DIGITAL DATA:

A MATTER OF EDUCATION AND CITIZENSHIP

Opinion of the Economic, Social and Environmental Council

presented by

rapporteur Éric Peres

on behalf of the

Section for Education, Culture and Communication

Mandate 2010-2015 – adopted on 13 January 2015

Introduction

Edward Snowden's revelations concerning the NSA's practices opened the public's eyes worldwide to how Internet-based systems that provide them with new services can also bring them vulnerabilities. Today, 86% of French mobile telephone users want to be able to prevent transmission of their geolocation data to commercial enterprises.

At the same time, digital data concerns are more than ever at the heart of economic issues and their underlying models. Some of these cases revolve around exploitation of user data for advertising purposes or analysis of this data to develop new value-added services in the health, energy, transport, tourism and cultural sectors. The global economy for digital products and services already represents over one-sixth of that for traditional goods and products (estimated respectively at €15 and 100 trillion). The digital transition gives rise to democratic challenges in a society where the relationship between surveillance and the rule of law is being re-examined in light of the means used to ensure control and supervision of these data streams.

Observations and issues

Big Data: uses and issues

Origin and definition

Although the term "Big Data", meaning "exploitation of extremely large volumes of data", only appeared in 2010, the concept dates back more than a dozen years, when data became too vulnerable to be stored and manipulated using conventional techniques. The central issues involving Big Data systematically concern the data and how it is processed. The Big Data phenomenon should

not be viewed solely in the context of new data harvested from blogs and social networks. A significant portion of Big Data concerns data from the banking and media sectors, as well as public networks such as energy or transport. The origins of Big Data are found in this explosion of voluminous information. In fact, the Big Data phenomenon is not limited to "new data" (in particular, from blogs and social networks). A large part of the observed exponential growth concerns data traditionally processed by businesses, whether from the banking and media sectors, or public networks such as energy or transport.

Recent developments in information technology have impacted datafication by simplifying, accelerating and expanding the scale of **data** collection and processing. Data is, by definition, coded information, fixed and transferable, that necessitates encoding to allow both its collection and consolidation with other data represented in the same repository. However, a significant part of it is not perceived as data by users. For example, an individual's Internet browsing history constitutes valuable economic data, yet users often do not perceive it as such. Note that **personal data** is composed of declarative information about an individual, but also a set of undeclared information that is collected automatically, in particular when browsing websites. For example, when a user registers on a site to access a product or service, he provides his email address, along with his full name and, sometimes, additional information. The user's personal data therefore includes all his contact information, traces left on websites, search engines and social networks, as well as in the physical world (e.g. museums, hotels).

The **storage issue** for digital data and, indirectly, the issue of digital data protection, directly concern three types of stakeholders: citizens, businesses and the State. Citizens are faced with the issue of their personal data being stored in foreign countries where their national jurisdiction does not necessarily apply, and under potentially insecure conditions. This issue also applies to businesses, along with a dilemma: whether to outsource data storage or manage it internally, with the risks inherent to this activity. Finally, the State is faced with all these issues, in addition to those of energy consumption and sustainable development: data storage infrastructures require, among other things, electrical distribution systems.

Digital data is stored on physical hardware at ***data centres*** (DC). In 2011, 2,087 existed worldwide. Investment in data centres – located mainly in the Asia-Pacific region – increased in 2012 by 22% worldwide compared to 2011. Data centres cover from a few hundred to tens of thousands of square metres. They include servers for data processing, hardware for storage and internal and external networks, cooling systems and equipment to supply electricity. Today, it is estimated that a 10,000 m^2 data centre could have an electrical consumption equivalent to that of a city with 50,000 residents. According to McKinsey & Company, the management consultancy firm, less than 10% of most servers' energy consumption is used to process data; the rest is consumed in idle mode or dissipated as heat!

Metadata is structured information that describes, explains, localises or facilitates the searching, use or management of information resources (e.g. video files, music files). In other words, metadata organises and accompanies the entire digital life cycle of important information, including procedures, processes and users to whom tasks are assigned. They thus provide precise traceability within the framework of the protection and organisation of data. They can also generate, in turn,

data on the tastes and preferences of users that becomes the basis of online recommendation systems.

Big Data is, above all, the point of convergence between the proliferation of unstructured data, demands for analysing it and technological progress. It is often defined in terms of the "3 V's" (volume, variety and velocity), to which Christophe Brasseur has added a fourth: value (or valuation). However, this need for volume has a downside. It can encourage data collection agents to seek to acquire a large amount of information, including personal data. The same applies to the variety of data collected, since Big Data is based on establishing relationships between data of different types, furnished, in particular, by browsing histories. Veracity has become a major, strategic feature for Big Data, since erroneous information can have adverse consequences from all points of view.

Leveraging digital data in the social, economic and environmental domains

More than the characteristics of Big Data, it is the possibilities for analysis of the information behind digital data that are already a growing part of the data economy's strategic importance. The initial information provided by a site's customers and users is associated with the information needed to establish a customer base, which is a primary source of value for a company. For example, in 1997, Amazon employed around forty people to make personal recommendation to its customers for online book sales. From an advertising perspective, this theoretically allowed high-precision targeting of individuals. Moreover, this "datafication" of users appears to fulfil a long-time marketing dream: the ability to tailor supply to demand, by precisely characterising the targeted customers. This development benefits both large companies, which can optimise their investment, and VSEs and SMEs, which can benefit from tools or resources that were previously inaccessible to them. In this perspective, Big Data is a new step towards the automation and robotisation of the world. All sectors of activity, whether public or private, can be "datafied" and thus reap the benefits of Big Data. These benefits can take the form of incremental innovations, which give rise to better tools, or radical innovations, also called "disruptive innovations," that restructure the sector concerned. And these innovations can come from actors involved in these sectors, such as the State or existing companies, or from intermediary companies that specialise in either the collection or the processing of data.

The greatest opportunities of Big Data have probably not yet been discovered. In a sense, Big Data is a powerful way to reveal reality: the activity, whether public or private, is no longer based on agents' experience, insights or rational beliefs, but on statistical facts. There are numerous prospects for innovative reuse of public health data. The analysis of Big Data concerning health offers several major benefits: improving patient care (shifting from a curative to a preventive approach), ensuring the efficiency of public spending (in view of the doubling of today's senior population by 2030) and opening new areas for analysis and experiments to the scientific research community (e.g. epidemiology, chronic diseases, pharmacovigilance).

Thanks to digital technology, medicine is progressing by leaps and bounds. Biomedical techniques allow a longer, healthier lifetime, and healthcare takes comfort, well-being and longevity into consideration, particularly through sporting activities. In particular via digital techniques and medical imaging, new tools have appeared that allow a deeper understanding of our health and enhanced case analysis and surgical operations. Today we can use computers to model organs, study complex biological systems, detect diseases and even optimise surgical procedures with augmented reality

and specialised robots. Thus, a recent study by Microsoft Research concerning the fight against nosocomial infections, based on data from 25,000 hospital beds, showed how cartography could be used to manage patients' relative locations and limit risks.

The digital transition and sustainable development

No sector can escape Big Data, not even agriculture, also swept along by this digital wave. Far from productivity-based approaches, the collection and processing of data from sensors, automatic sprayers, drones and satellites has transformed the work of farmers. Digital tools help farmers improve irrigation, limit waste, apply the right amount of fertilizer and ensure ecological management of an area's freshwater resources.

Another example is the smart city. Equipping a city like Santander, Spain, with tens of thousands of sensors allows information on people's behaviour to be collected from different sources (e.g. available parking, noise, temperature). The data is transmitted to the city's public and private operators in the form of Open Data in order to optimise services. Analysing the data provides a better understanding of the city's social structure and encourages public and private initiatives.

Citizenship in the digital age, a new empowerment to act

Digital literacy and access to knowledge

While digital technologies multiply access to information (with a non-negligible risk of rendering it uniform) and open up certain domains previously reserved for an elite, providing worldwide information access (e.g. museum collections, photos, the press, books, films) in real time, instant access to data should not be confused with knowledge. That is because, in addition to the imperative to understand this information that is now available to us, we must keep in mind that it is presented in a biased fashion, as a consequence of its access via search engines.

Education in the digital world: from the flipped classroom to massive open online courses (MOOCs)

What is digital education? Does it mean informing people or building their skills regarding the uses made of the data we produce? It should certainly go much farther, because nothing is the same in the digital age. Even mathematical theory has been upset. The mathematician Giuseppe Longo, a specialist on the work of Alan Turing, has shown how the digital medium even transforms the conditions of mathematical knowledge. In astrophysics, Big Data produced by space-based observatories has completely changed the conditions for the production of a planetology. Similar impacts have been seen in biotechnology and language science. In the digital age, Google's digital approach can transform the languages and acquisition modes in all scientific domains. Our understanding of this remains weak, mainly because it is so rapid. Massive open online courses (MOOCs) are transforming teaching methods, targeting groups of students much larger than a traditional classroom and allowing them to interact with each other and the teacher on the subject being covered.

Schools in the digital world: a brief overview

According to official guidelines, students are expected to develop the following behaviour and knowledge:

– In nursery school, children discover computers and understand their use and operation.
– In primary school, children learn to type on a keyboard and to use a dictionary. They begin to acquire the computer skills for a "*brevet informatique et Internet*" (B2i, Internet and computer user's certificate for secondary school pupils) using the basic functions of the computer. They become aware of the uses of the Internet and the associated risks. The emphasis is on sensible use of digital technology, multimedia and the Internet. The B2i covers five domains: setting up a working IT environment; adopting a responsible attitude; creating, producing, processing, and using data; researching and gathering information; and finally, communicating and interacting with others. Students study how to respect people's integrity and avoid harming others, including via the Internet.

When students are about 11 years old (at the end of primary school), they should be able to:
– use digital tools to research, gather information and present their work;
– use digital technology to communicate;
– demonstrate a critical approach to information and its processing.
During lower secondary education, mastery of digital tools should be implemented in all subjects. Critical analysis should be a key focus, including organising information and using digital tools. Students should be exposed to elementary algorithms, manipulation of images, colours, text and audio, understanding the principles and proper use of the Internet, messaging systems, etc.

Freedoms in the digital age: a tense relationship

Exponential growth in data collection versus the risks of hyper-surveillance

For the first time since the creation of the Internet, Edward Snowden's revelations have created the conditions for a schism between the Internet industry and the U.S. government. While they (rightly) raise questions about the risks of mass surveillance in a democratic society, the questioning of the confidentiality of corporate data was the most disturbing aspect for the entire range economic players. Thus, the giants of Silicon Valley have expressed to Barack Obama the extent to which the NSA's activities could call into question the cornerstone of the Internet: the trust of its users. Mark Zuckerberg, Facebook CEO, recently stated, "The U.S. government should be the champion for the Internet, not a threat..."

The notion of mass surveillance has become a reality in the eyes of public opinion worldwide. Beyond individual appropriation of the operation of services and technologies serving social, cultural or professional needs, it is also the collective appropriation of these technologies and thus the ability of our societies to create a digital architecture consistent with their principles and valuesthat will be decisive in allowing our societies to develop; yet it is precisely this capacity for collective appropriation that is called into question by the Snowden affair. The long-term social and political consequences of the Snowden affair are only beginning to be felt. Already, certain assumptions about the nature of communication over social networks are starting to be questioned. Thus, contrary to common perception, social media seem to be less suitable for the exchange of opinions, especially when these opinions apparently disagree with those people for whom a close relationship can be established, particularly in social or professional contexts.

Personal data and network interoperability

The digital revolution has been accompanied by a growing irreversibility of interactions and exchanges with increasingly-sophisticated technological systems. With the growing interoperability of these systems, the increasing interconnection of data files and the commingling of social and personal time with professional and leisure time, together with heightened activity on networks, leads us to question the very notion of privacy.

With the vigorous emergence of social networks, users are concerned about the use of their data, yet they are simultaneously disclosing more and more personal data, whether voluntarily or not. This could be called the "paradox of privacy." More precisely, it concerns people's desire to use these systems, along with their concomitant feeling of loss of control. As French people's use of digital technology increases, so does their concern about how it works and their desire to be reassured; this trend can only continue. The retention period for data and the right to be forgotten are central to their concerns. Why has this apparent inconsistency become, in a few years, a prominent part of the debate on privacy?

Protection and control of data: new issues, new approaches

Protecting personal data: a democratic imperative

The establishment of individuals' privacy rights gave rise to the development of numerous means designed to protect the personal data collected by professionals. An example is France's *Commission Nationale de l'Informatique et des Libertés* (CNIL, French Data Protection Authority), an independent administrative authority created by the legislature for the reasons mentioned earlier. The CNIL is now the primary authority for the protection of digitally processed personal data and aims to enumerate all instances of "files gathering personal data and to authorise the creation of files containing so-called 'risky' data". Any computerised "customer file" that a professional creates constitutes, under the law, "a personal data filing system", "a structured and stable set of personal data that are accessible according to specific criteria", and therefore must respect the CNIL's guidelines. Article 34 of that law thus provides that "The data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorised third parties". Three fundamental legal principles form the backbone of the CNIL's legal reasoning and specify a set of legal requirements that the controller must respect on pain of criminal sanctions: the principles of finality, fairness and proportionality.

The protection of personal data: between regulation and self-regulation

A number of actions could be carried out to favour the protection and control of digital data, on the assumption that innovation is enhanced when the ethical principles of transparency and trust are respected. Pitting them against each other, as some have done, is nonsensical, or perhaps the expression of dangerous cynicism. In other words, privacy and innovation are not antagonistic. Open innovation is not only technological in nature, but also an opening to society's expectations and aspirations. The principle of responsible innovation must include this ethical dimension as a driving force for new applications and new tools.

Recommendations

Promoting digital literacy

Supporting the family's educational role in the digital transition

It is essential to make children aware about the digital world from an early age. Teaching our children not only to orient themselves and find their way in these new environments, but also to benefit from them safely, is imperative for both leisure and education. The family is a privileged place of learning where children adopt and retain practices observed in their parents. However, today's parents belong to the first generation truly affected by the major changes in communication and information technologies. Families do not all have equal opportunities in the digital domain. Some of them have minimal background, both in the educational domain and in fields as varied as new forms of communication and correspondence. Additionally, these new methods to introduce people to the digital world are expensive and can be thwarted by unemployment and job insecurity, thus reinforcing the digital divide. Moreover, this process of increasing people's awareness and helping them discover the perpetually-changing digital universe must be lifelong.

The ESEC (Economic, Social and Environmental Council) recommends the development of public awareness campaigns regarding the protection of personal data with the participation of the CNIL and all concerned associations, in particular, associations for parents of students, families and extracurricular activities. Furthermore, the ESEC recommends making digital literacy the "major national cause" in 2016 and in this regard supporting the EducNum collective to implement awareness actions concerning potential, knowledge and digital skills and to label sites that meet the data protection criteria.

The ESEC considers that the family plays an essential role in digital education, and therefore supports the implementation of actions designed to develop parents' awareness that, in the interest of their children, and particularly the youngest, they should accord importance to the use of digital technology.

<u>Strengthening the protection of minors</u>

The near-permanent presence of mobile devices in the home environment presents new risks that children may access inappropriate content. In addition, so-called "sharing" features that are behind the success of social networks make it even more imperative for parents to monitor the content accessible via these devices. While it is now possible for parents to ask their Internet provider for a restricted connection, this limitation in fact constitutes false security. Attracted by lower cost and higher bandwidth, many mobile users, especially younger people, connect to the Internet via Wi-Fi.

The ESEC has called for a European strategy to protect minors on mobile devices. The French representatives to the European Commission must encourage the implementation at European level of a requirement for companies to integrate parental control features in the operating systems of mobile devices.

Supporting the deployment of digital literacy training from nursery school through higher education

To promote general training in "proper use", the ESEC advocates the development of training programmes in schools for students to learn (e.g. via serious games) about laws and regulatory texts related to the use of the Internet and social networks. In this regard, specific actions for the educational community should be implemented and pursued, within the framework of moral and civic education. Many regional education administrations (*académies*) have taken up this challenge (e.g. the Versailles *académie* and its "*Citoyen de l'Internet*" Internet Citizen programme).

The ESEC proposes that the introduction to computers at school should not be limited to simply using computers, and should rather be designed to introduce students to three fundamental concepts of computer science: language, information and algorithms. The ESEC does not intend for the teaching of programming skills to lead to the creation of a new subject in the classroom. Instead, the three fundamental concepts of computer science should be integrated into course material or transversally.

The digital world is both a source of content and a tool for teachers, supporting their educational missions. To make digital tools part of all teaching activity, the ESEC recommends ensuring better integration of digital technology in content and teaching methods for school curriculum. The ESEC considers that it is up to the *Conseil Supérieur des Programmes* (CSP, French Senior council for the national curriculum) to ensure, in accordance with its proposal for a common base, that digital literacy is treated in a transversal manner, so that it benefits all disciplines.

Promoting improved certification via the B2i

Created in 2001 and generalised in 2006, the B2i is a certificate issued to students in primary school (B2i level 1), lower secondary school (B2i level 2) and upper secondary school (B2i level 3), which verifies their ability to use computer-based tools and the Internet, as well as certain documentation and ethical skills. If the B2i is retained, the ESEC recommends perpetually adapting its content to enrich its facets associated with socio-economic and social issues. The "digital ethics" part of this certification could pay particular attention to personal data security issues in the era of Big Data.

Strengthening digital training within National Education and higher education

Currently, IT remains a discipline entrusted to specific teachers. While students planning a career in the digital sector must be offered specific training with specialised teachers, the curriculum common to all students must use a transversal approach.

The ESEC recommends that teacher training in *Écoles supérieures du professorat et de l'éducation* (ESPE, French Teacher training and education faculties) should allow classroom use of digital methods, e.g. flipped classrooms, cooperative practices and student peer support. It advocates stronger efforts in this regard within continuous training to massively train the current teaching staff. The ESEC endorses the integration of a digital literacy component in school plans (*projets d'établissement et d'école*) supported by educational engineering and a person assigned responsibility for it. This would make it possible to assess, within the institutions, the need for

personal training in digital practices and the implementation of a multi-year plan to develop training for teachers to gain mastery of both digital and educational techniques.

The ESEC recommends reinforcing the attractiveness of B2i for all degrees and diplomas issued by schools and universities. To ensure the adequacy of the IT infrastructures and the processing tools for Big Data, and to anticipate corporate needs regarding protection of personal data, the ESEC states that training for IT engineers and other scientists should precisely addresses all these issues. More specifically, the ESEC recommends the development of high-level training for data scientists and data brokers and encourages the CNIL to strengthen its partnerships with all educational institutions concerned.

Combating new digital divides

In addition to schoolchildren, digital literacy must also address the entire population, including those who are the most challenged in terms of access or social difficulties. Just as with "real" citizenship, virtual citizenship is palpably affected by inequality. We are all equal under the law, but multiple factors make us, in fact, unequal. For example, not everyone has an Internet connection. And even when people have Internet access, they have not all been properly instructed on the use of everyday tools. The issue of e-inclusion gave rise to a report from the *Conseil national du numérique* (CNN, French Digital Council) in November 2013 entitled "Citizens of a digital society – access, literacy, mediations, power to act: for a new policy of inclusion" (*"Citoyens d'une société numérique - accès, littératie, médiations, pouvoir d'agir: pour une nouvelle politique d'inclusion*"). The objective is to implement both long and short term projects, and target public actions situated at different points in the inclusion-exclusion spectrum, e.g. exclusion for physical, economic, social or geographical reasons. Building on the findings of various works by the CNN, the ESEC believes that the vision of e-inclusion must henceforth be inseparable from social inclusion, and be built on continuous and comprehensive public action.

Revitalising Digital Public Spaces (EPN, *Espaces publiques numériques*)

For the ESEC, public policy for training on "digital issues" must combat the lack of awareness of social mechanisms that result from new digital-related uses and the insufficient consideration of these issues in local policies. To accomplish this, those policies must favour the diversity of partners (e.g. scientific, cultural, technical, social, educational, sports) and beneficiaries of services (e.g. young people, parents, seniors) in a perspective of social transformation via digital techniques (critical thinking, new forms of commitment, knowledge production and cultural creations).

For people to become informed and responsible users of digital data and not simply consumers, and to prevent the use and processing of such data from being confined to enterprises and government administrations, access points must be deployed across the country. These would facilitate the manipulation, understanding and valuation of data for everyone while respecting rights and freedoms. The EPNs are an initial action in this regard. Reflecting the diversity of the organisations to which they are attached, as well as the cultural, social and professional missions to which they are dedicated, the EPN networks are a mosaic of over 7,000 locations throughout the country. The diversity of the EPN's missions is a positive point in the French digital mediation landscape. The ESEC advises reaffirming the role of the EPNs to become outreach and popular education sites for all, truly favouring awareness and providing mediation for the manipulation and creation of data.

What digital literacy training is appropriate for businesses and public administrations?

Without people's trust, the digital world's growth cannot yield all its potential benefits in terms of economic, social and environmental progress. Our citizens' need for trust, security and protection thus creates a new imperative for both businesses and public administrations, which must address these issues in order to use data harmoniously and equitably.

Promoting a policy of security and data protection within businesses and public administrations

Some businesses also suffer from poor data protection and deficient IT security. They risk damaging their reputation and their interests in the fields of innovation and research. As such, the ESEC recommends developing training and hiring experts in computer security and data protection. For public administrations, the ESEC recommends a substantial effort to train public employees in the use and processing of personal data and the need for to anonymise certain data, in particular when Open Data is deployed.

The vast majority of businesses and public institutions have entered the digital age in a haphazard fashion, yielding a situation where digital resources are used and processed intensively, including resources provided via data collection or processing, and resources feeding Big Data. This is coupled with an illusory belief regarding their mastery of the constraints and issues associated with these technologies. A large number of these players do not recognise their weaknesses that reflect their lack of digital maturity. The ESEC, with a view towards promoting good practices, considers it essential that the government make free and simple self-assessment tools generally available to measure compliance with good practices regarding personal data, mobility, the cloud and Big Data.

Promoting digital ethics in businesses and public administrations

Trust in digital technology, particularly when used for human resources management, must be reinforced within digital-sector businesses and public administrations in order to promote their digital ethics. Respect for individuals' privacy must therefore be part of their business model. This is essential in order to build a business model founded on the trust of end customers. To distribute these new technologies, this trust model requires an assessment of potential risks, information directed towards the authorities and customers and an appropriate response to address the risks. Respect for employees' privacy must therefore also be an integral part of ethical, responsible management. To promote the development of virtuous digital literacy within businesses, the ESEC recommends that the CNIL guidelines relating to the workplace be updated and promoted. The ESEC also recommends that Employee Representative Bodies (IRP, *Instance représentative du personnel*) benefit from training adapted to issues of managing protection of digital data within businesses, and that this commitment should extend to employees' personal data, so that they can benefit from full transparency.

Building digital public policy and industrial strategy

Developing a digital agenda for the State's data and technology

France's recent appointment of a Chief Data Officer (AGD, *Administrateur général des données*) should permit the implementation of a public policy on digital data protection as well as data security and anonymisation technologies. The ESEC advocates, as suggested by the French Senate's Common mission of information on access to administrative documents and public data (*Mission commune d'information sur l'accès aux documents administratifs et aux données publiques*) among others, including the schedule for publishing public data as Open Data in government authorities' contracts of objectives and defining continuous training on data to improve public employees' skills in this domain. Finally, the ESEC endorses the creation of a position of State Chief Technology Officer (*Administrateur général des technologies de l'État*) to coordinate the "French technology platform" and to enhance technological capital developed in France. This position must report directly to the Prime Minister.

Developing a digital public policy coordinated with an industrial policy that particularly favours start-ups.

Digital public and industrial policy should be based on the need to impel all businesses towards digital literacy, enabling them to grow via this new digital paradigm. However, it is also essential to allow start-ups to emerge in the digital domain, which demands a study of each sector concerned. Considering that all sectors (e.g. industry, agriculture, services, crafts, associations) are affected by the digital revolution and the issues surrounding data processing, the ESEC encourages the concrete implementation of these changes in the "*contrats de filière*" (industry-wide statements of objectives), with those devoted to digital administered by the *Conseil national de l'industrie* (National Industry Council), and associating trade unions and businesses. The ESEC advocates implementing an industrial policy targeting young digital companies in order to provide them with support and promote their development, thus favouring employment in the digital sector, as called for by the Grand Coalition for Digital Jobs, launched by the European Commission in March 2013 with abundant funding.

Echoing the opinion of the European Economic and Social Committee in "Digital society: access, education, training, employment, tools for equality," 9-10 July 2014, the ESEC supports the proposal to promote European SMEs in the digital sector and support start-ups with high-risk programmes (e.g. the health sector) within the framework of the Digital Agenda. The ESEC, like its European counterpart, calls for a "strengthening of financial support" and shares the disappointment of the European ESC "regarding the sharp cuts in the budget allocated to the Digital Agenda for 2014-2020, reduced from the initial proposal of 9.2 billion euros to 1.14 billion euros."

Controlling energy impact to improve data protection

It is currently difficult to obtain comprehensive data on the energy impact of data centres. According to the NGO Greenpeace, transparency is not the rule in this activity and, for reasons of security or competition, even the location of sites may not be disclosed. With the exception of a few leading operators, there is no willingness to assess the true externalities of this activity and to remedy them. Electrical power consumption constitutes their primary impact. Greenpeace notes in its report that the electricity consumed by data centres is produced mainly from coal: 50-80% for the largest digital companies (GAFA and others). There is a paradox between the desire to maximise dematerialisation to reduce resource consumption (in particular fossil fuels, thus benefiting the ecological transition) and the realities of data centre operation. Data centres are a significant reason for the growth in

emissions of Greenhouse Gases (GHGs). Another clear impact is related to the use of diesel-powered generators. This backup equipment must be tested regularly.

The European Commission has established a Code of Good Practice to respond to the increasing energy consumption of this activity and the need to reduce its environmental, economic and energy repercussions. The ESEC supports this Code of Good Practice and requests its accelerated dissemination at European level, not to mention to other partners worldwide. In view of the sector's extremely high growth, the ESEC considers it necessary for the Commission to set ambitious goals for adherence to this Code and ensure its promotion and monitoring, in particular by proposing effectiveness indicators for this type of infrastructure. Furthermore, the ESEC calls for greater transparency on the part of data centre operators regarding their actual energy needs so that local authorities can anticipate environmental and energy impacts on their regions and allow electricity supply to be aligned with demand without penalising other local economic activities.

Building a realistic and strict framework for data protection in the digital age

Edward Snowden's revelations and the PRISM affair have demonstrated the need for tighter rules designed to ensure the protection of citizens' privacy. Balancing national security and individual freedoms is a challenge for societies and for the rule of law. This obliges the urgent definition of a universal ethical framework to restore trust in the digital economy and its capacity to protect freedoms. This observation confirms the need to accelerate work on the revision of the European directive of 1995 and on the modernisation of Convention 108 of the Council of Europe, and to actively participate in defining the objectives of the United Nations, where "Guidelines for the regulation of computerised personal data files" were adopted unanimously by the General Assembly in 1990 and, alas, remain non-binding.

The ESEC advises French authorities to undertake a clearer, bolder involvement in the reforms of European and international texts. It recommends the implementation of veritable digital diplomacy.

Creating a framework for data protection at international level

This international regulation, while necessary, must not replace other forms of national regulation; it must supplement the fight against external risks and against discrimination in Internet access through an approach that integrates the European dimension, supports digital players and addresses civil society worldwide. We must believe that cooperation and balance of power, according to the rules of justice at European level, can allow us to draft a bill of rights for the digital age. The ESEC advocates, first and foremost, adherence to international legal instruments that already exist in this domain, such as Convention 108 of the Council of Europe, and the negotiation of an international convention for the protection of personal data.

A multilateral treaty must be initiated by France, Germany and Brazil, which share concerns on fundamental freedoms and their expression on the Internet. In the medium and long term, they must work for its adoption by all UN Member States to preserve the architecture of the Internet vis-à-vis potential attacks.

Enhancing and supporting the draft European Regulation on protection of personal data

The ESEC supports the European approach to the draft regulation on the protection of personal data as a fundamental right of every individual. This approach makes it possible to assert an undeniable right to access, modify and delete that data (the "right to be forgotten"). The ESEC recommends further harmonisation, within all European supervisory authorities, of the conditions for implementation of the right to be forgotten, following the judgement of the Court of Justice of the European Union concerning Google. In this regard, the principle of applying the law in force according to the complainant's place of residence and the possibility of appealing to a unique supervisory authority in each country of the European Union must also be added to the legal means for data protection. The ESEC advocates ensuring an identical level of protection in all EU countries, regardless of the place of establishment of the controller. Harmonisation should consider the best levels of protection in each EU country and make improvements thereto. The unifying themes for the amendment to the 1995 Directive must be better protection of freedoms and fundamental rights.

Securing international data transfers

The Binding Corporate Rules (BCR) set down an internal code of conduct that defines group policies regarding transfers of personal data outside the European Union. The BCR must be binding and respected by all entities of the group, regardless of the country in which they are located, and by all their employees. These BCR constitute an alternative to standard contractual clauses, since they make it possible to ensure an adequate level of protection for data transferred outside the European Union. In this sense, they also offer an alternative to the Safe Harbour principles for transfers to the United States. The businesses concerned are multinationals that export data from their entities located within the European Union to non-EU countries that do not ensure a level of protection equivalent to that of the EU.

The ESEC recommends promoting the BCR as the basic data transfer protocol at European level, in particular because they allow easier assessments. The deployment of the BCR must promote and harmonise the personal data protection practices in international agreements providing for this type of exchange.

Strengthening regulatory powers and promoting co-regulation

More than ever, civil society expects the CNIL to implement and enforce the fundamental principles of Article I of the French "*Informatique et Libertés*" data protection law, which states that "information technology should be at the service of every citizen. Its development shall take place in the context of international co-operation. It shall not violate human identity, human rights, privacy, or individual or public liberties". Faced with the global objective of providing rights and freedoms in the digital sphere, individuals have a particular role to play and it is essential to strengthen their rights.

The ESEC proposes to introduce into the law the possibility to delete minors' personal data, in particular online, via exercise of the right of opposition.

Given the global dimension of the data protection issue, the ESEC proposes allowing the CNIL to share this confidential information with its counterparts, carry out inspections and initiate coercive procedures within the framework of its cooperation with its non-EU counterparts, as is the case with its partners in EU Member States under Article 49 of the Law of 6 January 1978.

The ESEC also advocates increasing the maximum penalties the CNIL can apply: currently 150,000 euros, this sum might penalise small businesses but is insignificant for digital giants such as GAFA. To protect citizens, but also to protect virtuous businesses against unfair competition from economic actors with little respect for the legal framework, the ESEC recommends drawing upon the European draft regulation that provides for substantially increasing the sanction based on the company's turnover, limited by a ceiling, in order to guarantee the proportionality of the mechanism relative to the financial capacity of sanctioned entities.

Protecting personal data within Open Data

The State, local authorities or businesses make certain data in their possession available to the public via Open Data. However, this data could be personal data collected by the entity, requiring special attention. It is important to continue to raise awareness of this issue among all entities that adopt an Open Data policy, especially if the number of these entities continues to grow and their means decrease, particularly due to the modest size of some. Therefore, data anonymisation and the free and informed consent of users should be ensured.

Seeking ways and means to allow individuals to control their personal data

The ESEC encourages exploration and funding of procedures to give individuals control over the use of their personal data. Every individual must be able to obtain the same information that any company on the Internet possesses regarding him. Economic actors can contribute via veritable transparency and committed loyalty, particularly when drafting their terms of use and sales conditions in order to better control data.

The ESEC also recommends that web service providers make it possible to ensure that access to a user's data is blocked when the account is deleted and provide a function to delete all user data, guaranteeing users pure and simple deletion of all their data and files, with an option authorising users to export data to another service. This would lead to creation of a right to data portability, allowing users to leave services, download all their data (e.g. photos, posts, emails), store that data themselves, export it to other services or delete it entirely. The ESEC also advocates making "opt-in" the default for the collection and use of profile data, suggestions, messages, photos, videos and all developments concerning individuals' privacy.

Reviewing Terms and Conditions of Sale and the Terms and Conditions of Use

The ESEC advocates placing Terms and Conditions of Sale and of Use online, which would, in a clear fashion, allow users to give their consent to the use of their data for the purposes set out in those terms and conditions. The ESEC encourages, in this respect, the initiatives, in particular via competition, to develop a tool that can automatically identify changes to such Terms and Conditions and to compare versions, and also identify clauses that may be particularly dangerous or unfair. Finally, the ESEC advocates the use of royalty-free licensing to ensure that content produced by users, susceptible to be reused, can never be the object of an exclusive appropriation.

From data retrieval to data sharing, the role of the trusted third party

Ultimately, information sharing between businesses and individuals could be a positive evolution and promote better-informed consumption. By retaining the information that businesses hold concerning

him, every consumer could access data about his expenses, his diet or his carbon footprint. This could suggest different consumption patterns, more respectful of health and the environment. Collectively, consumers with similar needs could then influence the commercial proposals they receive. All this data could also allow the creation of new services, both private and collective, such as the management of data about the consumption of goods and services in a "smart city." The ESEC proposes to study the implementation of local boards in charge of conserving and managing personal data, e.g. used to improve city services. These boards would be administered by all the city's stakeholders (residents, local governments, businesses, associations) and could in particular, in the context of a social, solidarity-based economy, participate in the emergence of trusted third parties. The ESEC recommends that the CNIL label these trusted third parties and that they be subject to regular external audits, as suggested by the National federation of trusted third parties (CNTF, *Fédération nationale des tiers de confiance*).