ESEC'S OPINION

RÉPUBLIQUE FRANÇAISE
LIBERTÉ - ÉGALITÉ - FRATERNITÉ
CONSEIL ÉCONOMIQUE SOCIAL ET ENVIRONNEMENTAL

Les éditions des Journaux officiels

Towards a European digital sovereignty policy

Benoît Thieulin

CESE 07 MARCH 2019

2019-07

NOR: CESL 1100007X

mercredi 13 mars 2019

OFFICIAL JOURNAL
OF THE FRENCH REPUBLIC

2015-2020 term - Session held on mercredi 13 mars 2019

TOWARDS A EUROPEAN DIGITAL SOVEREIGNTY POLICY

Opinion of the Economic, Social and Environmental Council

presented by

Benoît THIEULIN, rapporteur

On behalf of the

Section for European and International Affairs

Question referred to the Economic, Social and Environmental Council by decision of its Bureau dated 11 September 2018, in accordance with Article 3 of Amended Order no. 58-1360 of 29 December 1958 introducing the organic law on the Economic, Social and Environmental Council. The Bureau tasked the Section for European and International Affairs with preparing an opinion entitled "*Towards a European digital sovereignty policy*". The section, presided by M. Jean-Marie Cambacerès, appointed Mr. Benoît Thieulin as rapporteur.

Contents

Opinion

Presented on behalf of the Section for European and International Affairs

The whole draft opinion was adopted by open ballot by 147 votes with 13 abstentions

TOWARDS A EUROPEAN DIGITAL SOVEREIGNTY POLICY

Benoît THIEULIN, rapporteur

I - DIGITAL REVOLUTION IS AN UNPRECEDENTED CHALLENGE FOR EUROPEAN SOVEREIGNTY

A - A proven economic dependency with major societal implications

1. The overwhelming dominance of the American GAFAM and the growing presence of Asian platforms (BATX)

Since 2007, when Apple introduced the first smartphone, the development of digital features[1] and uses has increased the concentration of European and international markets around a few mainly-American major players, referred to as GAFAM (Google, Amazon, Facebook, Apple, Microsoft). This "tactile revolution" built on operating systems allowing the use of applications on smartphones (IOS for Apple, Android for Google) has improved the position of these economic operators and has widely contributed towards the development of other companies offering hosting, online marketing or social networking services (e.g. Facebook which has purchased Instagram and Whatsapp), referred to as "major digital platforms". Available data[1] confirms such domination by a handful of stakeholders. In 2016, the global mobile phone operating system market was split between Android (85%) and IOS (14%), and as regards tablets, this market was dominated by Android with 66% of the market, with 22.4% for IOS and a little over 11% for Windows (Microsoft). As regards search engines, in 2018, Chrome (Google) accounted for over 67% of pages visited compared with 11% for Firefox and 7% for Internet Explorer (Microsoft), with the remainder shared between Safari (a little over 5%) and Opera.

The global market for smartphone sales also highlights the growing presence of Asian stakeholders: during the third quarter of 2018, South-Korean company Samsung dominated the market with a little over 20% of all sales compared with 14.6% for the Chinese company Huawei, 13.2% for Apple, 9.7% for Xiaomi and 8.4% for Oppo, with the remainder being shared between several other actors with less than 1% each[2]. During the 2010s, the Chinese BATX (search engine Baidu, online retail website Alibaba, platform Tencent and Xiaomi, a company manufacturing electronic and computer equipment) have become important stakeholders in the current digital world and are showing a growing interest in the EU market. These companies are cementing their presence through alliances

[1] ZDnet website.
[2] ZDnet website.

(Tencent and Spotify, Alibaba and Auchan), equity investments (Tencent's investment in Snapchat) or offensive marketing strategies (highly competitive quality/price ratios for Xiaomi equipment), made possible due to their dominant position in their domestic market and to support from the Chinese government which appears inseparable from the social control model in place in this country.

These digital giants' global market capitalisation[3] reflects not only their control over the sector but also their considerable financial weight in the global economy: Apple, Alphabet (Google), Microsoft and Amazon's market capitalisation stocks represent somewhere between €354 and €837 billion, BATX's are somewhere between €47.5 and 347 billion[4] - although the GAFAM's market capitalisation has been in decline since September 2018 due to several recent highly-publicised cases, as well as growth perspectives and market regulations which have made investors more cautious. In terms of investments, the GAFAM also hold significant weight with €46.6 billion invested by the top 20 digital companies in the world during the first quarter of 2018, including €32.5 billion by the GAFAM alone, primarily in the field of cloud computing (*data centres*)[5].

Opposite this strike force, there are no European digital operators among the leading global companies in the sector, nor are there any occupying a privileged position in any of its segments. Only a few European platforms are able to hold their own, such as the Swedish company Spotify, valued at €26 billion in April 2018, the French company Deezer - both music streaming leaders - and the Germany company Zalando (€4.8 billion) in the field of online retail. In fact, Spotify and Zalando are the only European platforms to feature in the Forbes Digital 100 ranking which lists the 100 top global digital companies all sectors included (October 2018). Furthermore, the EU is home to several tens of unicorns - i.e. start-ups valued at over $1 billion and not listed on the stock exchange -, two of which are French: the collaborative platform Blablacar (€1.6 billion) and the hosting service provider OVH (€1.1 billion). However these nuggets are still modest in size compared to the American and Asian giants whose ability to massively invest can be seen, in some respects, as a way of preventing any real competition, or at the very least as a way of stopping any market newcomers from closing the gap and cementing their position. In such a context, and in the absence of a global leader, European operators' ability to make the most of the sources of growth promised by the rise of the data-driven economy is questionable. These doubts are all the more valid given that the European digital sector is expected to be weakened by Brexit, with the United Kingdom being the State with the most unicorns (over 10, ahead of Germany), although, conversely, the United Kingdom's exit from the European Union could also make it more difficult for American platforms to access the single market.

[3] PriceWaterhouseCoopers firm, 2018.

[4] Source: Bloomberg, November 2018.

[5] Synergy Research firm.

Furthermore, the use of human resources by major American platforms also increases their lead. In the field of new technologies, there are many young graduates trained by the main French schools and universities who are moving abroad to use their talents to profit major digital companies or Silicon Valley *start-ups*: the channel France Info estimates that there are around 70,000 of these graduates. As underlined in the French Economic Analysis Committee's report on "Preparing France for International Talent Mobility" (May 2016), this brain drain poses an issue in terms of fairness, as the cost of their training has been borne by the State and, in return, they will not be contributing towards the country's growth; this brain drain therefore also feeds tax competition (or tax dumping) by penalising the States in which the proportion of public funding for higher education is high (France, Germany, Nordic countries) to the benefit, for example, of the United Kingdom or the United States[6]. However, for France, the magnitude of this phenomenon should be relativized. As the ESEC recalled in its opinion of October 2015 "International migrations: a global issue", our country has a significant delay in this field compared to its neighbours (Germany, United Kingdom) and is therefore in a catch-up phase, as confirmed by the low number of figured and reliable data on the topic. Our country, like other European countries, is also marked by a lack of women in digital training and digital occupations. Women represent only 33% of all employees in digital occupations, and 75% of this third work in "support" functions (human resources, communication, administration, etc.), when they are more qualified than men. In a context of global competition, this lack of women is a major "loss of opportunity".

2. Real risks for the EU's economic development

This sector's unbalanced situation, which is sometimes described as a "colonisation" of the European digital market by major American platforms, is a huge risk for the EU's economy, but also for its workers and citizens who only benefit from a limited offer. The first risk is that of witnessing obstacles to competition that are likely to arise from an oligopolistic situation[7]. For example, the division of the smartphone operating system market between Google and Apple alone means that all users within the EU are now held captive by Android or IOS when installing apps on their phone, and that the companies developing these apps are also dependent on these two giants to make their products available to the public; this lack of competition could adversely affect the setting of fair prices and the quality of products, as well as innovation and working conditions. Similarly, the near-monopoly exercised by the main digital platforms on the search engine market allows them to control website referencing and affects the transparency of the algorithms that determine the order in which search results appear, resulting in significant

[6] OECD 2015.

[7] An oligopolistic market is marked by a low number of suppliers (sellers) and a high number of consumers (customers).

consequences on the accessibility of the websites referenced and on their market potential in respect of users.

Thus, in accordance with Article 102 of the Treaty on the Functioning of the European Union (TFUE), the European Commission condemned Google on two occasions for abusing its dominant position: once in June 2017 for having favoured the use of its e-commerce interface *Google Shopping* (imposition of a €2.42 billion fine); and a second time in July 2018 for having imposed recourse to its search engine *Google Search* and protected its dominant position using various methods including selling apps as a bundle, providing financial incentives to manufacturers, obstructing the sale of competing versions of Android (including Amazon's Fire OS), with the €4.34 billion fine having been combined with the obligation for Google to put an end to its anti-competitive practices or risk a new fine of up to 5% of its worldwide turnover.

Furthermore, for other multinational companies, the dominant position held by the main digital platforms has favoured the implementation of complex tax optimisation and tax avoidance frameworks. By sentencing Apple to refund Ireland €13 million during the summer of 2016, the European Commission highlighted the payment of illegal State aid leading to a "distortion of competition" in the form of a highly-beneficial selective tax treatment: in 2014, the tax rate applied to Apple Sales International profits was of only 0.05%. A similar situation was discovered in Luxembourg with the LuxLeaks scandal. In its opinion on "Tax avoidance mechanisms, their impact on tax consent and social cohesion" of December 2016, the ESEC demonstrated how some multinational companies manage to reduce their tax base or repatriate all of their profits to a single Member State with a more favourable tax regime or to their head office outside of the EU, thereby depriving the States in question of budgetary resources, damaging social progress and fuelling a strong sense of tax injustice.

In the digital economy, these well-known issues are compounded by the effects of the platforms' structures and the type of services offered. These services can be accessed without the company being represented within EU territory or within the Member State in question (such as social networks, streaming websites) or can involve structures present in several countries, which makes it more difficult to assess the notion of "permanent establishment". More importantly, for platforms, the principle of value added tax, which structures international tax rules, clashes with the fact that these platforms are based on an unprecedented form of value creation, built on exploiting users' data. The data generated by Internet users are exploited by the platform for targeted advertising purposes or sold through a data broker to an entity intending to analyse them or sell them to a third-party company: the value created from such data, which is often collected with users' unwitting collaboration, is therefore based on a new type of intangible property which is difficult to define and therefore difficult to subject to tax. All of these factors help to explain that, according to the European Commission, despite a high growth rate - of around 14% (against 3% for the average European company) -, the tax rate applied to digital economy companies is on average around 14 points lower than similar companies in other sectors (9% versus 23%).

All of these marketing and tax distortions have a significant effect on medium-sized economic operators, who find themselves in asymmetric relationships in which they are more or less dependent on major platforms, as demonstrated by the Google Search scandal. This dependency can result in the application of unfavourable marketing conditions and other types of questionable practices, for example as regards referencing. It also directly weighs on the emergence of the European digital market, comprised of a few exceptional (Zalando, Spotify) medium-sized operators. Confronted with the need to reach a critical size to ensure their development and escape a relation of dependency on American and Asian Internet giants, these medium-sized operators are fa ced with a significant obstacle in terms of financing. While public financial institutions concentrate on financing research and innovation, the next stage in companies' development is provided for by venture capital companies in the absence of a stock exchange listing for European start-ups. As such, European companies often have very few issues in financing the first stages of their development, sometimes relying on advantageous national initiatives such as French Tech; however, they do experience difficulties in finding European investors for the following stages. In such a context, in most cases, European digital companies can only grow by turning to investors outside of the EU, or by simply being bought by major American or Asian operators.

In addition to digital operators, a growing number of economic sectors are becoming increasingly and quickly dependent on dominant platforms. Many digital platforms play a role as a vital intermediary in pre-existing commercial transactions. In this respect, two types of platforms exist: those which merely match supply to demand, similar to an improved small ads system (e.g.: Le Bon Coin, a French advertising platform); and those which organise work by managing workers with more or less dependency (e.g.: Uber), and which raises the question of whether or not these arrangements should be requalified as employment contracts.

Although the collaborative platforms' ambition of acting as an intermediary to facilitate access to goods, content, information or services offered by private individuals or companies (*relation platform to business* - P2B) is a powerful lever for development for companies, improving their relations with potential customers, it also poses a risk due to the asymmetry between the dominant position held by major platforms and the high number of companies using their services (estimated by the European Commission at around one million in the EU in 2015). Platforms are therefore able to influence referencing by removing a company from search results or by removing a product from an online sales service; they can also change pricing conditions or terms and conditions of use without notice, which was the case during the summer of 2018 with the sharp increase in GoogleMaps' professional tariffs. The situation of the accommodation sector in light of platforms such as Booking.com or Expedia is another typical example of these platforms collecting an increasing share of added value generated by a given sector. Small and medium-

sized enterprises (SMEs) are particularly vulnerable to these practices due to the amount of them that use online service platforms - around 42% according to the European Commission - with a large majority of them using search engines to promote their products[8]. Furthermore, with the development of collaborative platforms, new uses and models have appeared, causing major upheaval in many activity sectors, with tourism, accommodation, transport and retail on the first line. These sectors must compete with a new offer, based on a collaborative model between private individuals, between companies and individuals, or between independent workers and individuals; the effects of this are all the more significant given that this movement had not been anticipated by the "original" sector and that these collaborative consumption models appear to match citizens' profound aspirations. In sum, the boom of the data-driven economy generates a systemic risk which increases the EU's vulnerability as a result of its relative situation of dependency, whilst profoundly affecting its social relations. In view of the strong presence of digital platforms in the United Kingdom and this country's position as a financial intermediary, Brexit's consequences on these evolutions could be significant; and yet, in the absence of a stable agreement on the terms of the United Kingdom's exit and on its future relationship with the EU, these consequences are difficult to determine.

3. A major societal impact constituting a challenge for the European model

The tactile revolution, and particularly the rise of collaborative platforms offering a wide range of activities (Airbnb, Uber, Blablacar, Deliveroo, etc.), has generated doubts regarding the models used to structure relationships between companies, between companies and private individuals, and between individuals themselves - and as a result those used to structure relationships between social partners. As underlined by the General Inspectorate of Social Affairs (Inspection générale des affaires sociales, IGAS) in 2016[9], this issue is still under-documented and encompasses a wide range of realities and statuses (employees, independent workers, microenterprises) with their overall impact on the volume of employment being difficult to assess; however, all signs point to the belief that these platforms have a significant potential for growth and that they will have major effects on employment in the future. While the introduction of platforms as intermediaries, and often as trusted third parties, generates new forms of employment, it could also deteriorate working conditions in the sectors in question, with at least some of the jobs thus created being low-skilled and low-paid work (drivers, couriers). In its opinion on "The new types of independent work" in November 2017, the ESEC described the new "faces of independent work" - platform workers and micro-

[8] Eurobarometer 2017.

[9] General Inspectorate of Social Affairs, report on "Collaborative platforms, employment and social protection", 2016.

entrepreneurs - and underlines the fragility of their position both in terms of social rights and in terms of their dependency on a major principal. These new forms of employment often turn the employee/employer relationship into an individual service provider relationship. This results in a relationship of economic subordination in which the worker bears all of the risks and which goes against the principle of equal treatment[10]. At European level, these vulnerable workers are estimated to account for 17% of independent work[11].

Given the role played by digital technologies in economic development, working relationships and social relations in all of their aspects, accessibility has become a crucial issue both materially (connectivity, access to the service) and on the virtual scale of uses. While access to digital technologies is likely to reduce territorial isolation and even promote employment - for example by reducing the impact of mobility issues -, the distancing of digital tools, in terms of equipment or skills, is, on the contrary, a considerable factor that worsens inequalities and social and territorial fragmentation. In 2017, 87% of EU households had access to internet and 57% of Europeans aged between 16 to 74 used the Internet to make online purchases[12]. While these figures demonstrate the democratisation of access to digital technologies, they do not provide details regarding the skills to use these tools, although 13 million French citizens state that they do not have the necessary skills to use digital interfaces (platforms of all kinds and online public services)[13]; an observation which is said to attest to the situations in which social rights were not activated following the substitution of physical desks by online platforms. Due to the fact that it reduces access to public services and social rights, the digital divide has become a factor causing exclusion, which breaks with equality; yet, the digital can and must be a factor of social progress. Furthermore, although the difference in Internet access is now very low and even non-existent between urban and rural areas in Northern Europe (Scandinavian countries, Luxembourg, Germany, Belgium), it is still significant in Member States such as France, Bulgaria, Greece or Portugal[14]. Therefore, the issue of digital inclusion for social and territorial cohesion in the EU and its Member States should not be underestimated.

The EU's situation of dependency as regards digital technology could also threaten the implementation of the environmental model that it is striving to achieve and which it perfected by signing the Paris Agreement. While digital technology is likely to promote the appearance of new and more environmentally friendly-

[10] It is worth noting that in its Decision no.1737 of 28 November 2018, the Court of Cassation issued a ruling on a case involving a contract between a bicycle delivery person and the company Take Eat Easy: it identified a relationship of subordination between the delivery person and the platform and therefore considered that an employment contract existed between them.

[11] Euractiv, 2018.

[12] Eurostat 2017.

[13] Digital barometer 2017.

[14] Eurostat 2017.

production and consumption modes, its current economic model is no less problematic in terms of sustainability. The manufacturing of equipment (mobile phones, tablets, laptops, connected devices) has a significant impact on the environment due to the water and raw material resources - including rare metals - required, and due to the pollution that it generates; rare metals also mean the dependency of several Member States on producing countries, including China, a topic on which the ESEC issued an opinion in January 2019 entitled "Dependency on strategic metals, what are the economic solutions?". Furthermore, the commercial strategy adopted by manufacturers and the consumption methods adopted by users are themselves based, in some cases, on non-sustainable principles, on reduced life cycles[15] and on the acceleration of product renewal, which once again raises the issue of the consumption of resources necessary to manufacture the device, but also raises that of electronic waste and how to recycle these devices which contain harmful chemical substances. In 2016, the flows of this type of waste increased from 3 to 5% per year, while collection rates remained varied depending on Member States - from 26.3% for Latvia to 94.1% for Croatia (46.3% for France) -; of the proportion of waste collected, the rate of reuse, recycling and recovery was between 80 and 90% for most EU countries[16].

The environmental footprint of digital technologies is also determined by how much energy digital devices consume, and this depends on the amount of hardware and on the choices made in terms of coding, data management and processing (software), with consumption being lesser when codes are better written. Finally, uses also affect energy consumption, although studies are still needed to better understand its consequences. The IT sector (manufacturing, use) is said to represent 7% of electricity consumption worldwide and its environmental impact is said to match that of the aviation sector[17]. The number of operating devices worldwide (computers, smartphones, connected devices) is estimated to be around 9 billion, accounting for 47% of digital greenhouse gas emissions, with the remainder being shared between data centres (25%) and network infrastructures (28%)[18]. *In France, data centres alone consume around 3 TWh/year according to RTE, i.e. around twice the electricity consumed by the city of Lyon (2015 base)*[19]*. By taking into account the manufacturing and the use of all of these devices, the ecological footprint of the digital sector is estimated at around 200 kg of greenhouse gases and 3,000 litres of water per internet user, per year. Like the air and maritime transport sectors, the digital sector is therefore a significant emitter of greenhouse*

[15] Apple and Samsung were fined in Italy for planned obsolescence and, in France, a complaint made by the association *Halte à l'obsolescence programmée* has been under investigation since January 2018.

[16] Eurostat 2017.

[17] GreenPeace, "Clicking Clean" report, 2017.

[18] ADEME, report on "the dark side of the digital sector" ("*La face cachée du numérique*"), 2018.

[19] Negawatt, Will the digital revolution skyrocket our electricity consumption? (*"La révolution numérique fera-t-elle exploser non consommations d'électricité ?"*) & EDF, Data centres' energy efficiency (*"L'efficacité énergétique des data centers"*). ENR'CERT 2016.

gases, when no discussions have yet been launched at European or international level to reverse this trend which is expected to quickly increase in line with the number of users. Thus, in accordance with its commitments, the EU must implement rules and standards to reduce the digital sector's environmental footprint, and it must concentrate its initiatives around taking social aspects into account to ensure a fair transition.

B - Ethical and security implications making data management a crucial political issue for Europe

The economic model used by platforms such as Google or Facebook is based on the free provision of a service, ensuring that users' networks spread, which is made possible by exploiting the data collected to place targeting advertising and resell data. The value created using users' data, often without their consent, and the volume of digital data has skyrocketed: over 90% of data available today have been produced over the last two years[20] and the global volume of digital data, and particularly of personal data, has increased due to the rise of the Internet of Things. This concept is central to the economic model used by several digital giants, including Alphabet (Google) and Facebook, who generate 88% and 97% of their income respectively from exploiting data collected for marketing purposes[21]. In such a context, the development of a data-driven economy results in a significant increase in ethical, security and political issues relating to digital sovereignty. Although American operators' domination in Europe is not the source of this phenomenon, it does cause the asymmetrical relationship in which the EU must tackle these issues. Furthermore, the ethical and security issues addressed in this section are generic: although today's dominant operators are mostly American (and possibly Chinese), these issues also concern European platforms. They are tied to a natural propensity towards a monopoly over the platform economy in which "the winner takes all".

1. Issues pertaining to ethics and the protection of fundamental rights

The attention economy - or the commodification of the reader's available brain time - was not born with the rise of GAFAM. However, the digital era and the Internet have both caused a break-away: while a traditional newspaper generates income by selling content and through marketing, Facebook or Google also market "attention traces" left by their users - from a simple "like" or "retweet" to the connection location and the time spent on given content. For example, Google subjects nearly all of its services (Google search, Gmail, Agenda, Drive, Android,

[20] IBM.

[21] Statistica Digital Economy Compass 2018.

YouTube, etc.) to a single “privacy policy” which provides that the company can collect the name, photograph, email address and phone number provided by individuals with a Google account, but that it can also collect the identifier of the device used to connect, information on the use of the services (videos and images seen), the browsing history, search requests and many other types of data. Besides the highly-personalised displaying of advertising through the information provided by the data collected on the user, Google has also implemented a go-between feature which puts advertisers in contact with third-party websites wishing to earn an income through targeted advertising: on each of these websites, Google is in charge of the technical aspects of displaying each advert, which means that it can place cookies and other trackers allowing it to access the browsing history of internet users who do not even use its services. An analysis of the traffic on websites such as lemonde.fr, lefigaro.fr, hadopi.fr or defense.gouv.fr, among others, demonstrates that various requests are sent to doubleclick.net, Google’s marketing platform, when browsing these websites, allowing the platform access to the addresses of each page visited.

By disseminating open tools which allow developers to create mobile apps compatible with the Android operating system, Google was also able to promote the dissemination of trackers in many apps: thus, traces of Google trackers have been found in the codes of applications such as Deezer, Spotify, Uber, Tinder, Twitter, Le Figaro, L’’Équipe, Crédit Agricole, Boursorama and Angry Birds[22]. Similarly, the strong presence of Facebook trackers has been noted in mobile apps; although some of these trackers clearly state their intentions - targeting users for marketing purposes -, others are more secretive and do contain risks, such as Pregnancy apps (which collect information on children soon to be born, with the official purpose of accompanying young parents) or Diabetes:M, which provides Facebook with the identity of individuals suffering from diabetes. The risks that are inherent to the sprawling collection of personal data are further aggravated by the major expansion of new operators, in the form of data brokers: these data brokers - who collect personal data to analyse them, cross-reference them with digital identities and then resell them - constitute a third level of data collection, a new marketing strata under development. Among these companies, most of which are created in the United States, Acxiom is said to be the most influential: providing data and statistics to marketing and fraud detection companies, according to the Federal Trade Commission, it holds around 700 million pieces of data on consumers around the world, allowing it to generate close to €850 million in income in 2016[23]*; its subsidiary Acxiom Europe alone is thought to have collected up to 600 pieces of data per household on 6 million French households. Conversely, another American company called Datalogix retrieves its data from online bank transactions in order to sell them to groups such as Facebook and Google who use such data to better target their*

[22] Exodus Privacy

[23] Federal Trade Commission.

marketing offers: thus, a real data market has established itself, within which intermediation platforms, data brokers and other private and public clients all work together. These issues were also addressed in the ESEC's 2015 opinion on "Coproduction under the digital era" ("La coproduction à l'heure du numérique")

The problem with this data-driven economy is first that of valid and informed consent. While the General Data Protection Regulation (GDPR)[24] provides that, to be valid, consent must be explicit, a platform such as Google for example works on acceptance by default using pre-ticked boxes. Facebook was sentenced in several Member States by computer freedom protection authorities due to its personal data processing and illegal tracking policy, however it has not put an end to these practices: in 2017, in France, the Commission National Informatique et Libertés (CNIL, French data protection authority) sentenced the company to a €150,000 fine, while its Spanish counterpart sentenced it to a €1,200,000 fine. On 21 January 2019, following a collective action taken by the association La Quadrature du Net, the CNIL issued Google with a €50 million fine based on the GDPR: according to the French independent administrative authority, the lack of information provided by Google placed the internet user in a position in which "he/she was not able to understand the magnitude of the processing [...] of a particularly wide-scale and intrusive nature". The CNIL also noted that acceptance boxes, in addition to being difficult to access, were pre-ticked by default (such as the displaying of personalised advertising) and that the conditions for use were presented in such a way that users were forced to accept them all.

Similarly, the data extracted by data brokers is often taken without the free and informed consent of users, as they impose off-putting and rarely read general terms and conditions of use or conclude agreements with intermediation platforms. Clearly, these practices are issues in terms of respecting the EU's values, including the Charter of Fundamental Rights which provides that "everyone has the right to respect for his or her private and family life, home and communications" (Article 7), "to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law", as well as "the right of access to data which has been collected concerning him or her and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority" (Article 8).

Pursuant to the GDPR, the EU must therefore compel platforms, developers, data brokers and other private and public clients to respect users' valid and informed consent when collecting data. This particularly concerns manufacturers of connected devices, who should be bound by an obligation of information as regards the security risks and privacy violation risks relating to these devices as well as by

[24] In force in all member States since 25 May 2018, it provides EU citizens with a framework for the protection of their personal data.

the implementation of technological adjustments which would minimise these risks (mechanisms to block webcams for example).

In addition to the legal and ethical risks of data collection, the model adopted by platforms promotes algorithmic confinement which can result in individual or collective conditioning and even high-risk behaviours. While French citizens spend on average 4h48 per day on the internet and 1h22 on social networks[25], the Facebook company is said to have changed the newsfeed of 700,000 users in 2012, without informing them, so as to highlight content likely to influence their mood: the study concluded that "targeted users started to use more negative or positive words depending on the nature of the content that they had been exposed to"[26]. The aim of collecting data and attention traces, in a context of strong competition between platforms, has led these platforms to develop strategies with a view to psychologically influencing their users and maximising their presence on networks. One approach is to exploit users' profiles to suggest content that closely matches the content that they already like or view, in a space selectively structured around conflicting content , which some specialists refer to as a filter bubble: while the effect of such bubbles on individuals' opinions should not be over-estimated (In France, no terrorists seem to have become radicalised through this medium), the risk of ideological and cultural partitioning is still very real. Conversely, on some platforms, the hierarchisation of entirely personalised content can be a way of concealing underlying ideological opinions. Other hierarchisation algorithms are designed to grasp the users' attention, to the detriment of the quality of the information, and even on the users' well-being; in a report to the Prime Minister dated 20 September 2018, it was observed that there could be "*a perverse link between hate speech and marketing effects: individuals expressing shocking or extremist views are those who "earn" the most as they are the ones generating the most reactions, whether positive or negative. As such, the financial ambition of social networks is to accommodate as many as possible*".

Through these practices comes the broader and more fundamental issue of net neutrality and platforms' responsibility with regard to the content that they host. A founding principle of the Internet, neutrality ensures equal access to the network regardless of who the user is and the service that they connect to. In particular, it prevents any positive or negative discrimination with regard to the source, the destination or the content of the information transmitted on the network, meaning that no technical intermediary may promote, slow down or block the information viewed, unless requested by a judge; it ensures that all users have access to information and the means of expressing themselves under non-discriminatory, fair and transparent conditions. Given the interdependency between the different components of the digital sector, the principle of neutrality therefore originally relates

[25] App Annie, 2018.

[26] A.D. I. Kramer, J. E. Guillory, J. T. Hancock, Emotional contagion through social networks. Proceedings of the National Academy of Sciences 2014, 111 (24).

not only to platforms, but also to operating systems, telecommunication networks and the infrastructures providing access to the Internet: this principle applies to the digital sector as a whole. Although the topic is less discussed, the concept of net neutrality should also apply in two key fields: that of apps, particularly smartphone apps, in which the subscriber can be forced to use, at least by default, the applications provided by the device provider; and that of operating systems, for the same reasons. For example, in the industry, purchasing a 3D printer forces the user to use the operating system provided by the seller.

Yet, this principle of neutrality is now brought into question in the digital universe. Within the EU, the theoretically strict protection provided by law clashes with the quick development of uses. In the United States, net neutrality has already been abolished since a vote held by the Federal Communications Commission in June 2018. This measure would meet the expectations of telecommunication operators and service providers, who see in it a guarantee of freedom enabling them, for example, to offer differentiated offers to Internet users depending on their profile, or to request payment from companies that would like their services to be provided as a priority; according to these operators, the resources thus generates would allow them to modernise their infrastructures to adjust to uses that take up more and more broadband - with services such as Netflix or YouTube for example. However, for associations defending digital freedom, the end of neutrality presents a risk of a rise in prices and in censure; more importantly, the user's position as a subject, a customer of the service provider and an internet stakeholder would be transformed into a position as an object, a "good" that the telecommunication operator could "sell" to the platform via an agreement with the latter in order to promote its dissemination.

The decline of the principle of neutrality has serious consequences. Hiding content in search engine results or on a social network could be considered a denial of the user's right of access to information - when a study carried out in the United States in 2017 showed that over two-thirds of adults gathered their information from social networks[27]; from the point of view of the emitter of the content, this also raises the issue of freedom of expression, with search engines or social networks able to choose to reduce or entirely erase the visibility of a person and of their opinions. In a time marked by the digitalisation of cultural consumption and information, the risk of harming cultural diversity and the plurality of information cannot be ignored given the control taken by a small number of American platforms over access to entertainment: in terms of cinematographic content for example, it is clear that major producers such as Netflix, who have a better capacity of negotiating with operators, would be in a more advantageous position, whilst smaller operators could see the download rate for their content slow down, and therefore less pleasurable to use. Thus, the bringing into question of net neutrality weakens content producers by threatening their income, including as regards intellectual property. The German

[27] Pew Research Center, News Use Across Social Media Platforms, 2018.

media group Axel Springer lost 80% of traffic and was forced to abandon the idea of making Google pay to reference its papers after the platform benefitted from its dominant position to remove it from its news service *Google News*. The EU must therefore respect and impose net neutrality in accordance with respect for the principles of freedom of access to information and freedom of expression.

2. Increased vulnerability to cybercrime

With the extension of infrastructures, content, digital uses, societal and ethical risks are accompanied by growing security risks due to several factors[28]:

- the very model used by GAFAM is based on dispossessing users of their digital sovereignty by collecting their data and traces on the Internet, and on exploiting the "network effects" studied by Michael L. Katz and Carl Shapiro. This model clashes with the requirements of managing and securing data. The ubiquity of digital data[29] limits public authorities' ability, both in terms of security and of taxation, to regulate and control the cyberspace: the circulation of such data raises the issues of extra-territoriality, overlapping of sovereignties and therefore conflict of jurisdictions. Although these phenomena are tied to the nature of digital technology and not to the primacy of any given operator, they are no less exacerbated by the hegemonic position of the GAFAM;
- domination by a few major operators also promotes the increased centralisation of data management, which increases the system's vulnerability. This centralisation involves a process to standardise and homogenise tools, which promotes the dependency of a low number of operators; it also results from the pooling of large amounts of data on unique media, the failure or the denial of service of which is likely to cause the malfunctioning of many client services in a short period of time. This is how, in early 2017, the failure of Amazon's *cloud computing* service, which alone represents over one third of the global market and hosts the data of many companies - including 80% of that of the CAC40 - and administrations (such as the American *Security & Exchange Commission*) affected a large proportion of the internet worldwide for several hours and threatened the entire global economy. This concentration trend should accelerate, bringing the proportion of global digital data stored by major American hosts to over 50% in 2025 and promoting the development of gigantic infrastructures, "*big data centres*", 40% of which are located on United States territory[30];

[28] F. Douzet, Les actions offensives dans le cyberespace sont permanentes (Offensive cyberspace initiatives are permanent). Le Monde, 23 July 2018.

[29] The notion of ubiquity of digital data translates the ability to access such data from any device, anywhere and at any time.

[30] M. des Gayets, La grande dépossession - pour une éthique numérique européenne (The great dispossession - towards European digital ethics). Fondation Jean Jaurès & Fondation européenne d'études progressistes, 2018.

- the security risks thus linked to the model adopted by platforms and the data-driven economy should continue to increase with the development of the Internet of Things. While the number of connected devices in circulation could exceed 30 billion within three years according to some estimations, these are likely to be misused with the risk of not only compromising their users, but also enabling attacks on third parties. In August 2017, the *Food & Drug Administration*'s discovery of security breaches allowing third party operators to change the orders of pacemakers implanted in over 500,000 individuals worldwide - 40,000 of which in France - illustrates the first type of risk; whilst the second materialised in 2016 when the European host OBH was attacked by a confluence of requests from over 145,000 connected devices that had been hacked by the Mirai malware. Smart networks and smart meters could also increase the available attack surface due to the fact that they lead to a multiplication of entry points to a single network on which sensitive data is exchanged[31];
- the vulnerability arising from these structural weaknesses is compounded by the tendency of all stakeholders, whether individual users, companies or administrations, of underestimating the dangers that are inherent to digital platforms. This warped perspective appears to be not only a result of a lack of knowledge of risks relating to the use of digital tools - 63% of security incidents affecting companies are caused by the behaviour of an employee -, but also of the satisfaction felt by platform users in respect of the service provided, which would lead them to make more or less conscious choices towards benefits (which are real) to the detriment of risks (which are hypothetical), and this choice is made easier by the frequent existence of a significant time gap - sometimes years - between the theft of data, its discovery and the potential misuse of such data. The managerial departitioning enabled by digital technology and which multiplies the number of holders of potentially sensitive data, and the complexity of the use of secure tools could also play a role in the overall vulnerability of systems.

The consequences of security threats to European sovereignty affect economic activity as well as social relations and the functioning of political institutions. The impact of cybercrime on corporate life and on economic growth should not be underestimated: according to the 2017 *Breach Level Index* report, 2.5 million pieces of data were stolen that year worldwide, mainly from internet websites or company servers, representing and +88% increase in one year; 60% of companies having lost their data, all sectors included, were forced to file for bankruptcy in the following semester, with the average cost of a data breach amounting to $3.6 million. In addition to the hacking of confidential industrial data - which is said to have affected

[31] M. des Gayets, La grande dépossession - pour une éthique numérique européenne (The great dispossession - towards European digital ethics). Fondation Jean Jaurès & Fondation européenne d'études progressistes, 2018.

30% of companies across the world in 2016 according to the 2016 Global Index Data Protection study - risks arise from the criminal disclosure of customer files - which the company Uber fell victim to in 2016 -, online payment fraud, identity fraud, and the paralysis of systems by computer viruses: the French group Saint-Gobain was a victim of this in 2017.

As regards the risk affecting social ties and the respect of EU values, it is clear that the development of platforms - and particularly collaborative platforms - has gone hand in hand with the increased dissemination of illicit content, whether racist or antisemitic messages, homophobic or sexist messages, violence against women online, incitement to hatred, information relating to illegal activities such as terrorism or child pornography, or content violating economic rights such as copyrights. The EUKids investigation considers that children aged between 11 and 16 years old are 20% more likely to be confronted with hate speech. This situation could be a result of the rapid technological and structural development of the digital world as well as of the sharp rise in the volume of digital content; it could also be encouraged by the anonymity granted by the Internet, although this factor is disputed, as well as by the lack of education on digital issues which is said to promote a dissociation between offline life and online life by Internet users, with the second of the two being considered “unreal”.

However, it appears that the main factors are the weakness and heterogeneity of regulatory provisions currently in force in the EU and in Member States, the lack of affirmation from public authorities on these issues and the insufficient resources devoted to prevention and action, thereby slowing the development of necessary cooperation between public and private stakeholders on these topics at EU level. For example, for France, the Act of 21 June 2004 for trust in the digital economy has had a lesser impact due to the modest nature of the potential penalties ; in most Member States, the mechanisms for users to report illegal content and for platforms to block such content are not very effective as they are not transparent enough and are slow and difficult to implement. At EU level, the difficulty arises from the ambiguity of the position taken by platforms as regards the content disseminated, with the European directive on e-commerce setting out the principle according to which online intermediary service providers must not be held responsible for the content that they transmit, store or host, if they only have a passive role.

Lastly, cybercrime presents a political and strategic threat for the EU and its Member States, as it does on other States and international organisations, which can only be amplified by the digital dependency experienced by Europe. While geopolitical power relations are in the process of solidifying, reducing State’s desire to cooperate to regulate systemic risks together, around thirty States in the world are officially claiming their ability to roll-out offensive initiatives in cyberspace: the EU’s sovereignty is also tied to its ability to face these threats, which include risks to digital and telecommunication infrastructures - military, but also civil, e.g. energy infrastructures -, the collection of data by foreign intelligence agencies, the exploitation of vulnerabilities in the produces disseminated by companies and the dissemination of *fake news* capable of destabilising entire companies. In this respect, the United States’ domination over the European digital sector is all the more worrying given that this country has adopted an accommodative legislative which allows its intelligence agencies to access Internet users’ data held by its

companies, which collect most of the data produced or disseminated in European countries. As such, in 2014, the proportion of Member States' Internet traffic that actually stays within their territory was estimated by the Institut des hautes études de défense nationale at 70% for Hungary, Malta or Cyprus, and less than 25% for France, Germany, the United Kingdom, Italy, Greece, Romania, and Belgium, the Netherlands and Luxemburg.

3. Digital sector governance: a challenge for the rule of law and the democracy in the EU and its Member States

The EU's desire to establish solid Internet governance and to regulate the activity of online platforms is faced with many obstacles. Beyond the rapidity of technical and commercial development in the digital sector and the wide variety of platforms, which complicate the establishment of a single and legally relevant definition, several factors relate to the EU's unique situation or to its relationship with dominant American and Asian stakeholders:

- the European cyberspace is marked by its fragmented nature, due to the legislative and regulatory differences between Member States, whether in terms of cross-border e-commerce, consumer protection, online service portability, online administration, contractual law, intellectual property law or the fight against illegal content. Interoperability and normalisation are still insufficient at Union level. As a result of this fragmentation which restricts e-commerce and will continue to be exacerbated by Brexit, only 37% of cross-border online retail websites are estimated by the European Commission to have allowed a transaction to be completed in 2016, and, in 2015, less than 10% of companies and 16% of consumers are estimated to have performed a transaction in another Member State than that in which they resided[32];
- the absence of a unified European cyberspace makes the work carried out by supervisory authorities more difficult, both in Member States and at European level. Surveillance, control and penalty procedures are still slow and complex, tools to monitor and track platforms' activity are rare and not enough to counterbalance the lack of transparency of the algorithms that they are governed by. Cooperation between national public authorities on these topics is still very limited, as are the powers of the bodies established for this purpose, such as the Body of European Regulatory for Electronic Communications (BEREC). The resources granted by the EU and Member States to research digital technology and the role of platforms in the economy, as well as to promoting a sustainable Internet, capable of keeping digital "ecosystems" open, are insufficient given the stakes;

[32] R. Viola, O. Bringer, Vers un marché unique numérique: faire de la révolution numérique une opportunité pour l'Europe (Towards a single digital market: making the digital revolution an opportunity for Europe). Revue d'économie financière 2017/1 no. 125.

- according to X. Merlin and M. Weill, the fact that the EU has not yet succeeded in generating a digital giant capable of competing with the main American or Asian platforms has led the latter to promote " a specific digital company model centred around values (personal data protection, fair competition, fair taxation, etc.), the defensive aspect of which is often seen as a form of anti-Americanism"[33]. The European regulation model therefore falls within a context of industrial and capitalistic weakness, at the risk of curbing and coercing digital stakeholders instead of accompanying them. Furthermore, the lack of a shared international approach, particularly as regards regulations on sensitive personal data, causes significant friction between different legal systems for the commercial agreements that are currently under negotiation;
- lastly, a contradiction seems to have appeared between the aim of regulating platforms and private and public security requirements. In the private sphere, the confidentiality of exchanges demanded by users, for example following cases such as Apple v. Federal Bureau of Investigation or Edward Snowden's revelations on the widescale surveillance carried out by the National Security Agency, have led major digital platforms to offer improved encryption tools. For States, a dilemma has developed between their desire to protect personal data and the higher interest pushing them to exploit such data for security purposes. The EU, which benefits from the information provided by its American ally based on data relating to European citizens hosted by GAFAM, therefore has its strategic autonomy all the more restricted given that several Member States depend on NATO for their national security. France itself is striving to reconcile its concern for strategic independence with the development of strong operational cooperation with the United States. Conversely, the United States were able to prove the extra-territoriality of their right over data on American citizens hosted in Europe: this was the topic of the case opposing the United States and Microsoft's subsidiary in Ireland. The Chinese *Belt & road initiative* (BRI) aims to reach the European market by using not only railway and harbour infrastructures but also digital infrastructures, leading major Chinese platforms to increasingly invest in *data centres* located on European territory: the geopolitical and security issues arising from data management are no longer only transatlantic, but are becoming increasingly Eurasian. This issue is no longer restricted to American companies but is now raised in several countries as regards the network devices and hardware provided by Chinese companies such as ZTE and especially Huawei, who are accused of offences and collusion with public authorities in their country.

[33] X. Merlin et M. Weill, Quel avenir numérique pour l'Europe? (What does Europe's digital future look like?) Réalités industrielles, 2018.

The imperfect regulation of digital platforms' activities poses risks both for the organisation and the operation of Member States and for the EU's political stability. Platforms could compete with the authority role played by States, particularly in terms of security and justice, but also in terms of accreditation and assessment or adoption of public decisions; at the same time, the rule of law could be endangered by authorities' ability to use the surveillance and control opportunities provided by digital technology - and particularly metadata technology - to their benefit, as demonstrated by the links between private platforms and security services, at the risk of generating a society in which individuals are monitored by using algorithmic prediction systems. The public assistance and information role played by States, as public service providers, is also competed for by platforms, who are likely to cause private initiatives to take charge of services that up until now were public - the supply of electricity for example - or to make some activities profitable which up until now were not; this raises the question of how these alternative methods can provide safeguards in terms of security, continuity, neutrality and accountability. In addition to these roles, it is also the State's very organisation which is put to the test by the rise of digital platforms: traditionally structured in silos, the State is also encouraged to evolve into a "Platform State", providing resources enabling the general public to develop the services that it needs[34]. The State must maintain control and its role as a public service safeguarding general interest and the equal rights of citizens, by remaining physically present across the territory: public service is also defined by the maintenance of human contact - which promotes social cohesion - alongside digital services.

Lastly, the development of digital platforms brings into question how democracy works and the political stability of the EU and its Member States. The Cambridge Analytica scandal (Facebook) which, by its CEO's own admission, extended its activities to voluntarily disseminating false information, spying on its political opponents and resorting to corruption to manipulate public opinion abroad is a telling example of the political use that can be made of personal data. The British company was therefore able to use the data belonging to 87 million of the social network's users to benefit Trump as a candidate to the American Presidential elections of 2016; it was also accused of having influenced the outcome of the Brexit referendum in the United Kingdom. Russian interference in the 2016 American elections, a hybrid attack by which both information and data were instrumentalised to destabilise an entire company, is another example of the abuses that are now possible with the collection and exploitation of data, and the challenge posed by the informational threat to political democracy. Data management is an influential tool made all the more powerful due to the fact that its processing is not very well framed. A binding framework must therefore be put in place to ensure that

[34] French Council of State, report on "Puissance publique et plateformes numériques : accompagner l'ubérisation" (*"Public powers and digital platforms: accompanying uberisation"*). 2017 annual study.

the EU's democratic values are respected and to avoid that citizens are subject to any potential manipulation or control.

II - TOWARDS A EUROPEAN DIGITAL SOVEREIGNTY POLICY

A - Strengthen regulation of digital platforms EU-wide

In addition to regulatory measures such as the GDPR, regulations must be created in a more comprehensive manner, by creating a supervision framework based on compliance with community guidelines, by forcing platforms to exchange with stakeholders to set out collective rules for the management of the common goods that they generate, and by allowing for class actions in the case of non-compliance to complement the fines already issued by regulatory authorities. Competition law is therefore a temporary solution which would benefit from being completed. Furthermore, although this opinion only addresses the European aspects of digital technology, it is clear that many of the following recommendations could or should also be implemented at national level. This could be addressed by other works carried out by the ESEC.

1. Establish the conditions for fair competition on the European digital market

The European competition policy is based on combatting agreements and cartels as well as abuses of a dominant position and barriers to free competition (Article 102 TFEU): in this context, the European Commission has investigatory powers and, if it finds that an abuse of dominant position or practices affecting free competition have been committed, it can impose a fine of up to 10% of the company's turnover worldwide; it can also issue commitment decisions, where necessary with a legally binding nature, forcing the company in question to comply with the decision rendered and to bring its practices into compliance with EU competition law. The Google Search, GoogleShopping and Apple cases referred to above also constitute barriers to free competition which resulted in the European Commission imposing fines amounting to several billion euros (€13 billion for Apple for having benefitted from State aid in Ireland in the form of tax benefits[35]). These tools - proven to be effective - could be mobilised more widely by the European Commission under the supervision and the authority of the European Parliament, which would require that their resources be increased. These institutions could therefore increase the number of initiative investigations that they carry out, reduce

[35] Apple has started to pay this fine to Ireland but has appealed the Commission's decision to the European Court of Justice.

the length of a case's investigation and improve the effectiveness of their decisions by providing them with a legally binding nature on a more regular basis.

Recommendation no.1:

Further empower the European Commission, under the Parliament's supervision and authority, in tackling abuse of a dominant position and barriers to free competition and improve the effectiveness of sanctions adopted by making decisions legally binding.

According to European law, situations involving a monopoly or an oligopoly are only disputed in cases in which they prevent free competition or go against consumers' interests, but are not in themselves problematic. Outside of the security and defence markets and the markets restricted to operators with at least 30% of disabled or disadvantaged employees (Directive 2014/24/EU), there are no antitrust laws in Europe like those that exist in the United States, such as the *Buy American Act* or the *Small Business Act* which require that a proportion of purchases under public procurement contracts include American goods. This type of antitrust framework would also go against the positions that the EU has defended up until now within the World Trade Organisation (WTO). Furthermore, the digital sector is not a traditional activity sector as it implies the online provision of services, networking and is based on the exploitation and marketing of data: these aspects have not yet been addressed by the bilateral or multilateral trade negotiations involving the EU, even though the negotiations on the Trade in Services Agreement conducted by the WTO were suspended in 2016. Lastly, it seems unrealistic to restrict the power held by GAFAM by limiting their market share to the benefit of European stakeholders, especially in a context in which, without any credible European alternative, European digital stakeholders could be penalised as a result. The risk of reviving trade tensions with the United States, who up until the summer of 2018 had threatened to impose customs duties of 25% on European vehicle imports, should also be considered. In this context, the implementation of an antitrust policy could only work by resorting to safeguard measures, provided for in the EU's arsenal of trade defence instruments. These measures were initially designed to protect industrial sectors considered strategic and not activities based on the provision of services or intermediation, as such, impact studies must first be performed before these measures are extended.

Recommendation no. 2:

Have the European Commission carry out in-depth and documented studies on the European, national and international consequences of clauses introducing reserved contracts in some segments of digital economy.

Re-establishing fair competition also implies improving the tax treatment of major digital companies who must not be exempt from their social obligations towards other stakeholders. While digital giants have growth rates that are significantly higher than other EU economic operators, their low tax rates are an injustice which is widely criticised by a large proportion of European civil society. Although platforms' activities create new forms of value creation and renders the notion of permanent establishment and the system based on value added tax obsolete, they

can be assessed in a given country based on criteria such as the number of users and their turnover. The European Commission therefore proposed Council Directive COM(2018) 148 final of 21 March 2018 aiming to quickly introduce a temporary 3% tax on digital services applied to the proportion of revenues from the processing and use of users' data (placing of advertising online, sale of personal data, facilitating the interaction of users); a threshold of €750 million worldwide and of €50 million within the EU is set to determine which companies this tax applies to; the EU expects an income of €5 billion, with €500 million for France. In the longer term, the Commission suggests introducing "rules relating to corporate taxation of a significant digital presence" (Proposal for a Council Directive COM(2018) 147 final of 21 March 2018) in order to revise the notion of "permanent establishment" and the characteristics used to identify which companies are subject to tax, in order to take into account the evolutions generated by digital transformation; this second phase would fall within the framework of the Common Consolidated Corporate Tax Base (CCCTB) project. In any case, the implementation of such measures requires that a method to calculate the revenue generated by the exploitation of digital data be developed: for platforms operating on two-sided markets, this valuation could be determined by requiring that they provide users with an equivalent paying offer - in addition to the free service offer financed by the exploitation of personal data - ensuring that data is not stored.

Driven by France during the Council of Ministers of Finance and Economy of 6 November 2018, the proposal of a temporary tax on digital services did not receive the unanimous consent required for tax affairs: Germany objected, concerned about the United States hardened tone in trade affairs. Despite the United Kingdom having adopted, in October 2018, a tax on GAFAM's turnover which should reach 2% by 2020, the EU was forced to postpone the examination of this measure to the same 2020 deadline, planned for the completion of the works carried out under the OECD (*Base Erosion and Profit shifting system* project) - BEPS launched in 2012 to combat tax optimisation and avoidance strategies[36]). At European level, the ESEC can only regret that the euro zone's Council of Ministers of the Economy and Finance has postponed this important tax justice measure on the eve of the 2019 European elections, and in a context in which the next European budget will need to meet new challenges without increasing tax pressure on households; for this reason, it supports France's decision to introduce such a tax at national level. In the short term, in order to make progress at European level on this crucial topic, the ESEC also encourages the implementation of improved cooperation between

[36] Launched in 2012 by the G20 and implemented by the OECD, the BEPS project is comprised of fifteen actions aiming to provide governments with the means of countering tax optimisation. On 20 January 2019, the OECD announced that the international community had made important progress towards resolving the tax challenges arising from the digitalisation of the economy and "has agreed to continue working multilaterally towards achievement of a new consensus-based long-term solution in 2020". 127 States support this project.

favourable Member States, in particular Spain[37], Italy, France and Greece. Lastly, it supports the proposal made by the European Commission to include the topic of transitioning to a qualified majority for tax decisions in the Council's agenda.

Recommendation no. 3:

Step up efforts of persuasion and the forging of alliances at European and international level to pave the way towards the adoption of European Directives COM(2018) 147 and 148 and the adaptation of an international tax framework applicable to the digital sector as planned by the OECD's BEPS project by 2020. In the meantime, study the introduction of data tax at European level and engage in enhanced cooperation between the Member States for the introduction of a GAFAM tax on the revenue of digital platforms from the processing and use of users' data, similar to the tax already decided by France. A suitable tax threshold must be determined to avoid penalising start ups under development and medium-sized European stakeholders.

2. Take account of the social and environmental impact of digital platforms at EU level and within Member States

The development of collaborative platforms, facilitating interaction between natural or legal persons for the sale, lease or provision of goods and services has promoted the appearance of new forms of employment, particularly for those furthest from employment. Although the magnitude of these consequences is still difficult to assess without any precise and reliable data, many stakeholders have come together to criticise the situations of precariousness in which platforms such as Uber or Deliveroo place their works, weakening their social rights by promoting their individualisation and forcing us to rethink protection in order to guarantee collective rights.

As recalled by the ESEC in its opinion of November 2017 "*Les nouvelles formes de travail indépendant*" ("The new forms of independent work"), France responded to these situations by enhancing platforms social responsibility with regard to workers by the Act dated 8 August 2016 (Article 60) while the European Commission used discussions with European social partner organisations to suggest that these workers be included in the European Pillar of Social Rights in order to improve their social coverage, a step forward which should be solidified. The idea put forward by Jean-Claude Juncker in 2017 to create a joint labour authority charged with ensuring that labour rules are complied with[38] is a step in the same direction. Furthermore, the activity performed by platform workers generates

[37] The Spanish Council of Ministers approved plans for a GAFA tax on 18 January 2019, which should be debated in the Parliament. The Italian government announced the adopted of such a measure after the failure of negotiations among the 27 countries, without providing a timeframe.

[38] C. Stupp, Bruxelles promet une inspection du travail européenne (Brussels promises a European labour inspectorate). Euractiv.com, 2017.

marginal additional income in relation to the main income, which are currently not taxed in a uniform manner across the EU but according to national tax rules. With the rise of the economy based on sharing as a result of digital technology, the traditional borders between different statuses are being erased: we must therefore rethink the frameworks to protection and assist individuals in a world dominated by the plurality of activities and statuses. Digitalisation is therefore a significant challenge for our social security, unemployment insurance and retirement systems and more generally for the balance of social accounts.

Recommendation no. 4:

Have the European Commission (Directorate-General for Employment) publish a white paper across the EU on the impact of the activity of collaborative platforms on employment: new forms of labour, working conditions, social coverage, remuneration, relationship between workers and principals. Establish comparisons between countries in order to assess any potential disparities and any social dumping cases which may arise therefrom.

Recommendation no. 5:

At European level, effectively deliver on the integration of collaborative workers into the European Pillar of Social Rights by providing for suitable corporate statuses (e.g.: business and employment cooperatives, umbrella companies, collaborative service companies, microenterprises, etc.) adapted to the specificities of collaborative labour, in collaboration with social partners, and setting up a joint labour authority tasked with supervising, in liaison with the national authorities, compliance with the relevant regulations.

In its “appel à engagement, pour une convergence des transitions écologique et numérique” (“call for commitment, towards a convergence of ecological and digital transition”), in 2015, the Conseil National du Numérique (French Digital Council, CNN) underlined the risks inherent to the ecological footprint of digital tools and the abuses of an unsustainable digital sector; simultaneously, it highlighted the potential of digital technologies to accelerate the ecological transition in progress. By facilitating networking and the new collaboration, participation and mobilisation methods that these technologies create, they invite us to rethink current models to make them more sustainable and compliant with the principle of sustainable development principles. The digital sector’s contribution towards the development and management of the “commons” as defined by winner of the Nobel prize in Economics, Elinor Ostrom - which implies the coordinated management of goods or resources by users based on collectively-defined rules -, was highlighted by many researchers and by associations, who see it as an approach that promotes respect for the environment and for individual freedoms. The contribution of digital tools towards environmental transition is therefore a major issue which implies a new paradigm for the use of resources.

However, this new paradigm can only appear in favour of the improved dialogue with all stakeholders involved, whether citizens as users, public authorities, associations, the academic world; researchers and companies have a particular role

to play to develop innovative solutions such as materials reducing dependency on strategic metals and energy consumption, or data storage solutions that are more respectful of the environment. Public authorities will need to launch studies to improve available knowledge on the link between the digital and the ecological transition and raise stakeholders' awareness - through communication and information campaigns - on the unsustainable nature of certain digital practices, for example by reiterating simple consumption and usage rules (keep devices longer, turn devices off, use them less systematically) and by supporting associations in their advocacy work. They would also benefit from adjusting the financing granted by the EU to R&D projects based on environmental criteria. An a posteriori assessment of the consequences of innovations, in the form of discussions involving the different stakeholders, including citizens, should be the rule underlying these transitions.

Recommendation no. 6:

Implement national and European rules and standards, in collaboration with stakeholders, aimed at bringing about methods for producing, using and recycling digital tools that are likely to improve their length of service and put them to work for the benefit of the ecological transition, taking into account its social impact for a fair transition.

3. Guarantee compliance with the principles and values of the EU in the data economy as well as net neutrality

The GDPR confirms the vital principle of explicit consent in terms of personal data protection and sets out significant sanctions in the event of a breach, in order to ensure the effectiveness of the law: in France, the CNIL can be referred to for collective complaints and can issue fines of up to €20 million or 4% of the company's global turnover (the highest of the two is applied). However, the regulation allows any company to collect and use personal data if it has a legitimate interest and if such collection and use does not constitute a disproportionate breach of data subjects' interests; since 2014, the CNIL and its European counterparts have taken the stance of excluding behavioural analyses for the purpose of targeted advertising from the scope of "legitimate interest", which as a consequence should only be permitted with the user's consent.

In 2017, in order to protect the freedom of "explicit consent", the French CNIL was also led to specify, to Facebook and Whatsapp, that forfeiture of privacy protection cannot be a condition to access a service: this by application of the democratic principle which prevents the marketing of citizens' fundamental freedoms. However, as part of ongoing negotiations to revise the regulation on privacy and electronic communications (e-privacy), the risk that this principle could be brought into question has been underlined, with some versions of the project providing that the user must provide consent to access a service: while the independent authorities in charge of protecting public freedoms in Member States' digital universe, European public opinion (according to the Eurobarometer) and the European Parliament are opposed to this measure, it is important that France exercises all of its influence in Brussels to solidify the principles on which the GDPR is based during these negotiations. Furthermore, there are questions regarding the

current conditions under which platforms collect a user's free and explicit consent. Currently, this consent is gathered by agreeing to General Terms and Conditions of Use which are often complex, hard to read and are legally considered contractual provisions, generally under California law, without the European user being clearly informed. As part of the ongoing revision of the e-privacy regulation, the EU would benefit from strengthening the requirement for free and informed consent set out by the GDPR, by limiting restrictions of access to the service in the event consent is refused and by clarifying how users can find out about their rights and express their consent.

Recommendation no. 7:

As part of the ongoing revision of the Regulation on Privacy and Electronic Communications (e-privacy), strengthen the principle of free and explicit consent by users concerning the collection and use of their personal data by limiting restrictions of access to the service in the event consent is refused. In this context, specific protection must be provided for highly sensitive data such as health data, and the creation of a European civil society stakeholders - a *DataWatch* - should be encouraged to defend an emancipatory European data use model.

With the development of the data-driven economy, the diversification of uses and the growing role of digital technology in all aspects of social life, platforms' accountability in respect of their users is a critical issue. This topic is comprised of two requirements: on the one hand, it requires that the scope of the operators involved is legally set out; and, on the other, it implies that the nature of their accountability, particularly as regards net neutrality, is specified. As regards the first requirement, it should be noted that European regulations in force (e-commerce directive of 2000) differentiates between two statuses with different responsibilities: the "host", a passive technical intermediary that is merely an interface between the user and the content hosted, without any influence over the latter or on its presentation; and the "publisher", who plays an active role and is at the source of the content disseminated on its website. While major platforms such as Google or Facebook are now qualified as hosts, it is clear that this definition does not match their true role: by hierarchising content using algorithms, these platforms are not neutral as regards the dissemination of such content, although they are not necessarily at the source of the content either.

A new type of hybrid status must therefore be created for the EU to be able to subject these operators to obligations in terms of content regulation and neutrality, and particularly algorithmic neutrality. According to the ESEC, this European status must be applied in a broad manner, including all of the current entryways to the Internet (social networks, search engines) and must be flexible enough to adapt to rapid evolutions; it must also apply to devices for their relationships with digital applications. This status could draw inspiration from the definition of online platforms introduced in France by the 2016 Act for a Digital Republic, which identifies them as "*any natural or legal person offering an online communication service to the public as a professional, whether free of charge or against payment, based on the listing or referencing of content, goods or services offered or published online by third parties, using computer algorithms, or putting several parties in contact for the purposes of*

the sale of a good, the provision of a service or the exchange or sharing of content, goods or services".

The responsibilities tied to how platforms operate under this status could therefore be detailed in order to reconcile the many requirements arising from their activities. For users, the principle of net neutrality is a guarantee of impartiality in the exercise of their freedom of expression and their right to information; in P2B relationships, it helps to protect companies who use platforms' intermediation services (listing, referencing, etc.) against the risk of unilateral measures which would deny them commercial visibility or arbitrarily increase their costs. While the EU - unlike the United States - armed itself with a regulation "on the Open Internet" in 2014, which rigorously accepts net neutrality and this principle with a legal scope, it is important to protect this asset against the recurrent attacks which are attempting to justify the increasingly frequent derogations to the principle of neutrality under the pretext that the innovations in progress - such as 5G and autonomous cars - will consume an increasing amount of the Internet's bandwidth. For the ESEC, on the contrary, the 2014 regulation offers a suitable framework for the implementation of such services, by ensuring that no discrimination can be made between different service providers and by protecting the bandwidth granted.

Recommendation no. 8:

As part of the revision of the European Directive on e-commerce, strengthen the legal regime for the accountability of platforms by providing them with a unique status, inspired by the status set out by the 2016 Act for a Digital Republic, and by introducing a trusted third party to reassure all users. This status must include a set of basic common security rules, the possibility of challenging and referring to the courts, compliance with social and consumer protection standards, civil liability insurance and a tax system based on the turnover achieved in the country in which the service is provided.

As important as it may be, net neutrality must take into account additional requirements, particularly as concerns the protection of users and the fight against illegal content. In this respect, it is normal that hosts are not exonerated from all controls on the content published online. However, the provisions which delegate the filtering of content to platform algorithms appear to be of a nature to hinder the development of Europe's digital economy in that it is likely that only major platforms would have the resources to comply with these obligations. As a result, they could result in the abandonment of sovereign surveillance and censure powers to a handful of hegemonic private stakeholders. Furthermore, experience shows that algorithmic filtering tools are fallible and potentially biased for marketing or political purposes; by ignoring the subtleties of human behaviour, these tools neutralise the legitimate exercise of exceptions to copyright and to the freedom of expression. Thus, since 2012, the Court of Justice of the European Union (CJEU) considers that platforms' obligation to actively monitor content is a breach of European citizens' right to privacy and to freedom of information, as recognised by the Charter of Fundamental Rights of the European Union (CJEU, SABAM v. Netlog, 16 February 2012). Lastly, such requirements would only increase the ongoing delocalisation of the moderation of content from third party States, where it is moderated under degraded wage conditions by employees sometimes working under inhumane conditions. Conversely, for the fight against illegal content and misleading information, as for copyright protection[39], it seems preferable to defend net neutrality by banning the use of filtering algorithms a priori and by setting out a framework for hierarchisation algorithms which tend to highlight anxiety-inducing, controversial or violent information with a view to increasing the website's traffic. The supervision of ranking algorithms could therefore be entrusted to an independent European authority, with the status of Executive EU agency and with the necessary policing powers and tools, and particularly the necessary testing abilities to determine the impact of any potential breaches of the principle of neutrality which are outside of

[39] The question of the consideration of copyright in the digital economy does not fall within the perimeter of this opinion.

the reach of association stakeholders; this authority could be afforded powers to issue sanctions and refer to the CJEU in the event of discriminatory practices.

Recommendation no. 9:

Reassert the principle of net neutrality: strict impartiality in network access as provided for by the Regulation on Open Internet, and a framework for content ranking algorithms under the control of an independent authority, which could be referred to for individual and collective complaints and bring them before the Court of Justice of the European Union (CJEU).

B - Set the stage for a digital "ecosystem" in line with the principles and values of the EU

1. Lay the groundwork conducive to an open digital "ecosystem" in Europe

The introduction of a regulatory framework conducive to the development of an open European digital universe first implies finalising the digital single market by reducing the disparities that currently exist with a view to providing digital companies on the pan-European market with the tools they need to develop and provide them with the ability to benefit from the effects of the network on which their economic model is based: in 2015, the European Parliament this considered that the digital single market - the leading digital market worldwide - could contribute €415 billion euros to Europe's economy. In this respect, two improvements are crucial: the elimination of obstacles to the development of the e-commerce of goods and services in the EU and the development of online administration. These improvements could be implemented whilst maintaining the vital physical presence of local public services, which guarantee that citizens' general interest and equal rights are respected across the territory. While, in 2016, cross-border online commerce represented around €510 billion, i.e. a +12% increase compared with 2015 according to e-commerce News 2016, its growth has been stunted by regulations that are too complex and not sufficiently uniform across all Member States - this is said to be the raison for European consumers' loss in purchasing power, estimated by the European Commission at around €11.7 billion per year[40]. Rules relating to the rights and obligations of parties to a sales agreement (possible means of action in case of non-performance, legal warranty periods) could also be harmonised to enable European e-commerce companies to invoke their national law, based on a common core of imperative contractual rights in the EU.

[40] European Commission, the Single Market Strategy. Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2015.

The EU would also benefit from developing enhanced means to apply and monitor this regulation, on the one hand by encouraging Member States to extend the powers granted to national authorities in charge of consumer protection, and on the other hand by improving cooperation between these authorities, particularly through European bodies such as BEREC. This body could see its prerogatives extended so as to become a true regulatory public authority at Europe level, with the task of monitoring digital technologies in Europe - based on the platform observatory model imagined by Mariya Gabriel, the European Commissioner for Digital Economy and Society -, the scoring and accreditation of platforms - based on ethical, social, and environmental criteria and on compliance with best practices -, the collection of data from such platforms - including by force, with a view to sharing such data with users (researchers, *start-ups*, the general public depending on the case) -, and an advisory role to Member States and European institutions[41].

The proper operation of the European digital market also implies that interoperability be developed in Europe in order to ensure effective communication between digital components such as devices, networks or data repositories, and between stakeholders, i.e. user communities, actors from the industry and Member States' public authorities. This also requires that the digital technology normalisation process be accelerated at EU level: while laws are now often established outside of the EU under the influence of industrial actors, at the risk of weakening Europe's industrial competitiveness, this would provide the Union with the ability to identify technological laws which is considers essential for the digital transition of its industry and services. This means that the EU must step up the adjustment of its rolling plan to normalise information and communication technologies in order to bring it in line with technological evolutions, and that it must launch an integrated standardisation plan which would set out the main priorities in this field, by highlighting the technology and industrial sectors that are considered crucial for Europe. The creation of common European standards could also facilitate the development of high-capacity networks and therefore help to reduce the digital divide in Europe, a factor that generates exclusions which go against the principle of equal treatment. In this respect, the creation of common 5G standards, the continuation of adjustments to the European Electronic Communications Code and the adoption of the European Commission's legislative proposal on promoting Internet connectivity in local communities and public spaces ("WiFi for EU") - which require a revision of Directive 2002/22/EC on Universal Service - should be made priorities.

[41] Mariya Gabriel, A digital Europe: continuing efforts! Politique internationale no. 160, 2018.

Recommendation no. 10:

Harmonise regulations applicable to cross-border e-commerce by reforming regulations bearing on electronic telecommunications and connectivity, by launching an integrated plan to standardise digital technologies, and strengthen the resources and competences of the Body of the European Regulators of Electronic Communications (BEREC).

Improving cybersecurity on the digital single market thus established must be a priority. With this in mind, the EU will benefit from developing cooperation between competent national authorities in terms of data protection and cybersecurity (in France, the Autorité de régulation des communications électroniques et des postes - Electronic Communications and Postal services Regulatory Authority, ARCEP -, the Agence nationale de la sécurité des systèmes d'information - the French network and information security agency, ANSSI -, and justice and intelligence services), particularly through information and awareness-raising campaigns targeting these stakeholders and relating to topics such as the prevention of electoral interference and the fight against *fake news*. The UE will also need to strengthen its own cooperation and monitoring bodies: the European Data Protection Board (EDPB), charged with providing guidance and suggesting standardisation between Member States; and the European Union Agency for Cybersecurity (ENISA), which, since 2004, has supported the EU and its Member States in their efforts to improve protection systems, by promoting cooperation between States, the development of capabilities and the provision of expertise.

Promoting cybersecurity competitivity and innovation is also key to improve results in this area. This objective is placed at the centre of the missions carried out by the European Cyber Security Organisation (ESCO), which was created in 2016 to improve the sharing of knowledge and best practices, to develop research and innovation projects and to explore new trade opportunities to the benefit of its 230 members from all segments of the cybersecurity market. The EU will also need to increase its public investments in the framework of this organisation. Cybersecurity innovation could also be supported by including specifications on this topic in public tenders.

To strengthen cybersecurity on the digital single market, the EU must also develop cooperation on the international regulation of cyberspace, in a multilateral context, with third party States with which it entertains strategic partnerships, and especially the United States and the United Kingdom after Brexit. The *Global Commission on the Stability of Cyberspace*, which brings all stakeholders together, including those from the private sector and the academic community, could be an appropriate forum to promote cybersecurity cooperation processes, confidence-building measures between States and the control and repression of cybercrime on an international scale. Common standards, such as those aiming to make the public core of internet safer suggested by France in November 2017, or the Tallin manual adopted in 2013 by NATO in order to apply international law to cyber conflicts, or even the Geneva Convention on cyberspace proposed in February 2017 by Microsoft, could be discussed within this forum. The ILO is another forum that should address this topic, in order to establish a new international law, on a tripartite

basis, with a view to ensuring respect for workers' fundamental rights and social justice.

Recommendation no. 11:

Improve cybersecurity cooperation between Member States, the EU and its strategic partners, not only between public authorities but also between all stakeholders (companies, social partners, academic community, users). Refer to the ILO on this topic in order to establish a new international law, on a tripartite basis, whilst respecting workers' fundamental rights.

2. Support the development of a digital Europe

The implementation of a framework promoting a digital Europe also means combatting the digital divide, which is a source of exclusions and unequal treatment between companies, citizens and territories. As a result, investing in very high-speed connection infrastructures such as fibre optic networks and next generation mobile networks (4G and soon 5G), particularly in areas that do not receive good service, must be encouraged. The European Commission's strategy on high-speed broadband, which it adopted in 2016, will need to be updated and its implementation should be accelerated in order to reach the objective of providing a high-speed gigabit connection to all public service providers (schools, universities, research centres, transport hubs, hospitals, administrations) and to all European urban and rural households, and of providing uninterrupted 5G coverage to all urban areas and major roads and railways by 2025. A universal right to access a minimum broadband speed must be introduced in order to promote the extension of coverage. The financing tools serving this strategy must be strengthened, in particular by further mobilising European Structural and Investment Funds (ESIF) which are currently under-exploited, and in particular the European Regional Development Fund (ERDF), as underlined by the ESEC in its opinion on "the reform of European structural funds" ("*la réforme des fonds structurels européens*") dated June 2018. The Fund for high-speed broadband infrastructures, announced by the European Commission and the European Investment Bank (EIB) as part of the European Fund for Strategic Investments (EFSI) and whose task would be to invest in underserved areas should also be implemented without delay and its public fund allocations should be revised upwards, which would require increasing the importance afforded to the digital sector in the Multiannual Financial Framework (MFF) for 2021 - 2027.

Recommendation no. 12:

Accelerate the roll-out of high-speed broadband coverage across Europe through fibre optic networks and next generation mobile networks by establishing a universal right to a minimum level of megabits and unlocking European public resources.

The development of a digital Europe in a context dominated by American platforms calls for a strategy to accelerate the integration of digital technologies by European companies that are active within the EU's sectors of excellence. This approach would improve the competitiveness of key industrial sectors and keep jobs in Europe, even potentially creating new ones: experts estimate that the gain in

revenue that should be expected from the digitalisation of European industry at around €110 billion over the next five years[42]. The main focuses of this strategy should be as follows:

- at EU level, improving coordination and the sharing of experience as regards national and regional, public and private initiatives, to digitalise companies. The EU would therefore benefit from creating greater consistency in the strategies and action plans that is has set out for itself to strengthen companies' overall competitiveness, particularly for SMEs: Investment Plan for Europe, Single Market strategy, Capital markets union, Energy markets union, etc. It must also ensure that it regularly brings stakeholders together under the aegis of the European Commission;
- setting up Digital Innovation Hubs (DIH) in all areas of Europe. Inspired by the digital skills centres created in many European cities and regions from university laboratories, research and technology organisations (e.g. Catapult in the United Kingdom, Smart Industry field laboratories in the Netherlands) and start up incubators (e.g. the Start-Up Europe or FIWARE initiatives), these centres aim to generate a wave of ascending digital innovation affecting all activity sectors. By promoting collaboration between companies and universities from one end of the chain to the other and by enabling the development of test facilities and experimental digital innovation, these centres will aim to provide each European company with access to the latest digital technology, enable the creation of a one-stop shop for the most recent technology, accessible to each company through a network of DIHs on a smart thematic specialisation platform, and facilitate said companies' access to funding by providing them with technical assistance (and particularly SMEs) and by creating a Euro Tech label inspired by the French Tech model in France;
- increasing the public and private financial resources afforded to the digitalisation of the economy, under public supervision. For public resources, the proportion of the MFF 2021-2027 dedicated to the digital sector must be boosted by increasing allocations for the Digital Europe programme; by concentrating and further mobilising the ESIF - and particularly the aspects relating to SMEs - to improve the financing of DIHs, which the European Commission estimates will need to reach around $1 billion by 2020; by making further use of the EFSI, which serves to finance digital projects with an important research and innovation aspect and therefore which are high-risk; and lastly, by increasing the proportion of the Horizon 2020 and Horizon Europe (2021-2027) research programmes allocated to DIHs. These partnerships, which involve the entire value chain, from its components to its applications, could become real "ecosystems" for young digital companies

[42] European Commission, Digitising European Industry. Reaping the full benefits of a Digital Single Market. Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, 2016.

and could become crucial to implement digital strategies at EU level, to ensure closer ties between Research and Development (R&D) and standardisation, and to promote the use of all available financial instruments. Financing needs for the next few years are evaluated at close to €1 million per year for the EU's research programmes, in addition to the €3 million per year provided by Member States and an equivalent amount invested by companies[43]. The mobilisation of private financing, in private equity and venture capital, could also be encouraged at the same time by creating an environment conducive to the harmonisation of the status of companies across the EU, and a more qualitative venture capital system capable of ensuring the improved management of costs and related legal risks. An enticing framework, inspired by the research tax credit or the Young Innovative Company tax credit introduced in France, although better targeted and framed, could be implemented at European level; for optimal efficiency, this framework should be extended to all innovative companies based on a young European company status corresponding to the Euro Tech label and must be accessible through the one-stop shop referred to above.

Recommendation no. 13:

Improve young European companies' access to digital technology by creating a Euro Tech label, a European one-stop shop, as part of the European network of Digital Innovation Hubs, and a financial incentive similar to the research tax credit - only better targeted and better regulated - or to the Young Innovative Companies tax credit.

Both supporting digital companies and reducing the digital divide require special efforts to promote digital skills and qualifications in Europe, with a view to reducing the disparities that are still present in this field. These efforts must first focus on workers and job seekers to ensure a fair transition: in fact, the European Commission considers that over 800,000 jobs may not be filled by 2020 due to delays in this respect[44]. In order to improve the level of digital skills in the EU, Member States and European regions must be encouraged to improve their digital technology training offers at all education and vocational training levels. A real public policy on digital training and vocational skills must be implemented as from initial education and training by public services in order to ensure that all citizens have access to equal opportunities and career progression. In this respect, stakeholders may rely on the content and programmes provided to them by the European Commission as well as on training frameworks, such as Erasmus Intern, financed

[43] European Commission, Digitising European Industry. Reaping the full benefits of a Digital Single Market. Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, 2016.

[44] European Commission, the Single Market Strategy. Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2015.

by the latter; the role played by sandwich courses could also be enhanced as regards digital training, by establishing partnerships between companies and educational bodies. Improving digital training must go hand in hand with the development of complementary skills in the field of unionism, employee representation, entrepreneurship, management or engineering, as future jobs will require an appropriate combination of basic, technical, non-technical and specialised skills adapted to the activity sector. Improving the recognition of qualifications and skills, based on a common European pillar of digital qualifications and skills which is yet to be defined, and including "humanities", would also improve the overall level. The EU must further the works launched towards this goal, such as the European Digital Competence Framework[45] and the European Reference Framework to improve companies' digital transformation abilities (Digiframe)[46]. This would allow it to improve the instruments used by its policy to encourage the guidance of youths towards science and technology, and particularly women who are still underrepresented in this field, for example by drawing inspiration from the tools developed by States such as Israel, which, within 10 years, was able to triple the amount of vocations in these fields.

Lastly, the development of basic digital skills must be an objective for the entire European population: in its 2015 opinion on "Digital data, a challenge in terms of education and citizenship", the ESEC had already recommended promoting digital education at all stages of life to counter the digital divide and to raise awareness on best practices. Digital education for all, at all ages, is vital to provide each citizen with the means of moving freely and safely in the digital sphere. At European level, specific ERDF and ESF credit lines could be created to support associations' initiatives towards combatting the digital divide and to assist citizens with digital uses and challenges: restoring a European digital sovereignty also involves providing individuals with complete knowledge on issues relating to data and allowing them to fully exercise their digital citizenship.

[45] http://www.ecompetences.eu/
[46] http://ictprofessionalism.eu/

Recommendation no. 14:

Determine basic digital skills and competences which will constitute a European Common Pillar and, on this basis, improve the digital technology training offer accessible to workers, job seekers and the general public. With this in mind, mobilise the European Structural and Investment Funds (ESIF) for associations, whose role in assisting populations most distanced from digital uses and in raising the awareness of young women on digital occupations must be supported.

3. Invest in alternative technological solutions capable of solidifying the EU's position

In the medium term, the EU will need to bet on alternative technologies capable of providing it with a comparable advantage when competing with American and Asian platforms. In order to develop world-class abilities in terms of transmitting, storing and processing data, similar to those possessed by major actors such as the United States, China or Japan, it must first accelerate the implementation of the cloud computing initiative (European cloud) that it adopted in 2016[47]. Such abilities are crucial not only for the European research community - who are therefore spared from having to process big data outside of Europe - but also for companies who will access these technologies at a lesser cost. Reaching this objective means developing further transparency and control before strengthening the public/private partnership on big data, which is currently allocated €2.7 million in funds. This partnership could be strengthened by using the EU's research programmes, the Connecting Europe Facility (€3 billion), the Euro High Performance Calculation initiative (HPC: €1 billion) and national credits to finance both the open platforms which contribute towards the adoption of data-based economic models that are more innovative and competitive by European companies - and particularly SMEs -, and computing facilities. The European Commission's ambition to acquire next-generation supercomputer by 2023, and the aim of developing quantum technology, should be stepped up to position Europe among the three leading global actors in the field of high-performance computing[48].

[47] G. Babinet, Pour garder sa souveraineté, l'Europe doit créer des "clusters de data" (To retain its sovereignty, Europe must create 'data clusters'). Capital Finance no. 1342, 2018.

[48] European Commission, Digitising European Industry. Reaping the full benefits of a Digital Single Market. Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, 2016.

Recommendation no. 15:

Speed up implementation of the European Cloud Initiative, acquisition of next-generation high-performance computers and development of quantum technology in order to make the EU a major actor in the data-driven economy by 2020.

Enhanced abilities in terms of cloud computing and high-performance computing will enable the EU to develop artificial intelligence technologies by accelerating the implementation of the road map presented by the European Commission on 25 April 2018 on this topic. The aim is to support the development of a European artificial intelligence model, based on ethical values that are in line with the EU's values. This should involve[49]:

- the definition of a cross-disciplinary strategy involving all links in the chain (infrastructures and equipment, R&D, SME transformation, training) and by coordinating the various national strategies on artificial intelligence - France and United Kingdom have both adopted such strategies, Spain and the Netherlands are in the process of preparing theirs. This European framework must be flexible and capable of supporting national strategies without stifling them with excessive centralisation. The team comprised of France and Germany could play a driving role, as suggested by the adoption of the Meseberg declaration on 19 June 2018 which provides for the creation of a Franco-German research centre on artificial intelligence;
- the definition of an ethical and legal context capable of ensuring the dissemination of "positive" artificial intelligence which takes account of the most sensitive users and which respects fundamental European principles, particularly as regards data protection, the reasonable circulation of such data, transparency and openness. This framework must be binding and drafted in collaboration with the ILO with a view to taking into account the impact of artificial intelligence on workers' fundamental rights and on social justice. This framework must be proposed by the European Commission based on the guidelines referred to above and could include the issue of the legal status afforded to robots, which is currently being discussed by the European Parliament and the Council;
- further support for research on artificial intelligence, promoting an inter-disciplinary approach within multi-disciplinary institutes like those launched in France. These European artificial intelligence research centres, spread across the various Member States, would benefit from being included in a European network, similar to existing initiatives such as the Confederation of Laboratories for Artificial Intelligence in Europe (CLAIRE); they will encourage the development of ambitious and collaborative projects at EU

[49] N. Boujemaa, Intelligence artificielle: pour une souveraineté de l'Europe ("Artifical Intelligence: towards European sovereignty"). Le Monde, 7 November 2018.

level, which the *Joint European Disruptive Initiative* (JEDI) is an excellent example of today. The European Commission estimates that the funds necessary to development these initiatives will be of around €20 billion by 2020; this can be compared to the €200 billion planned by the United States to develop artificial intelligence technologies in the coming years. This budget could be financed by mobilising European programmes (€1.5 billion have been provided for as part of the Horizon 2020 programme, an amount which should be higher for the Horizon Europe programme) and national programmes (€1.5 billion euros have been planned by France following Cédric Villani's report on artificial intelligence); under public supervision, this could also involve increasing recourse to private resources by implementing development sponsorship initiatives to serve research and training on artificial intelligence technologies. The effective implementation of the European Agency for breakthrough innovation, discussed by the European Commission, would contribute towards these efforts;

- support for innovation and the roll-out of artificial intelligence to all sectors of European economy. Artificial intelligence could therefore contribute towards a European agriculture that is less focused on production and more human. By promoting the transformation of key industry sectors (health, mobility, construction, agri-food, etc.) and services, the EU could stimulate the development of an artificial intelligence which matches its values and provides its economy with a real competitive advantage. This requires that platforms dedicated to digitalising industry - based on the French "Future industry" model or the German "Industry 4.0" model - and services are set up in Member States. Such platforms, which would come together to constitute a mega-platform at European level, would facilitate artificial intelligence experiments. The EFSI could be mobilised, providing at least €500 million to help SMEs and start-ups to start on this path[50].

In particular, applying artificial intelligence to industry could provide the EU with a leading role in the development of the Internet of Things (IoT), a niche position which would allow it to separate itself from the less-specialised GAFAM. Given the privacy risks that are inherent to the collection of personal data by connected devices, the European Commission will need to specify which technological standards are necessary to develop the IoT and clarify the binding regulations relating to the distribution of accountability in this field, in order to provide actors with legal security, under public supervision. Standardised grammar allowing to define the properties of connected devices, in a way that is easily understandable to the general public, and setting out standards in this field could be developed; the Alliance for the Internet of Things Innovation, which is comprised of the majority of

[50] European Commission, Digitising European Industry. Reaping the full benefits of a Digital Single Market. Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, 2016.

the stakeholders involved, could be useful in this respect. The European Commission could also invest in wide-scale pilot projects and in flagship initiatives based on demand, in fields such as autonomous cars (roll-out of test facilities), mobile health (med tech), agri-food or energy (smart meters and thermostats such as the French Net Athmo), by financing open inter-sectoral platforms capable of accelerating corporate innovation[51].

Recommendation no. 16:

Adopt an "artificial intelligence and disruptive technology" package by 2020 for which implementation will be entrusted to a European Agency for Disruptive Innovation financed by the European budget. This package will include an artificial intelligence deployment strategy at EU level, accompanied by an action plan and a regulatory framework consistent with the ILO's fundamental standards, which is conducive to ethical use of this technology.

In addition to specific applications or technology, and given the dominant positions held by non-member states, the EU will benefit from developing a plural system culture and from promoting the diversity of the digital world in order to protect actors' freedom of choice. Faced with an American digital model based on the capitalistic and technological market and concentration, and a Chinese model based on close control and surveillance of the net by authorities, it would also benefit from promoting the common goods model - that of a technological and legal pillar based on rules established jointly - under public supervision. To reach this objective, the EU will need to:

- develop independent infrastructures and its own binding regulations, in line with the ILO's fundamental standards, and its own rules and standards as set out above, in order to avoid being forced to adopt the rules and standards set out by American or Chinese operators;
- base its innovation on blockchain technology[52], which allows the development of decentralised systems and is therefore structurally difficult to hack, rather than on the global web. Here again, the EU must set out basic regulations to develop the use of blockchains and to prevent any fraudulent use, particularly in terms of taxation, accounting treatment, and the fight against money laundering; finance the development of secure blockchain infrastructures whilst managing their environmental impact; and lastly, support the application of this technology to fields of excellence or fields of strategic interest to the EU[53];

[51] J. Chrétien, Intelligence artificielle: bâtir la voie européenne (Artificial intelligence: setting out a European path). Strategic note EU Digital Challenges, 2018.

[52] The Blockchain technique allows the transmission of information - grouped into "block chains", with a high level of security using encryption methods and transmission protocols.

[53] J. Toledano, report on "Blockchain challenges" ("*Les enjeux des blockchains*"). France Stratégie, 2018.

- increase recourse to open source software, with an accessible and auditable source code: the Open Street Map software, used by the departments of the French Republic's presidency to organise presidential trips, the Wikipedia platform, which alone drains over one third of the 300 million daily Google Search requests, or the secure E-mail service Proton are all examples of such open resources, written in open source outside of companies and institutions and which are real common goods operators. A policy supporting the development of these resources could include the implementation of cooperatives bringing together several small developers, so as to reduce the imbalance in power that exists in respect of the GAFAM; it could also set out the requirement for a proportion of open-source software in responses to public tenders. Financial support may be provided at European, national and regional level to projects aiming to develop alternative solutions based on open-source software for services considered of a general interest (geolocation, educational and cultural content, the promotion of regions and heritage, etc.).

Recommendation no. 17:

Establish fundamental regulations governing the use of blockchains and free software in Europe and support their development by setting up developer cooperatives, introducing quotas in public tendering processes and financing projects meeting collective needs at local level. Regulations must allow the appearance of types of governance that are not energy consuming and that are open to civil society and ensure the interoperability and neutrality of the solutions proposed.

ESEC'S OPINION