development of Big Data.** Indeed, many uses of Big Data are not aimed at individuals as such but at the **statistical exploitation** of data concerning them. The principle of defined purposes does not, in fact, exclude the freedom to reuse data for statistical purposes: under the current legal framework, a statistical purpose is always presumed to be compatible with the initial purpose of processing. Conversely, where the use of Big Data targets individuals as such, for example to establish a profile to predict their characteristics (solvency, dangerousness, etc.), the fundamental principles of data protection must be applied in full.

Whilst such principles remain pertinent, **the mechanisms used for data protection must be adapted and updated.** Four complementary avenues should be explored:

the use of technologies to increase individuals' capacity to control the use of their data; defining a "chain of responsibilities", running from the designers of software and connected devices to end users, and supplementing the responsibility of the data controller; particular attention to the circulation of personal data; and the shift from a formal declaration-based approach to one based on continued compliance with the regulations, guaranteed by internal and external controls.

The changes underway in European Union law are rightly focused on reaffirming these principles and updating mechanisms. In the first place, the ***Google Spain vs AEPD*** **decision** of the European Court of Justice of 13 May 2014 **assigns responsibility to search engines for the processing of the personal data** they collect when they receive requests concerning an individual. It implies the existence of a **right of removal**, based on the individual's right to oppose the processing of their personal data and the right to the removal of data that has not been processed in accordance with directive no. 95/46/EC. Basing itself on the principles of the 1995 directive, the ECJ has therefore created a new mechanism appropriate to the issue of "e-reputation" in today's digital society, which will nevertheless need to be implemented in a way that can be reconciled in a balanced way with freedom of expression (cf. proposal no. 5 below).

Secondly, on 25 January 2012, the Commission adopted a **proposed regulation** relating to personal data, designed as a substitute for directive no. 95/46/EC. The adoption of this regulation by the European Parliament and the Council would help to establish a single body of rules within the whole of the European Union and thus **place protection on a continental footing** that is more appropriate to the transnational nature of the internet. The regulation updates a number of mechanisms, in particular by removing the obligation on declaring processing, which was too formalistic, making it compulsory for data controllers to designate "data protection representatives", introducing the concept of "privacy by design" and establishing administrative sanctions to act as deterrents. Although such changes are welcome, other innovations could be encouraged, in particular technologies to improve privacy or the development of certification and co-regulation.

➔ *Surveillance of communications by the public authorities raises specific issues and calls for appropriate responses*

The principles governing the surveillance of communications by the public authorities were established in the act of 10 July 1991. This reaffirmed the confidentiality of communications and only authorised its infringement in two hypotheses, either on the decision of a judicial authority or "in exceptional circumstances" and for purposes defined in law, on a decision of the French Prime Minister and subject to the control of the National Commission on Control of Security Interceptions (CNCIS). Since then, however, the communications surveillance practices of the public authorities and the context in which they take place have undergone profound changes, raising significant debates around their role and the safeguards that need to be established. The upsurge in electronic communications and data storage and analysis capacities has increased the

possibilities of interception. The two most recent defence white papers have made collecting information through this route one of the priorities of France's national security policy, which has resulted in a significant increase in the services' tangible resources. More recently, the ECJ's *Digital Rights Ireland* decision of 8 April 2014 challenged the European framework on data retention and the revelations contained in what has become known as "the Prism affair" have brought these issues to the fore of public debate throughout the world. Although since the act of 10 July 1991, the legislature has proceeded on the basis of successive extensions of the scope of information gathering, there now appears to be a need to embark on a broader re-examination of the legal framework of communications surveillance, with the aim of **maintaining France's capacity to protect its national security whilst implementing all the safeguards necessary to protect fundamental rights.**

In the *Digital Rights Ireland* decision, the ECJ declared directive no. 2006/24/EC of 15 March 2006 invalid; the directive provided that states were obliged to require communications operators to retain all metadata concerning their users for a period of between six months and two years, in order to guarantee that such data would be available for the purposes of research, detection and prosecuting serious crimes. It held that a general obligation to retain such data constituted a particularly serious interference in respect of the rights to privacy and protection of personal data guaranteed by articles 7 and 8 of the Charter of Fundamental Rights of the European Union; whilst it accepted that such interference was justified by public-interest objectives such as combating terrorism and organised crime, it held that this was disproportionate since the directive covered data on everyone, provided no safeguards concerning access to the data retained and defined the retention period without considering the usefulness of retaining such data in relation to the objectives the directive was aiming to achieve.

The ECJ's decision raises the question of the compliance of national legislation with European law; French legislation, for example, provides for a similar obligation on the general retention of data.

In light of the issues involved in communications surveillance for the protection of national security, the Conseil d'Etat study does not propose to remove this obligation but recommends strengthening safeguards around access to and use of such data.

II.2. Promoting freedoms in the era of "platforms"

Digital technology clearly has a positive impact on exercising freedom of expression, freedom to do business and freedom of association. It also, however, facilitates unlawful behaviours such as abuses of freedom of expression and counterfeiting. Furthermore, situations of inequality of power and allocation of scarce resources may, as in other areas of economic and social life, justify the intervention of the public authorities in promoting as much freedom as possible for everyone.

➔ *Network neutrality, fair platforms and combating unlawful content*

The Conseil d'Etat study proposes to **enshrine in positive law** the principle of **net neutrality**, since it constitutes a fundamental guarantee of the safeguards set out above by enabling any business, any association and any individual to benefit from equal access to all internet users. The current threats to compliance with this principle are also more substantial than in the early days of the internet, because of the dominant position of certain content providers and the share of traffic represented by certain leading video-sharing sites. It is important, however, with regard to the European Union's proposed regulation (the "fourth telecoms package") to allow a sufficiently broad definition of "specialist services", under which operators can offer a guaranteed level of quality that is higher than that found on the internet in general. Indeed, specialist services of this kind need to be developed in order to offer innovative uses such as remote medicine. In return for a broad definition of this kind, the electronic communications regulatory authorities should have sufficient prerogatives to prevent specialist services from harming the quality of the general internet.

Electronic communications operators are not the only actors to play a decisive role in the exercise of freedoms on the internet: the situation of the "**platforms**" also needs to be addressed. This expression usually refers to sites that allow third parties to offer content, services or goods, or which provide access to such content, such as app stores, content-sharing sites, marketplaces, search engines, etc. Their role as intermediaries gives platforms both economic power and influence, which have a significant impact on how third parties exercise their freedoms and raises unprecedented questions for the public authorities.

The Conseil d'Etat study first makes the point that the fundamental division provided for in article 6 of the LCEN, which transposes the "e-commerce" directive of 2000 into French law, between technical intermediaries, whose liability is limited, and website publishers, is no longer appropriate in light of the increasing role of platforms. Indeed, numerous platforms are not content with passively storing the products and services of third-party companies or content published online, but organise them through indexing and, where appropriate, making personalised recommendations to internet users. Several decisions by the ECJ and the French Cour de Cassation have shown that a marketplace or search engine no longer fulfilled the condition of playing a purely technical and passive role, as provided for in the 2000 directive, to benefit from the status of hosting provider and the limited liability associated with it. Limited liability, however, plays a key role in exercising freedoms on the internet, by avoiding the need for platforms to carry out preventive censorship of content published online in order not to be held liable for it. It therefore seems necessary to create **a new legal category for platforms**, which would no longer be defined based on the technical and passive nature of their role but on the fact that **they offer classification or listing services for content, goods or services placed online by third parties.**

Platforms cannot be subjected to the same obligation of neutrality as electronic communications operators, because their role is to provide organised, ranked or

personalised access to the content published on their site or to which they provide access: a search engine cannot be asked to ensure equal treatment, since the very purpose of a search engine is to rank websites in order of priority. However, **platforms should be subject to an obligation to treat their users fairly**, both non-professional users **in the context of consumer law** and professional users in the context of **competition law.**

Because they act as a gateway for disseminating or accessing content on the internet, platforms are necessarily involved in the debate over combating unlawful content. Aside from their legal obligations when they are made aware of such content, they also implement **voluntary approaches in the context of "policies" on the content** they accept or tools for detecting counterfeits, which they make available to beneficiaries. This role is controversial, with some describing it as "private policing". The Conseil d'Etat considers that it would not be realistic to deny private-sector players the right to decide to withdraw an item of content and to leave this to the judges. However, it is important to provide stronger safeguards for the rights of people whose content is withdrawn and who are often unable to make their arguments known. Furthermore, the considerable *de facto* power associated with defining "policies" in relation to content should be exercised in more transparent conditions and on the basis of greater consultation with stakeholders.

➔ *The need to ensure audiovisual regulations have mechanisms appropriate to the digital environment*

Two of the theoretical foundations of audiovisual regulation, namely occupation of the public domain and the need to regulate "linear" programmes, cannot be transposed to audiovisual services accessible via the internet. The first is drawn from the general rules on the public domain, which allow the public authorities to impose public-interest obligations on those who occupy it and cannot apply to audiovisual services disseminated via the internet, which do not rely on restricted use of the public airwaves. The second fundamental point is what is generally known as the "linear" character of traditional audiovisual services. On the internet, users can switch as they wish from one site to another and therefore have greater freedom of choice.

However, a third theoretical foundation is also relevant, both for the internet and for traditional audiovisual communications methods: namely objectives that have a constitutional value, such as safeguarding public order, respect for other people's freedom and preserving the pluralist nature of trends in sociocultural expression, as well as the public interest associated with promoting cultural diversity.

The study proposes that communications operators should not be forced to differentiate between legal forms of content within the general internet, in order not to undermine net neutrality. Such obligations could, however, be envisaged in the context of distributing specialist services.

➔ *Gauging the role played by algorithms and designing ways of managing their use*

Algorithms lie at the heart of the intermediation role played by platforms. Platforms are not alone in using algorithms, however, and the development of "Big Data" means they are being applied in numerous areas. There is no doubt that algorithms are useful in optimising the operation of a number of services. However, they present three potential risks to the exercise of freedoms: locking the internet user into a "personalisation" framework that they cannot control; over-reliance on the results of algorithms, which are perceived as objective and infallible; and new problems of fairness resulting from the increasingly detailed use of personal data.

Managing the use of algorithms is a new area for the public authorities, but has become a necessity because of the increasing role played by these mechanisms and the risks they present to the exercise of freedoms. The Conseil d'Etat study advocates three ways of managing them: ensuring the effectiveness of human intervention in decisions made using algorithms; establishing procedural and transparency guarantees when algorithms are used to make decisions about an individual; and increasing the monitoring of results produced by algorithms, in particular for detecting the existence of unlawful discrimination.

II.3. Applying a basic set of compulsory rules for all digital technology actors, regardless of where they are based

The question of territorial jurisdiction on the internet is an issue in terms of simplifying and ensuring the accessibility of the law, but also a strategic one, insofar as it challenges both states' ability to protect their citizens' fundamental rights and their citizens' right to appeal. The implications for competition between digital businesses are significant.

➔ *Defining a basic set of compulsory rules applicable to all technology actors, regardless of where they are based*

As most major firms on the internet are based in the United States, the vast majority of **individuals and European businesses find themselves dealing with the jurisdictions and legislation of various US states**, as provided for in the general conditions of use of such services. It would be premature to deduce from this, however, that it is in the interest of European states to call for the systematic application of their own legal rules to internet users, regardless of the website's country of origin. Indeed, it is difficult to envisage the principle of the internet user's country becoming a general and absolute rule for determining the law applicable to the internet, since a site cannot reasonably be required to comply with all the legal rules of every country in the world, not least because these contradict each other on numerous points, and because complying with them could mean it was infringing the rules of its own state. Such a position would also imply that French or European actors are always destined to use the internet as consumers rather than as service producers.

The Conseil d'Etat therefore advocates **promoting the principle of the destination country not for all legal rules applicable to internet participants, but for a basic set of rules** selected for their specific importance in relation to protecting fundamental rights or public order. These basic rules would apply to all sites aiming their activities at France or the European Union (depending on whether the rule applies at a national or European level), with the concept of an activity aimed at a particular country being defined in accordance with case law.

Depending on the subject matter, the destination country-principle could operate in three ways:

- the application of the ordinary rules of private international law, which would, amongst other things, achieve the desired result in criminal matters;

- the **classification of "police law"** as defined in private international law, which would need to be used **in respect of protecting personal data** and **obligations on private-sector players to cooperate** with the judicial and administrative authorities acting **on grounds of national security**;

- coordinating national legislation through a European treaty or secondary legislation, which could be used to establish the destination country-principle in the audiovisual sector.

➔ *Ensuring effective cooperation with respect to implementation, both within the European Union and with other legal systems*

Responsibility for defining the scope of their legal rules falls to individual states or the European Union. The application of legal rules by actors from other states, however, implies positive cooperation with such actors. The study examines three types of relationship: the relationship between European Union member states, in light of the entry into force of the proposed regulation on protecting personal data; the relationship between the European Union and the United States; and the relationship with other legal systems.

Within the European Union, it is important to appoint a **"lead authority"** for data controllers based in several member states to ensure that regulation is effective. This must, however, **be accompanied by effective coordination mechanisms between authorities** in order to prevent "forum shopping" risks and to safeguard individuals' right to appeal.

As far as the relationship with the **United States** is concerned, the **"Safe Harbour"** mechanism **should be fundamentally reformed**. Its renegotiation with the US government should look at two questions: the switch from an approach based on declaring commitments and self-certification to one of binding regulations on member businesses, combined with more intensive monitoring by the authorities; and a change to the content of the obligations included in the Safe Harbour, given that the current obligations are often vague and far removed from the level of protection offered in Europe.

As regards the relationship **with other legal systems**, the **convergence of values** with certain states, such as Brazil and South Korea, **opens the door to a more ambitious policy** of mutual recognition and joint regulatory activities. Cooperation with regard to combating cyber-crime should be intensified, for example by setting up an inter-state action group that would produce detailed recommendations on the cooperation practices to be implemented and which would publish lists of non-compliant states.

III. – Ensuring digital technology supports both individual rights and the public interest

Essentially, the rights currently accorded to individuals are limited to enabling them to refuse to have their data processed (an option that is almost never exercised), without giving them any real power over the content of the service or how data are processed. Ensuring digital technology supports individual rights should be the main guiding principle for protecting fundamental rights in the digital arena. By adopting an empowerment-based approach of this kind, aimed at increasing individuals' autonomy, public intervention can increase individuals' capacity to take action to protect their rights and thus expand the opportunities for action available to the public authorities themselves. Faced with digital technology stakeholders whose success is reliant on a privileged relationship with their users, public authorities must also understand how to "join the crowd".

The second guiding principle of the proposals set out in section III is about ensuring digital technology supports the public interest. Digital technology can offer significant benefits to the effectiveness of policies to improve health, education, culture and security or to combat fraud, and to simplifying administrative processes; again, public bodies need to have access to appropriate legal frameworks and instruments to seize such opportunities, whilst ensuring protection for individual rights.

Although there is still room for domestic law to act autonomously, either through legislation or regulations, or through soft law, many of the proposals in this study fall within the jurisdiction of European Union institutions, either because they require a changed to existing EU law, or because the European Union represents the pertinent level of action.

III.1. Defining the principles underpinning fundamental rights in the digital era

It is sometimes recommended that individuals should be granted a real right of ownership of their data, on the basis that they would be more involved should they have a financial interest in the proper management of their information. The Conseil d'Etat does not support this recommendation. Whilst it does advocate strengthening the role of the individual as an active player in data protection law, it envisages this more as a **right to self-determination** than a right of ownership (**proposal no. 1**). In practice, acknowledging a right of ownership would not help to rebalance the relationship between individuals and economic actors and would complicate the exercise of regulatory powers by the public authorities. The right to "informational self-determination", a concept developed by the German Constitutional Court in 1983, is – unlike a right of ownership – a right attached to the individual, namely "guaranteeing in principle the individual's capacity to decide on how their personal data may be communicated and used". This right should not be defined as being supplementary to other rights (the right to information, right of

access, etc.) but as a principle that underpins those other rights; these in turn support the principle and should be interpreted and implemented in light of this objective.

The principle of **neutrality of electronic communications operators** needs to be enshrined in positive law, by providing for a broad definition of specialist services combined with significant powers being granted to the regulatory authorities to ensure that the general quality of the internet is maintained (**proposal no. 2**). Platforms would constitute a new legal category and should be subject to an obligation of fairness, which would consist of providing a listing or indexing service in good faith, without seeking to alter or distort it for purposes contrary to the interests of users (**proposal no. 3**).

III.2. Increasing the powers of individuals and groups of individuals

Individuals should have greater capacity to act at two levels, an individual level and a collective level.

At an individual level, the Conseil d'Etat study advocates:

- giving the **CNIL** in France and all European data-protection authorities an explicit role in **promoting technologies** that increase **individuals' control** over the use of their data (**proposal no. 4**);

- effective implementation of the **right of removal** recognised by the ECJ in its *Google Spain* decision, in particular by giving the publishers of sites who request delisting the opportunity to make their case and by explaining how the decision is implemented through guidelines issued by the data protection authorities (**proposal no. 5**);

- **defining platforms' obligations to their users** based on the principle of fairness: in particular, the relevance of the listing and indexing criteria implemented by the platform in light of the objective of offering better customer service to the user, and defining the criteria for removing lawful content in clear, non-discriminatory terms that are accessible to everyone (**proposal no. 6**);

- organising a **right to be informed** in relation to the protection of personal data, based on the "general" right to be informed recognised by the act of 6 December 2013 for any crime or offence (**proposal no. 7**).

The proposals in respect of collective actions are as follows:

- creation of a **collective action** with regard to protecting personal data, enabling certain accredited legal entities to secure an injunction from a judge to address breaches of the legislation (**proposal no. 8**);

- making all data processing **declarations and authorisations "open data"** by the CNIL (**proposal no. 9**);

- greater **participation by platform users** in **developing rules** defining the content that can be published on their site (**proposal no. 10**);

- making the CNIL or the Conseil national du numérique (National Council for Digital Technology) responsible for facilitating an ongoing dialogue on the **ethical issues** associated with digital technology (**proposal no. 11**).

III.3. Redefining mechanisms to protect fundamental rights and rethinking the role of the public authorities

➔ *Protection of personal data*

The legal framework for the protection of personal data was defined when the circulation of data and their economic value were limited. Public intervention now needs to ensure, on the one hand, that the use of data is legally secure, since it is a factor in the development of the digital economy, and on the other, closer supervision of the types of processing that present the most significant risks.

The following actions are advocated to ensure that uses that present limited risks for fundamental rights are legally secure:

- maintain unambiguous **freedom to reuse personal data for statistical purposes** in the regulations, regardless of the initial aim of processing, on the sole condition that such reuse should offer appropriate guarantees in terms of anonymity (**proposal no. 12**);

- ensure that the CNIL strengthens the **advice and support role of data controllers** and creates a "personal data ruling" (**proposals no. 13 and 14**);

- develop a system of joint regulation with professional stakeholders, by providing for a procedure to accredit codes of conduct; compliance with a code of conduct would then become one of the criteria used by the regulatory authority when deciding to issue authorisations or impose sanctions (**proposals no. 16, 17 and 18**).

The following recommendations are designed to ensure that supervision is proportional to the degree of risk of processing:

- create a periodic **certification obligation** for processing categories that present **the most significant risks** (supplementing the *a priori* examination by the regulatory authority as part of the prior consultation procedure) by an independent third-party organisation accredited by the regulatory authority (**proposal no. 19**);

- pay particular attention to **personal data being sent from one entity to another**, in particular by **codifying in law court decisions** on the nullity of transactions related to files that have not been declared to or authorised by the CNIL (**proposal no. 20**).

The legal system for identification numbers should be reviewed, expanding the options for use of the NIR (national health number) in the health sector (**proposal**

no. 22) and examining the creation of a national number that is not used for other purposes (**proposal no. 21**).

Finally, protecting fundamental rights means introducing tools to regulate the use of algorithms, in particular through the requirement for effective **human intervention** in data processing (**proposal no. 23**) or by observing their results, in particular to identify unlawful discrimination, and strengthening the human resources available to the CNIL for this purpose (**proposal no. 25**).

➔ *Freedom of expression*

It would be useful to place an obligation on hosting companies and platforms to prevent the reappearance, for a defined period, of content that had previously been withdrawn; this obligation would be pronounced by the administrative authority (**proposal no. 28**).

The existence of specific methods of controlling concentration, in addition to the general control exercised by the competition authorities, is an important guarantee of media pluralism. Given the overabundance of content, however, the main threats to recipients' free choice are no longer excessive concentration but the increasing vulnerability of the business model of the press, although it remains an essential source of high-quality information. It would be useful to begin thinking about a **reform of managing concentration** in the media generally and in particular quotas and measuring the audience pools used to limit it, in order to guarantee pluralism by taking into account the multiplicity of information sources (**proposal no. 30**).

➔ *Development of mediation*

Numerous disputes related to the use of digital technology, whether they involve personal data, negative impacts on reputation on the internet or withdrawing content that has been published online can be classified as "minor disputes": the issues are sometimes significant for the people concerned but the monetary interests involved are generally limited. Traditional court procedures are not particularly well suited to dealing with minor disputes, which means many people abandon attempts to exercise their rights; mediation would be more appropriate in many cases (**proposal no. 31**).

III.4. Ensuring protection for fundamental rights in the use of digital technology by public bodies

➔ *Openness of public data*

The so-called "open data" initiative has been part of a proactive government policy since 2011. Such political determination, expressed by demonstrating a principle of openness that today forms part of a mechanism based on soft law, contrasts with the weakness of the obligations provided for in hard law. Enshrining in law an obligation to gradually publish online all the databases held by the administrative authorities would present several advantages, in particular extending the "open data" policy to local authorities, whose actions in this area are currently inconsistent. The soft law route, however, seems more appropriate for promoting the development of **open data**, particularly with the local authorities. A **charter of commitments and good practices** could therefore be developed by the state, **local authority** associations and representatives of data users, which would commit each public-sector organisation involved to defining a programme of opening up its public data, complying with quality standards and working to limit the risks of re-identification (**proposal no. 32**). These risks would be limited by defining **good anonymisation practices** and by creating a centre of expertise on anonymisation in each ministry, *a priori* in the ministerial statistics department (**proposal no. 33**).

➔ *Police files*

Police files have expanded significantly over the last 15 years, largely as a result of the lengthening of the list of offences that have to be recorded. Without challenging how useful these may be for the police services, it seems advisable to strengthen the safeguards around their use and address certain legal vulnerabilities:

- For the Fichier automatisé des empreintes digitales (FAED – Automated Fingerprint File) and the Fichier national automatisé des empreintes génétiques (FNAEG – National Automated Genetic Profile File), it would be useful to explain the consequences of court decisions (acquittal, case dismissed, discharge and no further action) (**proposal no. 34**). For the "Processing of Criminal Records" file, it is a matter of ensuring effective implementation of the provisions that govern it (**proposal no. 35**), insofar as successive CNIL checks have shown a very high level of errors and failure to take account of judicial consequences.

- Decision no. 2010-25 QPC of 16 September 2010 of the Constitutional Council should be implemented, with a change to the period for which data are retained in the FNAEG depending on the seriousness of the offence and the age of the person when it was recorded (**proposal no. 36**).

➔ *Intelligence*

The **consequences** of the *Digital Rights Ireland* judgment need to be drawn with regard to **access to metadata collected in terms of the systematic retention obligation provided for in French legislation**, in particular by reserving access for police purposes to crimes and offences of sufficient seriousness, re-examining the systems that allow access by certain administrative authorities for purposes other than domestic security (in particular, the anti-piracy body HADOPI, the national agency for information system security ANSSI, the tax authorities and the financial markets authority, the AMF) and by regulating access to metadata using the specific rules applicable to parliamentarians, lawyers, judges and journalists on intercepting communications (**proposal no. 38**).

Commentaire [A1] : A valider (« sécurité antérieure » dans le français : doit-on comprendre « sécurité intérieure » ?).

In order to satisfy the requirement for the predictability of law derived from the case law of the ECHR, it would be useful to define in law the system for intercepting **communications abroad**, by defining the purpose of said interceptions, the specific safeguards available to French residents and the existence of regulation by the independent administrative authority (**proposal no. 39**). It would also be useful to define the legal system for the use by the intelligence services of certain special investigation methods, which are currently only governed by the rules of judicial procedure (namely decoding and capturing sound, images and computer data) (**proposal no. 40**).

The proposal is to make the CNCIS a regulatory authority for the intelligence services, equipped with increased human resources in both quantitative and qualitative terms, with high-level competences in terms of engineering electronic communications, computer equipment and data analysis. Its prerogatives must also be strengthened by giving it the power to inspect evidence on the spot and an expanded jurisdiction, covering interceptions abroad and the use of special investigation methods (**proposal no. 41**). Agents involved in implementing intelligence operations would have a **right to notify** the AAI (Independent Administrative Authority) of practices that are manifestly contrary to the legal framework, according to the secure methods designed to protect confidentiality around national defence (**proposal no. 42**).

III.5. Organising European and international cooperation

A **basic set of compulsory rules** applicable to all services aimed at the European Union or France (depending on whether the rule is European or national) regardless of their place of establishment, would include (**proposal no. 43**):

- European legislation on the protection of personal data, which for this purpose would be qualified as "**police law**" as defined in international private law;

- an obligation on hosting companies and platforms to cooperate with the administrative and judicial authorities, as provided for in article 6 of the LCEN, whose territorial scope would be made explicit;

- criminal law, in particular infringements of freedom of expression, which is already applicable to all sites, even those based abroad but aimed at a French audience.

In terms of protection of personal data, the Safe Harbour negotiated with the US authorities should be reformed, by providing a right of supervision of controls by the European authorities and strengthening basic obligations (**proposal no. 44**). In terms of combating cyber-crime, an inter-state action group should be created to define recommendations and publish a list of non-cooperative states (**proposal no. 47**).

The announcement of the end of the contractual relationship between ICANN and the US government opens up prospects for the reform of the governance of the internet, not only for ICANN but also for other bodies, which need to be given a public-interest mission guided by an international "mandate". The current reform process should provide an opportunity to reflect these requirements in concrete terms. The process of democratising ICANN should be promoted, in particular by creating a general assembly of all stakeholders, which can hold the board of directors to account. The role of states should be strengthened, by enabling the Governmental Advisory Committee (GAC) to adopt binding resolutions (**proposal no. 48**). The internet governance bodies of all organisations should be diversified by adopting selection criteria that impose real linguistic and geographical diversity and the implementation of influence strategies in France and within the European Union (**proposal no. 49**). An international convention of fundamental freedoms and internet governance principles should, amongst other things, set out the principles imposed on signatories (**proposal no. 50**).

***

When it embarked on this study, the Conseil d'Etat was aware of the expectations on it in respect of defending rights and fundamental freedoms. It also knew that it must not restrict itself only – notwithstanding the legitimacy of such a position – to protecting the rights of individuals. Its aim was to take into account the full potential of digital technology, in particular those aspects that make it a vector for an economy that supports growth and employment.

The Conseil d'Etat would have failed in its duties, its annual study and its objectives, if it had not treated concomitantly both aspects of a single reality, namely digital innovation and the protection of citizens' fundamental rights and freedoms.