January 2017

DIGITAL SOVEREIGNTY

Farid GUEHAM

FONDATION POUR L'INNOVATION POLITIQUE
fondapol.org

FONDATION POUR
L'INNOVATION
POLITIQUE
fondapol.org

DIGITAL SOVEREIGNTY – STEPS TOWARDS A NEW SYSTEM OF INTERNET GOVERNANCE

Farid GUEHAM

Translated from French by Caroline Lorriaux and Michael Scott.

FONDATION POUR
L'INNOVATION
POLITIQUE
fondapol.org

The Fondation pour l'innovation politique
is a French think tank for European integration and free economy.

Chair: Nicolas Bazire
Vice-chair: Grégoire Chertok
Executive Director: Dominique Reynié
Chair of Scientific and Evaluation Board: Laurence Parisot

The Fondation pour l'innovation politique is publishing this paper
as part of its work on *digital*.

FONDATION POUR L'INNOVATION POLITIQUE

A French think tank for European integration and free economy

The Fondation pour l'innovation politique provides an independent forum for expertise, opinion and exchange aimed at producing and disseminating ideas and proposals. It contributes to pluralism of thought and the renewal of public discussion from a free market, forward-thinking and European perspective. Four main priorities guide the Foundation's work: economic growth, the environment, values and digital technology.

The website **www.fondapol.org** provides public access to all the Foundation's work. Anyone can access and use all the data gathered for the various surveys via the platform «Data.fondapol» and data relating to international surveys is available in several languages.

In addition, our blog "Trop Libre" (Too Free) casts a critical eye over the news and the world of ideas. "Trop Libre" also provides extensive monitoring of the effects of the digital revolution on political, economic and social practices in its "Renaissance numérique" (Digital Renaissance) section (formerly "Politique 2.0").

The Fondation pour l'innovation politique is a state-recognized organization. It is independent and receives no financial contribution from any political party. Its funding comes from both public and private sources. Backing from business and individuals is essential for it to develop its work.

SUMMARY

Just how omnipotent will GAFA become in terms of accessing and processing our personal data? The convenience of voluntary servitude comes at a price – the exposure of our habits, purchasing and health.
Since the Wikileaks revelations, the commodity of data has become a resource coveted and envied by governments and companies. A new ecosystem has sprung up in response to the unbridled race for this prized commodity pitting the 'circles' of citizen, government and corporate sovereignty against one other. Is anyone capable of imparting a message of individual freedom without hitting a wall of powerful multinationals?
At a time when the European Union is refining its data protection policy, the rules of a fledgling system of governance are being shaped every day by a new balance of power. The issue of personal data protection, a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, both in and outside of European territory, has refocused attention on the urgent need to define an international framework of sovereignties.
With the European Commission's recognition of the Privacy Shield on 12 July 2016 and the Safe Harbour framework pledging equivalent protection of data outside the European area, a new system is emerging in a fierce and competitive environment reflecting the sudden yet necessary realisation that the age of the Internet with its innate freedoms has come to an end.

DIGITAL SOVEREIGNTY – STEPS TOWARDS A NEW SYSTEM OF INTERNET GOVERNANCE

Farid GUEHAM

Public sector consultant and contributor to the Fondation pour l'innovation politique on digital issues and innovation

The concept of 'digital sovereignty' arose in the early 2000s. Pierre Bellanger, the CEO of French radio station Skyrock, made an initial attempt to define it in 2011: 'Digital sovereignty is control of our present and destiny as manifested and guided by the use of technology and computer networks[1].' The quest for digital sovereignty is therefore a goal shared by companies, public authority stakeholders and, more recently, Internet users, citizens and consumers. At the consultations of the French National Digital Council of 2014, several proposals emphasised the critical role played by strong digital sovereignty in national sovereignty[2]. Faced with the ever increasing economic influence of GAFA (Google, Apple, Facebook and Amazon)[3], economic dependence and significant value transfer are feeding an imbalance which requires public authorities and economic operators to implement regulatory tools that are compatible with free movement and freedom, which are inseparable from our online practices.

* * *

1. Pierre Bellanger, 'De la souveraineté en général et de la souveraineté numérique en particulier' [Sovereignty in general and digital sovereignty in particular], Les Échos, 30 August 2011. ***LINK***.

2. Nicolas Colin and Henri Verdier, 'Souveraineté numérique : la piste industrielle' [Digital sovereignty – the industrial path], paristechreview.com, 30 June 2014. ***LINK***.

3. See 'Les géants du Web menacent-ils la souveraineté des États ?' [Are the giants of the web threatening State sovereignty?], a video from the forum 'Qui gouverne Internet ?' [Who governs the Internet?] organised by the newspaper Libération on 21 May 2016. ***LINK***.

GAFA has collectively made us accustomed to voluntarily waiving our rights regarding personal data. In return for relinquishing these rights, we receive a first-rate service at the cost of an alarming degree of vagueness regarding the future of our personal data. Consumers or users of services have grown used to waiving their rights without truly understanding the implications and repercussions of their actions for their personal data. This pattern of behaviour is gradually being replaced by a less automatic response. Some companies have taken stock of these changing attitudes and adapted their services, eager to retain the trust of consumers wishing to regain control of their data.

A Harris Interactive survey from March 2016 revealed that although two thirds of French people expect companies to offer them more tailored services, only a third are prepared entrust these companies with their personal data to achieve that end: "Ultimately, against the current backdrop of fragmented information, which often correlates with an attitude of mistrust or even rejection of big data, only 15% of French people consider big data as an opportunity for consumers due to its ability to better identify their requirements, while 81% believe that it puts consumers at risk of being 'tracked' " [4].

Faced with such mistrust from users/consumers, companies are committing[5] to more ethical and virtuous practices, notably by implementing privacy policies in order to meet new requirements in terms of confidentiality, transparency, support and security of data processing. Ethical data processing poses a challenge in terms of sovereignty, requiring the introduction of an appropriate legal framework, as reflected by changes in European laws[6], which already offer some of the best protection worldwide with regard to these issues.

As far as governments are concerned, the battle for data sovereignty is well under way and campaigns are conducted with varying degrees of success. In 2009, the French government funded two sovereign cloud projects, Cloudwatt and Numergy, which emerged from the Andromède programme. New companies were set up, which, in the case of Numergy, were supported by SFR and Bull, while Cloudwatt was forged from a partnership between Orange and Thales[7]. Their goal was to provide companies and the French authorities with remotely accessible and secure computing infrastructure capable of hosting data and applications. However, due to a lack of cooperation between

4. "'Big Data', qu'en pensent les Français ?" [What do French people think about big data], a Harris Interactive survey, March 2016. ***LINK***.

5. Quentin Ebrard, 'Le data, le nouveau "dada" des entreprises' [Data – companies' new 'dada'], lemonde.fr, 17 June 2016. ***LINK***

6. French Institute of Digital Sovereignty, 'Les nouveaux enjeux européens de la souveraineté numérique' [New European issues regarding digital sovereignty], *Cahiers de la souveraineté numérique*, n° 1, 2015. ***LINK***.

7. Sandrine Cassini, 'Cloud souverain, un gâchis à la française' [Sovereign cloud – a French shambles], lesechos.fr, 24 February 2015. ***LINK***.

manufacturers, the two entities were unable to achieve the initial goal of a 'sovereign cloud' despite the government's insistence on supporting a project with an unclear roadmap. This attempt is a clear illustration that innovation and competitiveness cannot be decreed and must be planned and prepared.
Companies have taken this on board and consequently adapted their services and internal structure. This is particularly true of those whose business relies on data processing, the cornerstone against which the concepts of sovereignty and trust rest. So how can this rationale of data capture by companies or governments be neutralised without balkanising a network whose very essence lies in the free movement of information? The protection of citizens' rights and confidentiality of consumers' information is at stake. Following an adolescence of experimentation and blind optimism, are we seeing the Internet growing up and the advent of an age of reason shaped by disillusionment and disenchantment with blind faith in the great borderless network? The balance of power between governments, citizens, companies and consumers is forging a new Internet of sovereignties, a new space whose rules remain to be defined. Several 'circles' of sovereignty are pitted against one another in this environment. The first concerns personal data[8], which citizens are free to grant or entrust to partners. It also relates to data that citizens pass on to the government and certain authorities. However, there is no guarantee for users paying their taxes online that their data will not be retrieved by hosts. In this first circle, the government's main duty is to protect citizens and their data. The second circle concerns the sovereignty of companies and organisations through data, which are companies' main resource and constitute their added value. The third and final circle concerns the sovereignty of States who, faced with the giants of the web, are only able to influence the debate on data protection within regional entities such as the European Union, whose position and protection mechanisms are being increasingly asserted against American hegemony. How is this new balance of power defining the rules of a fledgling system of governance?

8. Jean Étienne, 'Google Health, un carnet de santé personnel en ligne' [Google Health, an online personal health record], futura-sciences.com, 22 May 2008. ***LINK***.

Somewhere between the ideal of the free web and a climate of threats and surveillance, balkanisation of the network is currently under way

Debates on filtering and fragmentation of the network mark the origins of the concept of Internet 'balkanisation'. These are closely linked to policy and national security issues as well as tensions surrounding the coordination of legal frameworks. We are clearly witnessing a challenge to the multi-stakeholder model of Internet governance. States' increasing desire to provide a political framework both for use and content reflects this state of affairs, as does the commercial pressure applied by GAFA whose commercial interests are closely linked to digital compartmentalisation of content.

A balkanised Internet is uncharted territory with a system of governance in which States seek to assert or even impose their rules on a politically, technically and legally supervised cyberspace. But to what extent can national interference prompted by recent challenges to US online supremacy be legitimised or tolerated?

The concept of 'balkanisation[9]' covers a complex reality, with multiple and often contradictory fragmentation and opening processes occurring at different physical or legal levels of the network. Hence the difficulty in defining a French or European sovereignty strategy either for political or commercial issues. Moreover not one but several cyberspaces exist – the ideal of a free, open and universally accessible cyberspace seems to be undermined every day, not just by the political and economic tensions that infiltrate it, but also by an organisational structure that is more complex than it seems. The global Internet is composed of cultural and regional subsets and shaped by practices that differ from region to region. But in this fragmented Internet, US supremacy is still strong in terms of technical and infrastructure resources as well as content originating in America. The same applies to the military, intelligence and the legal framework of contracts. On the basis of the 'extraterritoriality[10]' principle, it was possible to extend and disseminate this power to other countries until the Wikileaks revelations.

9. See 'La balkanisation du web : chance ou risque pour l'Europe ?' [The balkanisation of the web – an opportunity or threat for Europe?] , a prospective and strategic study by the French Ministry of Defence (strategic affairs directorate) conducted by the French Institute of Geopolitics (University of Paris 8) with contributions from Alix Desforges and Frédérick Douzet, 2015. ***LINK***.

10. Hervé Ascensio, 'Extraterritorialité comme instrument' [Extraterritoriality as an instrument] paper for the French Ministry of Foreign Affairs, 2010. ***LINK***.

Weakness acknowledged and surveillance revealed – the Snowden scandal

The Snowden case marks a turning point in terms of the challenge to US supremacy. It revealed technological flaws while cyberspace found a new centre of power in emerging countries, especially in Southeast Asia. The scandal also showed the limits of increasingly contested US sovereignty. Political awareness significantly increased as a result of the Wikileaks revelations. The expression of this technological, political and legal activism laid the foundations of an appetite for shared digital sovereignty. In this version of sovereignty, the emphasis was on maintaining the respect, integrity and confidentiality of data in the face of increasingly covetous governments and Internet giants. However, this urge to regain sovereignty is at odds with the imperatives of international cooperation, for instance in the fight against cybercrime. The revelations came as an electric shock to Europe, which was determined not to be pushed around any more, even if this meant going on the counter-offensive.

Initial European retaliations and Safe Harbour

Safe Harbour was the perfect example of overlapping sovereignties, providing the basis for the keenly anticipated legal data transfer system, Privacy Shield, which offers a framework for data transfer between Europe and the US. When Safe Harbour was invalidated by the Court of Justice of the European Union (CJEU) on 6 October 2015, this shield temporarily allowed companies to continue business while awaiting the implementation of a new framework. Over 4,000 companies including GAFA and numerous European SMEs had used Safe Harbour for fifteen years. A second version was planned to correct the limitations of the initial agreement. Under criticism from the CJEU, which condemned the intrusion of US security agencies in the access and processing of European citizens' personal data once the data were transferred to their territory, America was therefore forced to go back to the drawing board. Europe wanted to protect its citizens and their fundamental rights, while the US protected its economic champions and their growth. The invalidation of the transatlantic Safe Harbour agreement by the CJEU was therefore a major step. In the same spirit, the decision taken by the German data protection authority, BfDI (the German Federal Data Protection Authority [11]), to suspend data transfer to the United States and ask companies operating in Europe to only store their data within the territory of the European Union, laid the

11. See 'The German Federal Data Protection Authority-The BfDI', Office of the Federal Commissioner for Data Protection and Freedom of Information, 2014. ***LINK***.

foundations for data processing practices that showed greater respect for the sovereignty of States and citizens. The protection and legal supervision of data gradually became a key factor in European digital policy as data established itself as the new commodity.

Data – the new political and economic commodity

Data is becoming established as the web's new commercial commodity and an increasing variety of online services is further fragmenting cyberspace, thus undermining the neutrality of the net[12]. In contrast, it is entirely in Internet companies' interests to maintain and preserve an open and interoperable environment with a view to developing and expanding their commercial activities. However, the balkanisation of the web is not a one-way street – it is the consequence of friction between the sovereign aspirations of States, private stakeholders, companies and citizens. Whatever the cause, these initiatives and claims are fragmenting the web and penalising all stakeholders.

From a business perspective, the boom in Internet and mobile device use and the advent of connected and smart objects have firmly established the commodity of data as a new commercial weapon. Essentially, its value lies not in raw data but in the added value of processing in accordance with companies' requirements. Every day, we receive over 2.5 trillion bytes[13] of data in a highly diverse range of formats including e-mails, text messages, posts on social media, videos, GPS data and measurement indicators from our sensors. Described by some as the new oil, data is providing business with a strategic challenge and big data is viewed as the most appropriate tool for efficiently processing this tsunami of data. Indeed the potential of big data is almost prophetic: the ability to process a mass of raw data to create competitive leverage for companies. From a customer perspective, data processing should in theory refine their experience and interaction with companies in a way that is tailored closely to their requirements. Finally, from an operational perspective, big data should enable more dynamic and smoother management of the value chain.

However, data processing comes with its own set of concerns. As Bernard Benhamou, Secretary General of the Institute of Digital Sovereignty points out, recent debates regarding an amendment adopted[14] in connection

12. 'Les contours de la neutralité du Net en Europe se précisent' [The boundaries of web neutrality are being defined in Europe], lemonde.fr, 31 August 2016. ***LINK***.

13. 'Définition du Big Data' [Definition of big data], IBM. ***LINK***.

14. 'Amendment no. CL129 presented by Mrs Batho and Mr Grandguillaume', National Assembly, 6 January 2016. ***LINK***.

with the French Digital Act reveal two analytical errors regarding the nature of industrial and technological realities facing France and Europe[15]. The amendment provides for the creation of a 'Commission for Digital Sovereignty' whose main duty would be to promote the creation of a sovereign operating system (OS). The notion of developing a sovereign operating system is appealing although largely unviable due to the number of barriers facing the project – although mobile OS are currently the industrial gold standard, they will soon be overtaken by new generation operating systems developed based on connected objects, thus bypassing our mobile terminals. 'At best, the idea that a national initiative (as opposed to a European one like the GSM standard) might provide a credible alternative falls within the realm of pious wishes', asserts Bernard Benhamou[16].

The second weakness of the amendment is the notion of the government creating sovereign encryption tools. The purpose of these tools would be to protect citizens' and companies' data through message and data encryption for which only the government would hold the keys. However, as the Snowden case demonstrated, State initiatives aimed at controlling all means of encryption invariably have perverse effects – flaws that are created deliberately may also be exploited by terrorist groups[17].

Companies, States, users – who should govern the Internet?

Who actually governs the Internet? It is difficult to provide a definitive response to this question since so many thousands of people are involved in the interactions that animate the network. Indeed a distinction should be drawn between the government or governance of the Internet and its political and legal equivalents, and management of the Internet, which is more associated with technical aspects of the network. In fact, technical decisions stem more or less directly from political choices and conversely, these political decisions are affected by technical limitations. This cross-influence is a cause of concern and tension in terms of both stakeholders' freedom and users' sovereignty. Consequently, 'Internet governance' operates based on a 'multi-stakeholder' model involving States, civil society, companies and international organisations. The Internet Corporation for Assigned Names and Numbers

15. Bernard Benhamou, 'Les contresens de la souveraineté numérique' [The contradictions of digital sovereignty], les Echos, 29 January 2016. ***LINK***.

16. *Ibid.*

17. See also, Bruce Schneier, *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company, March 2015.

(Icann[18]) and Internet Engineering Task Force (IETF) define some of these technical aspects, namely network protocols, jointly with the World Wide Web Consortium (W3C), which is responsible for web standards. American pre-eminence, the supposed guarantor of a single, open and decentralised network has now been widely contested for several decades. At the 2012 World Conference on International Telecommunications in Dubai[19], several countries, including China, Russia and Saudi Arabia challenged American domination and advocated the 'sovereign right' of governments to 'regulate the national segment of the Internet'. This attempt failed since Europe and the United States firmly opposed it. 'The architecture of the Internet has become both a major security issue and an issue of sovereignty. For a State, the very fact that power over a technical resource such as a top-level domain name is held by another State is a problem', explains Bernard Benhamou[20].

But what if the real battle were taking place outside Icann? This is a legitimate question, especially since Christopher Mondini, the institution's vice-president, stated that the obligatory reform of the agency was aimed at ensuring a system protected against State interference. However, we should not overstate the influence of an institution that is still relatively unknown to the public and whose prerogatives are rather limited in terms of handling attacks from States suspected of network censorship or surveillance, or indeed faced with GAFA's ambitions. Nevertheless, in political, legal and symbolic terms, the institution will no doubt have a role to play in defining digital sovereignty.

National security and the fight against cyberterrorism

Since the 9/11 attacks, jihadi organisations have significantly honed their web strategies. Cyberterrorism is a genuine threat for both nations and companies. Moreover, cyberterrorist attacks can also originate from States. It is clear from such phenomena as the Russian attack on Georgian computer systems[21] and the work of Syrian pro-Assad hackers that terrorists are determined to use the net as a means of conducting their offensives. States are faced with abundant threats such as hacking of telecommunication facilities and sensitive infrastructure such as airports, stations, underground train networks, etc. And although cyberterrorist attacks are discreet, they are no less harmful because of

18. Amaelle Guiton, 'Samedi, l'Internet sera un peu moins américain' [On Saturday, the Internet will be a little less American], libération.fr, 30 September 2016. ***LINK***.

19. *Id.,* 'Souveraineté numérique : un modèle à inventer' [Digital sovereignty – a model that remains to be invented], libération.fr, 20 May 2016. ***LINK***.

20. Quoted by Amaelle Giton, *ibid.*

21. 'La Géorgie prise sous les feux des attaques de pirates russes' [Georgia under attack from Russian hackers], jounaldunet.com, 12 August 2008. ***LINK***.

this. To date, they have only undermined the image of government sovereignty, but what happens when two trains are diverted from their routes, making this new threat a very real part of citizens' everyday lives?

Concrete measures for fighting cyberterrorism

Since 2003, cybersecurity has been presented in France as a government priority as reflected by the new focus given to the security services, police and Gendarmerie, starting with the Central Directorate of Interior Intelligence (DRCI), which treats Internet surveillance as a priority. Despite vague attempts at international cooperation and an exchange of data and best practice at European level, the government still responds more slowly than the terrorists. At present, cyberspace is viewed more as the instrument than the target of terrorist acts. However, it is now clear that terrorist movements such as Al-Qaeda and Islamic State have the technical means of conducting attacks on computer systems. And although these networks are currently not sufficiently interconnected to hack vital sectors of the economy, the terrorists are increasingly focusing on these types of targets.

The fight against terrorism raises not only the issue of funding but also citizens' sovereignty and the delicate balance between excessive common-law powers of surveillance and respect for civil rights.

Since the 9/11 attacks, the threat of cyberterrorist strikes has been on the rise. Although attacks on the physical world have not abated, as the series of attacks on French soil in the past two years have shown, cybersecurity experts are seeking to limit the impact of the threat by establishing a 'Maginot Line' based on various possible scenarios[22]. Moreover, terrorist groups' current financial resources are enabling them to acquire the necessary facilities and services for further actions, while also assembling the technical means of hacking computer systems. Although terrorist interest in this type of target is still limited, we are witnessing the emergence of a new concept of 'cyberguerilla warfare', a diffuse threat that can come from both small groups of individuals and isolated perpetrators.

22. See *Le Cyberespace, enjeu de souveraineté et de sécurité* [Cyberspace – a challenge in terms of sovereignty and security], proceedings of the 5th International Forum on Cybersecurity, 2013. ***LINK***.

Europe still divided on the issue of sovereignty

While the fight against cyberterrorism is still in its infancy, the battle for economic sovereignty is well under way. Can the European Union and its member states protect their citizens against such threats as network surveillance by the National Security Agency (NSA)[23]? Protecting citizens and States seems to go hand-in-hand with data protection, which should be 'deglobalised'.

In the European Union, sovereignty is also an economic issue with recent tax avoidance scandals raising the question of whether GAFA's income should be territorialised to force them into a legal framework that would account for actual income from their operations in the relevant countries. Since the battle for European digital sovereignty is also an ideological and cultural one, questions could be raised over the viability of a project like the European digital library[24] when faced with the success of Google Books.

Internet sovereignties concern all sectors and areas of responsibility of the EU in all its forms – digital sovereignty, information sovereignty, citizens' individual sovereignty, sovereign cloud, etc. The very notion of sovereignty has a scope that is all the more destabilising since it is constantly evolving. In technical, economic and political terms, the challenge to US domination of the web has prompted Europe to assert itself while also defining new powers, prerogatives and values with respect to States, companies and the giants of the net. Annie Blandin-Obernesser, a law professor at Telecom Bretagne, believes that the battle for sovereignties at European level raises the fundamental question of whether this is compatible with upholding the European Union's values such as openness on which the Internet was founded[25]. As regards the protection of personal data, a draft European regulation will replace the current Directive 95/46/EC[26], which was drafted over twenty years ago, and this should be applicable from 2018. This represents significant progress, especially since it will no longer be possible for GAFA to refrain from applying member states' regulations on the grounds of their disparity.

With regard to competitiveness, public procurement is an essential means of supporting European companies. As recommended by the Institute of Digital Sovereignty, central government and local authority public procurement could be used to earmark a percentage of contracts for the most innovative

23. This is the key issue addressed by a publication edited by Annie Blandin-Obernesser entitled, *Droits et Souveraineté numérique en Europe* [Rights and Digital Sovereignty in Europe], Bruylant, 2016.

24. See 'Europeana. Le patrimoine de l'Europe en ligne' [Europeana – European heritage on-line], bnf.fr. ***LINK.***

25. Annie Blandin-Obernesser, *op. cit.*

26 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data'. ***LINK.***

SMEs. Through their political decisions on economic development, the local authorities and regions of the European Union can guide and support local companies, enabling them to survive in a highly aggressive market.
In a report from July 2015, Akim Oural, a member of the French National Digital Council took this stance, arguing that support for public modernisation with a view to promoting economic development and employment is a major factor in regions' vitality and digital competitiveness. He also wrote that 'emphatic support for digital companies in the regions and for these new ecosystems is a means of strengthening the sovereignty of French territory, [...] ensuring that France is independent from solutions that are imposed uniformly by the giants of the web, who are generally American but in future will be Chinese[27].

GAFA – companies that are more powerful than States

The battle for sovereignty is essentially an economic one. GAFA have proved to be formidable opponents for whom nothing is off limits, whether in terms of anti-competitive practices, tax avoidance or questionable use of recurrent personal data. Faced with these repeated violations, Europe is toughening its stance on the giants of the web. How can GAFA be forced to play by the rules? Pressure from the European Union is beginning to pay dividends, especially with respect to Amazon, which has been forced to pay tax in all countries where the company has subsidiaries, whereas the group had previously centralised its income in Luxembourg. The Old Continent no longer intends to be pushed around and wants to be taken seriously by the big boys.
The time has come for a digital offensive – while the European Union resigned itself to American hegemony for several years, it never promoted the rise of a national champion capable of taking on Google or Amazon on equal terms, as China did with Alibaba or Russia with Yandex. The penalties imposed by Brussels on Microsoft and Intel for abuse of a dominant position stick in people's minds. Since 2010, and particularly since the new Commission took office in 2014, Europe has defied US imperialism, a permanent slight to its sovereignty, especially since the Snowden scandal which placed the spotlight on the US administration's use of European citizens' data. However, initiatives against American giants are still too rare to inspire fear.

27. Akim Oural, 'Gouvernance des politiques numériques dans les territoires' [Governance of digital policies in the regions], a report to the secretary of state for digital affairs, July 2015, p. 20-21. ***LINK***.

Users searching for meaning regarding the way their data is used

What sovereignty have consumers or users got if they are not sufficiently informed about how their data is used? With the advent of big data, companies and public utilities are redefining their strategies to incorporate this new parameter by questioning how consumer requirements can be understood and forecast in real time in order to interact with consumers as effectively as possible. In principle, it is difficult to oppose this objective. How could we fail to approve a logical assessment that involves determining who consumers are and identifying their expectations and requirements? From an economic perspective, many laws governing the use of data appear to impede the growth of companies in Europe. In the current climate, can citizens, consumers of commercial services or public utility users still claim to have sovereignty over their data? This issue echoes the legal power struggle between the Apple Group and American judiciary following the brand's refusal to allow the FBI to access the iPhone data of a suspected terrorist.

Should data be protected even if it means sacrificing innovation, which is so vital to companies? This is the dilemma facing data processing. In France, all companies established within national territory are obliged to declare all personal data processing activities to the CNIL (the French Data Protection Authority). Companies must also nominate a person responsible for data processing. Many companies claim that European data protection legislation is too restrictive and this framework impedes digital innovation, which is crucial for ensuring that French companies are able to compete against the American giants. One of the major differences between the American approach and the European vision on data processing is that across the Atlantic, regulation occurs retrospectively while Europe and France are moving forward on ground that has been marked out due to a desire for caution.

Users of digital public services do not trust the government any more than private companies when it comes to protecting their data. In response to this climate of distrust, in 2015 Sophie Nerbonne, director of compliance at the CNIL, recommended cooperation between public and private stakeholders: 'responsible innovation demands that barriers be removed between the various stakeholders – companies, legislators, regulators and hosts – who must work together in this area [28]'. However the question remains of how to write and enshrine the rules of a constantly changing game in which stakeholders, expertise, powers and regulations are both co-constructing and neutralising one another.

28. Quoted in Paul Morin, '[Big Data 2016] La protection des données freine-t-elle l'essor des marques ?' [Is data protection impeding the growth of brands?], e-marketing.fr, 24 March 2016. ***LINK***.

RESTORING THE SCOPE OF POLITICAL AND ECONOMIC SOVEREIGNTY THROUGH LAW AND TRUST

State sovereignty – economic and security issues regarding data

Between Safe Harbour and Privacy Shield – steps towards measured cyber-retaliation

On 12 July 2016, the European Commission acknowledged that Privacy Shield was fit for purpose. Although it was given limited media coverage, this decision marked the climax of lengthy negotiations between the European Union and the United States following the CJEU judgement. The protection of personal data is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union [29]. This protection afforded to European citizens' data extends beyond the borders of the Union, notably when data is transferred outside European territory. In more concrete terms, transfers of personal data outside the European Union are only permitted if the country receiving these data is deemed 'adequate' by the EU. It must therefore provide guarantees equivalent to those granted by European law. This was the status of the US, whose companies signed up to the Safe Harbour mechanism. One year prior to this, in its judgement of October 2015 [30], the CJEU invalidated the European Commission's decision to acknowledge that Safe Harbour was fit for purpose. The Court took the view that the Commission had taken its decision too hastily without any guarantees regarding the American authorities' access and use of data under the Patriot Act and that European nationals had no right of appeal against this access or use. At a meeting of the Article 29 Working Party, several data protection authorities including the CNIL therefore asked the United States to go back to the drawing board with a view to reaching an agreement within three months. An initial agreement was reached leading to the Privacy Shield [31]. However, this was only a partial success since, although it introduced new guarantees such as the appointment of a mediator in charge of appeals against access to European data by the American public authorities, the agreement still included a number of grey areas such as data collection methods and the effectiveness of the right to appeal.

29. 'New EU rules on data protection put the citizen back in the driving seat', European Parliament News, europarl.europa.eu, 1 June 2016. ***LINK***.

30. 'Invalidation du "safe harbor" par la Cour de justice de l'Union européenne : une décision clé pour la protection des données' [Invalidation of 'safe harbour' by the Court of Justice of the European Union – a key decision for data protection], cnil.fr, 7 October 2015. ***LINK***.

31. Édouard Geffray 'Le "Privacy Shield", exemple de la souveraineté européenne en matière numérique ?' [Privacy Shield – an example of European sovereignty in digital affairs?] , *Letter from the DAJ* [Legal Affairs Directorate], newsletter from the economic and financial ministries, No. 215, 8 September 2016. ***LINK***.

The GDPR, a new strategic challenge for the European Union in terms of sovereignty

The adoption of the General Data Protection Regulation (GDPR) will enable European citizens to benefit from more consistent and harmonised protection of their data throughout the European Union. This major development will finally give European citizens the right to inspect the way their data is processed by private organisations. However, the changes that organisations will have to make to comply with this new regulatory development, which will come into force on 25 May 2018, remain to be determined. The GDPR will also introduce new minimum standards concerning the processing, security and sharing of EU residents' personal data. Companies must get up to speed and plan the necessary changes to ensure they are compliant within two years of the fateful date. As regards Great Britain, it is unlikely that Brexit will hamper enforcement of the GDPR across the Channel since it relates to the personal data of all European citizens and the United Kingdom has still not specified the terms of its exit from the EU. Consequently, all European regulations in force still apply to it.

The GDPR will therefore replace member states' national data protection provisions. The strength of this harmonised system lies in the implementation of new standardised measures within organisations, a shared framework that will simplify operations for companies that are currently juggling twenty-eight different protection frameworks. Member states will retain the right to supplement and bolster European legislation with local provisions.

Other highlights of this new framework include the 'right to be forgotten' and the use of verifiable data protection technologies. Tougher penalties will also be applied with fines of up to 4% of organisations' annual turnover [32] or a maximum of €20 million for the most serious offences. The vast majority of companies appear prepared to toe the line and are planning to increase their investments in order to comply with data protection and sovereignty requirements. Infringements will entail severe consequences for companies which, if they fail to adapt within a two-year period, will run the risk of penalties or audits of their data protection systems.

Efforts to ensure compliance will rely on encryption technologies for protecting sensitive data. The obligation to notify data leaks also represents a challenge for companies and organisations, who will be obliged to update their problem resolution systems, enabling them to quickly provide an accurate overview of incidents.

32. Warwick Ashford, 'International IT trade group urges firms to prepare for GDPR', computerweekly.com, 29 April 2016. ***LINK***.

The case for internationalised Internet governance

Beyond the European strategies, there is growing awareness around the world of a new internationalised system of web governance. The organisation responsible for domain names and the technical structure of the Internet, which had been controlled by the US since 1998, is now opening up. This is rather a subtle revolution for the public but one that has genuine symbolic significance. At midnight on 30 September 2016, Icann ceased to be controlled by the US Department of Commerce. This organisation manages the domain names of web addresses including *.fr* and *.com*. It also manages network logistics at global level. Icann Vice-President, Christopher Mondini believes that although this new system of governance will have no major consequences in terms of how the Internet operates, it should protect it from excessive State influence. Icann is changing and evolving gradually to become a sort of 'United Nations of the Internet' with a multi-party system of governance grouped into four bodies representing the private sector, technical experts, civil society and governments. A court of arbitration will settle disputes and may annul decisions. In France, this limitation of American influence would have been met with approval, had the State Secretariat for Digital Technology not expressed concerns over a new architecture which, while limiting the role of States, gave prominence to the major companies of the web[33]. Across the Atlantic, the end of the monopoly on governance was met with less excitement and was described as an imperfect yet essential transition by Daniel Castro, Vice-President of the Information Technology and Innovation Foundation (ITIF). It is nevertheless a transition that marks a crucial constitutional moment in the overhaul of Internet governance.

Backdoors and data encryption – how can a balance be struck between States' pursuit of sovereignty, security objectives and the protection of civil liberties?

Without security, there is no sovereignty. How far should we go in defining and protecting the scope of these data? For States and companies, security requirements must not prevail over civil liberties and personal data protection. So says the CNIL in its annual report for 2015[34]. In a climate profoundly affected by the fight against terrorism, many States are legislating on intelligence, prompting a debate on the issue of data encryption. While

33. Nicolas Rauline, 'Pour la France, la gouvernance d'Internet est aux mains des Gafa' [Internet governance for France is in the hands of GAFA], lesechos.fr, 23 March 2016. ***LINK***.

34. 'Bilan 2015 : un nombre record de plaintes' [2015 review – a record number of complaints], cnil.fr, 8 April 2015. ***LINK***.

some leaders regard encryption as a tool for terrorists, the CNIL believes that data encryption could play a 'vital role in our security'. Encryption can also be a tool for protecting company and State computer systems, which are increasingly exposed to cyber-attacks from independent hackers or even foreign governments.

Representatives of agencies and States advocate the introduction of backdoors enabling the authorities to access encrypted data stored on mobile phones and even go as far as threatening penalties for companies who put themselves in the position of being unable to cooperate with the authorities. According to the CNIL, these measures are unnecessary and the current legal framework is adequate since it allows 'digital requisitions, access to login details, interceptions of correspondence, audiovisual recordings, capture of computer data displayed on-screen or entered by keyboard and consultation of technical experts with respect to encrypted data[35]'.

On the pretext of fighting cybercrime, the entire Internet ecosystem has been undermined. Indeed, the collective risk is too high and such measures would diminish individuals' level of security due to the scale of the cybercrime phenomenon and moreover are not capable of preventing hackers from using their own encryption tools. In France, the government appears to be in favour of encrypting personal data and e-mails. Indeed, an amendment approved within the scope of criminal justice reform that provides for 'a five-year prison sentence and a €350,000 fine for anyone 'refusing to provide the requesting judicial authority investigating terrorist crimes or offences […] with data protected by a cryptology tool that they have designed[36]' has moreover been adopted. This decision runs contrary to the recommendations of the French National Cybersecurity Agency (ANSSI), which also advocates encryption. According to Apple CEO, Tim Cook, weakening encryption while providing authorities with access via a backdoor would open a 'Pandora's box[37]' that would be difficult to close – a key left under the doormat may not only be of benefit to those who wish to do good. Other malicious parties may also find it, so the challenge is to ensure that only fully authorised people are able to access backdoors. On the pretext of protecting national security, these sovereign conflicts undermine the competitiveness of companies that are dependent on the trust placed in them by users to protect and ensure the confidentiality of their data.

35. CNIL. ***LINK***.

36 'Amendment n°. 90 (Rect)' to the law on fighting organised crime, terrorism and their financing', National Assembly, 2 February 2016, p. 2. ***LINK***.

37. Larry Greenemeier, 'Apple fears court order will open Pandora's box for iPhone security', Scientific American, 17 February 2016. ***LINK***.

Companies are pragmatic and more eager to ensure consumer sovereignty

Steps towards roll-out of digital codes of ethics

User/consumer sovereignty with respect to data clearly reflects a desire to regain control of information that has hitherto been blindly surrendered to companies and authorities. In keeping with this rationale, the La Poste group is planning to position itself as a trusted third party in the processing of these users' data, a role that far exceeds its traditional remit of logistics processing of letters and parcels. A privacy policy is intended to restore customer control over the way their data are used based on an open data web portal known as dataNova [38]. In keeping with the group's commitments to greater security and traceability in relation to data flow, a dedicated data management platform is due to be set up in 2017.

Several studies conducted in France and Europe have revealed consumers' growing concerns over the use of their private data. In January 2014, 81% of French people stated that they were 'concerned' about the protection of their personal data in a CSA study [39]. These concerns relate mainly to their online data (85% of respondents). Moreover, a study conducted by the Orange group between December 2013 and January 2014 in several European countries [40] revealed that 78% of respondents found it difficult to trust companies regarding the use of their personal data, 78% of respondents believed that service providers had access to too much information on their purchasing, habits and preferences, and 82% thought that consumers had few means of monitoring the way their personal data are used by companies and institutions. This mistrust has prompted companies to develop digital trust policies. They have realised that consumer and user scepticism towards their private data processing and protection policies constitutes a genuine threat to their brand image and consequently, growth. Nowadays, they are more eager to protect data entrusted to them.

For instance, a Dell group study [41] on companies' attitudes towards data revealed that 87% of the companies surveyed regarded data protection as a priority for their digital transformation plans. In the coming years, it is therefore likely that companies will have to considerably increase their

38. See datanova.laposte.fr/page/accueil/

39. 'Les Français et la protection des données personnelles' [The French and data protection], a study conducted by CSA for Orange, February 2014. ***LINK***.

40. Orange, 'The future of digital trust. A European study on the nature of consumer trust and personal data', February 2014. ***LINK***.

41. 'Data observatory. 2014 IDC study', Dell, study conducted in partnership with EMC and MTI, 2014. ***LINK***.

investments in data security by 40% for key accounts and 26% for SMEs. The public should be given greater access to companies' data security policies. Features included in all privacy policies include transparency of data use, details regarding the identity of the person in charge of data collection and consumer control over their own data. Finally, some companies offer to assist consumers with the protection, amendment and deletion of their data.

Since 2010, more and more companies are trialling these measures including the Orange group, which signed its privacy policy in November 2013[42], Moët & Chandon[43], the resume generation website Doyoubuzz and Axway[44]. Axway is a special case since it chose to incorporate its privacy policy in its website's general terms and conditions of use. Finally the 'data friendly' charter of French public national television broadcaster, France Télévisions[45] is an innovative initiative since the personal data of users who have been inactive for over eighteen months are automatically anonymised. Moreover, services relating to this policy can be accessed anonymously.

In addition to companies' desire to meet consumer expectations while protecting one of the fundamental aspects of their competitiveness, privacy policies also meet new legal requirements that came into force in October 2013 when MEPs in the Committee on Civil Liberties approved a major revision of EU data protection rules. This necessary development updated a European legislative framework that dated back to 1995 (Directive 95/46/EC) and provided new rules satisfying an urgent need to update legal principles that were no longer appropriate to the new web environment. It was therefore impossible to effectively protect individuals' right to data protection. In France, the CNIL provides companies with documents helping them to comply with rules on collecting, processing and storing consumer data. Despite the precious support this offers, it is not always sufficient for preventing legal or ethical pitfalls.

42. Orange, 'Charte protection des données personnelles et de la vie privée' [Personal data and privacy protection policy], December 2014. ***LINK***.

43. Moët & Chandon, 'Privacy policy', 15 March 2016 (fr.moet.com/Privacy-policy).

44. Axway, 'Charte des données personnelles' [Privacy policy], s.d. ***LINK***.

45. France Télévisions, 'Data friendly policy', 2014. ***LINK***.

How can users' sovereignty over their data be restored to them? Technological solutions provide inroads for regaining control, notably by promoting new regulation models devised in France

What if a home-grown solution could provide the answer for start-ups, VSEs and SMEs eager to regain control of their data? Besides the OVH group[46], the French Tech start-up network includes few success stories in terms of cloud and secure solutions. This offering which is still struggling to recover from the failure of the French sovereign cloud, Andromède, is therefore in urgent need of expansion. What if sovereign solutions were to emerge at regional level with closer involvement from local authorities? Philippe Clerc, a consultant with the French Chamber of Commerce and Industry (CCI France) and expert in international business intelligence suggests that 'server farms[47]' and spaces for sharing software capabilities may provide a new type of 'local sovereign cloud', meaning that regional sovereignty and pooling of resources within a local framework may provide the basis of French data sovereignty[48].

Corporate data protection constitutes a competitive advantage

The Snowden and Wikileaks scandals combined with intense media coverage on the issue of corporate personal data management due to Safe Harbour have helped increase awareness of digital sovereignty challenges among company managers. However, the very concept of 'digital sovereignty' remains abstract for managers of SMEs or VSEs who are more likely to consider these issues from a perspective of computer system security or cybersecurity.

As such, surveys on SMEs' business intelligence practices conducted by the Chamber of Commerce and Industry (CCI) for Brittany and other bodies[49] provide valuable insights. The results of the study reveal that although 44.2% of SMEs have set up a data protection procedure and 59% have trained their staff on the concept of data confidentiality, less than 60% assess threats and risks relating to data protection. The CCIs are looking to help SMEs manage these new challenges in partnership with professional federations and the government.

46. Antoine Crochet-Damais and Alain Steinmann, 'Comment OVH est devenu le premier hébergeur d'Europe' [How OVH became Europe's top host], journaldunet.com, 14 October 2013. ***LINK***.

47. Matthieu Quiret, 'Les fermes de serveurs régionales étendent leur toile' [Regional server farms expand their network], lesechos.fr, 3 September 2014. ***LINK***.

48. Philippe Clerc, "Souveraineté des données – 'Innovation ouverte, cloud, big data : entrer dans la révolution numérique tout en gardant nos données souveraines est déterminant pour l'économie française'" [Data sovereignty – 'Open-source, cloud and big data innovation: joining the digital revolution while retaining our sovereign data is crucial for the French economy'], interview, services.wiggam.com, 29 June 2014. ***LINK***.

49. 'L'intelligence économique dans les entreprises bretonnes' [Business intelligence in Breton companies], *Repères économiques Bretagne*, n°. 16, September 2015, n°. 16. ***LINK***.

Philippe Clerc suggests adopting a strategic approach to data protection that is similar to that used for tackling counterfeiting: 'In order to tackle this threat, we conduct regular, targeted awareness-raising campaigns based on close cooperation between companies, their representatives and the public authorities within the National Anti-Counterfeiting Committee (CNAC). This body provides a forum for discussion, analysis and influence. The same approach should be taken to data sovereignty instead of setting up a commission for digital sovereignty[50]'. It should be possible to escape technological dependence on GAFA, although not without genuine impetus from the public authorities. Chambers of trade, professional federations, the French national employers' confederation (Medef) and the General Confederation of Small and Medium-Sized Enterprises (CGPME) are waiting to see this political will, which is a prerequisite for promoting French digital solutions. This issue was raised in Senate proceedings during the debate on the 'Digital Republic' bill.

The open-source innovation of FabLabs are making data sovereignty an increasingly complex challenge to which the cloud appears to provide an attempt at a tangible response. French business is ready for the cloud, the primary condition being for companies to clearly mark out a 'cyberterritory' and define a clear relationship with service providers with regard to security. Moreover, companies must also educate their employees on the issue of data sovereignty by implementing strict security protocols.

How can improved data protection provide French companies with a competitive advantage? Across the Atlantic, data protection has always been perceived as a competitive advantage for companies, whereas it has too often been viewed as an additional cost by French companies who fail to appreciate the return on investment of such efforts. French industry must now adopt new ways of using data and the associated new tools, namely the disruptive technologies of big data, cloud computing and open data. Companies' data sovereignty is a challenge of the digital revolution and will provide an indicator of the dynamism of the French economy.

50. Philippe Clerc, art. cit.

RECOMMENDATIONS FOR REGULATED INTERNET GOVERNANCE

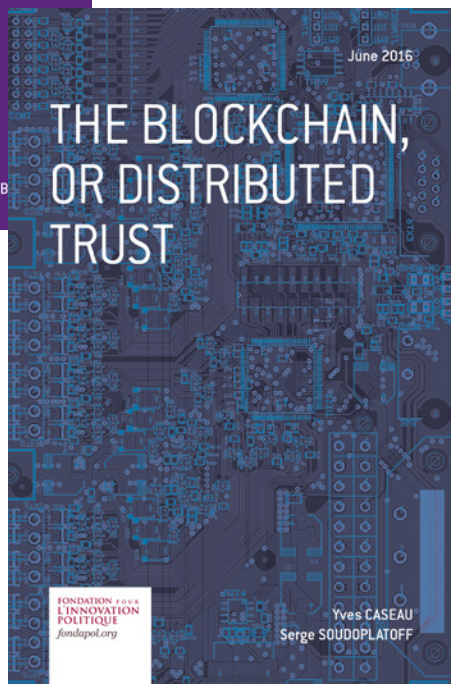
• The requirement for a European and international standard framework for a new system of governance Europe's standard-setting and regulatory powers, which are often blamed for the paralysis of the European Union could work in its favour since Europe is built on a model of economic integration, governance and shared management of standards. By setting up an appropriate legal system for the protection of personal data, it should be possible to ensure the security of European citizens' data. This sovereign framework would contribute to the influence of a European data protection policy that could be duplicated in other countries. Moreover, this sovereign framework of standards would help boost the appeal of the European area for foreign companies. Finally, this strengthened framework would enable the extraterritoriality of the United States and, more recently, emerging countries, to be limited in the battle for data hosting.

• Redefining international Internet governance in order to establish new collective security frameworks in the age of interconnected networks, the stances of European Union countries on cyberspace governance must be coordinated in a way that respects the sovereignty of member states and the values that unite them. In diplomatic terms, France has always been an advocate of multilateral Internet governance, with governments acting legitimately through the multi-stakeholder model that encourages dialogue between these various institutions and Icann in particular. The introduction of internationalised domain names such as .Paris, reflects this tendency. While encouraging private sector stakeholders to take a leading role in Internet governance, it is entirely in States' interests to promote a system of governance that respects the public interest without allowing commercial or regional interests to prevail. In such a scenario, State sovereignty would be fully compatible with a political framework based on the general interest that fosters trust among citizens and consumers as well as encouraging corporate investment.

• Companies – regaining users' trust. This requires greater trust and transparency in the processing of users' data through the threefold principle of 'regulation, co-regulation and self-regulation' of data. Moreover, an international code of conduct for multinational companies and a global monitoring body such as the International Internet Committee, which has already been discussed within the UN, are tangible options.

• The blockchain solution * is an asset guaranteeing the sovereignty of users' data. The ability to secure a company, authority or infrastructure by reviewing the entire chain of trust focusing on the weak links, while ensuring the integrity, confidentiality, traceability and archiving of these data is a priority for investigation.

* See Yves Caseau and Serge Soudoplatoff, *La Blockchain, ou la confiance distribuée* [Blockchain technology or distributed trust], Fondation pour l'innovation politique, 2016.



Economy of Knowledge
Idriss J. Aberkane, May 2015

The blockchain, or distributed trust
Yves Caseau and Serge Soudoplatoff, June 2016

OUR PUBLICATIONS

Rethinking our trade policy
Laurence Daziano, January 2017

Measures of poverty, measures against poverty
Julien Damon, December 2016

Austria of populists
Patrick Moreau, November 2016

Europe and the challenges of petro-solar energy
Albert Bressand, November 2016

Front National in the countryside. Farmers and the FN vote,
Eddy Fougier and Jérôme Fourquet, October 2016

Political Innovation 2016
Fondation pour l'innovation politique, PUF, October 2016

The new world of cars (2): The promises of electric mobility
Jean-Pierre Corniou, October 2016

The new world of cars (1): the dead end of combustion engin
Jean-Pierre Corniou, October 2016

The European Opinion in 2016
Dominique Reynié (dir.), Éditions Lignes de Repères, September 2016

Individuals against the state. Actuality of the French liberal thinking
Jérôme Perrier, September 2016

Rebuilding public broadcasting
Olivier Babeau, September 2016

Competition in the digital era
Charles-Antoine Schwerer, July 2016

Portrait of Muslims in Europe: unity in diversity
Vincent Tournier, June 2016

Portrait of Muslims in France: a plural community
Nadia Henni-Moulaï, June 2016

*The blockchain, or distributed trust**
Yves Caseau and Serge Soudoplatoff, June 2016

The radical Left: links, places and struggles (2012-2017)
Sylvain Boulouque, May 2016, 56 pages

Governing to reform: elements of methodology
Erwan Le Noan and Matthieu Montjotin, May 2016, 64 pages

Occupiers of Zones-to-defend (2): the temptation of violence
Eddy Fougier, April 2016, 44 pages

Occupiers of Zones-to-defend (1): a new anticapitalist phenomemon
Eddy Fougier, April 2016, 44 pages

Regional elections (2): political parties are questioned but not challenged
Jérôme Fourquet and Sylvain Manternach, March 2016, 52 pages

Regional elections (1): far-right vote and terrorist attacks
Jérôme Fourquet and Sylvain Manternach, March 2016, 60 pages

Law serving innovation and growth
Sophie Vermeille, Mathieu Kohmann and Mathieu Luinaud, February 2016

Lobbying: a democratic tool, Anthony Escurat, February 2016
Values of Islam, Dominique Reynié, January 2016

Shiites and Sunnis – is peace impossible?
Mathieu Terrier, January 2016

*Companies governance and society needs**
Daniel Hurstel, December 2015

Mutuality: meeting insurance-sector challenges
Arnaud Chneiweiss and Stéphane Tisserand, November 2015

*Noopolitics: the power of knowledge**
Idriss J. Aberkane, November 2015

European public opinion in 2015
Dominique Reynié, November 2015

Political Innovation 2015
Fondation pour l'innovation politique, October 2015

Good COP21, Bad COP21 (2): beyond political correctness
Albert Bressand, October 2015

Good COP21, Bad COP21 (1): Europe's Kant meet China's Machiavel
Albert Bressand, October 2015

SMEs: new financing methods
Mohamed Abdesslam and Benjamin Le Pendeven, October 2015

Long live motoring (2): the case for road use
Mathieu Flonneau and Jean-Pierre Orfeuil, October 2015

Long live motoring (1): conditions for user-friendly mobility
Mathieu Flonneau and Jean-Pierre Orfeuil, October 2015

Crisis of the Arab/Muslim conscience
Malik Bezouh, September 2015

Département elections of March 2015 (3): second round
Jérôme Fourquet and Sylvain Manternach, August 2015

Département elections of March 2015 (2): first round
Jérôme Fourquet and Sylvain Manternach, August 2015

Département elections of March 2015 (1): background
Jérôme Fourquet and Sylvain Manternach, August 2015

Higher education: the limits of a Master qualification for all
Julien Gonzalez, July 2015

Economic policy: the Franco-German issue
Wolfgang Glomb and Henry d'Arcole, June 2015

Laws of primaries, past and future.
François Bazin, June 2015

*Economy of Knowledge**
Idriss J. Aberkane, May 2015

Fighting theft and burglary: an economic approach
Emmanuel Combe and Sébastien Daziano, May 2015

Uniting for action: a programme for growth
Alain Madelin, May 2015

A new vision of enterprise and human value
Francis Mer, April 2015

Transport and funding mobility
Yves Crozet, April 2015

Digital technology and mobility: impact and synergies
Jean Coldefy, April 2015

Islam and democracy: facing modernity
Mohamed Beddy Ebnou, March 2015

Islam and democracy: the foundations
Ahmad Al-Raysuni, March 2015

Women and Islam: a reformist vision
Asma Lamrabet, March 2015

Education and Islam
Mustapha Cherif, March 2015

What have parliamentary by-elections since 2012 told us?
Dominique Reynié, February 2015

Islam and the values of the Republic
Saad Khiari, February 2015

Islam and the social contract
Philippe Moulinet, February 2015

Sufism: spirituality and citizenship
Bariza Khiari – February 2015

Humanism and humanity in Islam
Ahmed Bouyerdene, February 2015

Eradicating hepatitis C in France: what public strategies should be adopted?
Nicolas Bouzou and Christophe Marques, January 2015

Keys to understanding the Koran
Tareq Oubrou, January 2015

Religious pluralism in Islam or the awareness of otherness
Éric Geoffroy, January 2015

*Future memories**
a survey conducted in partnership with the Fondation pour la Mémoire de la Shoah, Dominique Reynié, January 2015

A disintegrating American middle class
Julien Damon, December 2014

The case for supplemental education insurance: middle class schooling
Erwan Le Noan and Dominique Reynié – November 2014

*Anti-Semitism in French public opinion. New perspectives**
Dominique Reynié, November 2014

The competition policy: a plus for industry
Emmanuel Combe, November 2014

2014 European Elections (2): rise of the FN, decline of the UMP and the Breton vote
Jérôme Fourquet, October 2014

2014 European Elections (1): the left in pieces
Jérôme Fourquet, October 2014

Political Innovation 2014
Fondation pour l'innovation politique, October 2014

Energy/climate: the case for an effective policy
Albert Bressand, September 2014

Global urbanisation. An opportunity for France
Laurence Daziano, July 2014

What can we expect from monetary policy?
Pascal Salin, May 2014

Change is constant
Suzanne Baverez and Jean Sénié, May 2014

Too many emigrants? Perspectives on those who leave France
Julien Gonzalez, May 2014

European public opinion in 2014
Dominique Reynié, April 2014

Tax better to earn more
Robin Rivaton, April 2014

The innovative State (2): Diversifying the senior civil service
Kevin Brookes and Benjamin Le Pendeven, March 2014

The innovative State (1): Strengthening the role of think tanks
Kevin Brookes and Benjamin Le Pendeven, March 2014

The case for a new tax deal
Gianmarco Monsellato, March 2014

An end to begging with children
Julien Damon, March 2014

Low cost: an economic and democratic revolution
Emmanuel Combe, February 2014

Fair access to cancer therapies
Nicolas Bouzou – February 2014

Reforming teachers' status
Luc Chatel, January2014

Social impact bonds: a social finance tool
Yan de Kerorguen, December 2013

Debureaucratisation through trust to promote growth
Pierre Pezziardi, Serge Soudoplatoff and Xavier Quérat-Hément - November 2013

Les valeurs des Franciliens
Guénaëlle Gault, october 2013

Settling a student strike: case study in Quebec
Jean-Patrick Brady and Stéphane Paquin, October 2013

A single employment contract incorporating severance pay
Charles Beigbeder, September 2013

European Opinion in 2013
Dominique Reynié, September 2014

*The new emerging countries: the 'BENIVM countries**
Laurence Daziano, July 2013

Energy transition in Europe: good intentions and poor calculations
Albert Bressand, July 2013

Minimising travel: a different way of working and living
Julien Damon, June 2013

KAPITAL. Rebuilding Industry
Christian Saint-Étienne and Robin Rivaton, April 2013

A code of ethics for politics and public officials in France
Les Arvernes and the Fondation pour l'innovation politique, April 2013

The middle classes in emerging countries
Julien Damon, April 2013

Political Innovation 2013
Fondation pour l'innovation politique, March 2013

Reviving our industry through automation (2): issues
Robin Rivaton, December 2012

Reviving our industry through automation (1): strategies
Robin Rivaton, December 2012

Taxation a key issue for competitiveness
Aldo Cardoso, Michel Didier, Bertrand Jacquillat, Dominique Reynié and Grégoire Sentilhes, December 2012

An alternative monetary policy to resolve the crisis
Nicolas Goetzmann, December 2012

Has the new tax policy made the solidarity tax on wealth unconstitutional?
Aldo Cardoso, November 2012

Taxation: why and how a rich country is a poor country ...
Bertrand Jacquillat, October 2012

Youth and Sustainable Development
Fondapol, Nomadéis, United Nations, June 2012

Philanthropy. Entrepreneurs in solidarity
Francis Charhon, May/June 2012

Poverty statistics: a sense of proportion
Julien Damon, May 2012

Freeing up funding of the economy
Robin Rivaton, April 2012

Savings for social housing
Julie Merle, April 2012

European opinion in 2012
Dominique Reynié, March 2012

Shared values
Dominique Reynié, March 2012

The right in Europe
Dominique Reynié, February 2012

Political Innovation 2012
Fondation pour l'innovation politique, January 2012

Free schools: initiative, autonomy and responsibility
Charles Feuillerade, January 2012

French energy policy (2): strategies
Rémy Prud'homme, January 2012

French energy policy: issues (1)
Rémy Prud'homme, January 2012

Revolution of values and globalization
Luc Ferry, January 2012

The End of social democracy in Europe?
Sir Stuart Bell, December 2011

Industry regulation: accountability through non-governmental rules
Jean-Pierre Teyssier, December 2011

Hospitality
Emmanuel Hirsch, December 2011

12 ideas for 2012
Fondation pour l'innovation politique, December 2011

The middle class and housing
Julien Damon, December 2011

Three proposals to reform the healthcare system
Nicolas Bouzou, November 2011

The new parliament: the French law of 23 July 2008 revising the Constitution
Jean-Félix de Bujadoux, November 2011

Responsibility
Alain-Gérard Slama, November 2011

The middle class vote
Élisabeth Dupoirier, November 2011

From annuity to competition
Emmanuel Combe et Jean-Louis Mucchielli, October 2011

The middle class and savings
Nicolas Pécourt, October 2011

A profile of the middle class
Laure Bonneval, Jérôme Fourquet and Fabienne Gomant, October 2011

Morals, ethics and ethical conduct
Michel Maffesoli, October 2011

Forgetting Communism, changing era
Stéphane Courtois, October 2011

World youths
Dominique Reynié, September 2011

Increasing the purchasing power through competition
Emmanuel Combe, September 2011

Religious freedom
Henri Madelin, September 2011

The ways to a balanced budget
Jean-Marc Daniel, September 2011

Ecology, values and democracy
Corine Pelluchon, August 2011

Valoriser les monuments historiques : de nouvelles stratégies
Wladimir Mitrofanoff and Christiane Schmuckle-Mollard, July 2011

Opposing technosciences: their networks
Eddy Fougier, July 2011

Opposing technosciences: their reasons
Sylvain Boulouque, July 2011

Fraternity
Paul Thibaud, June 2011

Digital transformation
Jean-Pierre Corniou, June 2011

Commitment
Dominique Schnapper, May 2011

Liberty, Equality, Fraternity
André Glucksmann - May 2011

What future for our defense industry
Guillaume Lagane, May 2011

Corporate social responsibility
Aurélien Acquier, Jean-Pascal Gond et Jacques Igalens, May 2011

Islamic finance
Lila Guermas-Sayegh, May 2011

The state of the right Deutshcland
Patrick Moreau, April 2011

The state of the right Slovaquia
Étienne Boisserie, April 2011

Who owns the French public debt ?
Guillaume Leroy, April 2011

The precautionary principle in the word
Nicolas de Sadeleer, March 2011

Understanding the Tea Party
Henri Hude, March 2011

The state of the right Netherlands
Niek Pas, March 2011

Agricultural productivity and water quality
Gérard Morice, March 2011

Water: from volume to value
Jean-Louis Chaussade, March 2011

Water: how to treat micro-pollutants?
Philippe Hartemann, March 2011

Water: global challenges, French perspectives
Gérard Payen, March 2011

Irrigation for sustainable agriculture
Jean-Paul Renoux, March 2011

Water management: towards new models
Antoine Frérot, March 2011

The state of the right Austria
Patrick Moreau, Februay 2011

Employees' Interest sustaining purchasing power and employment
Jacques Perche and Antoine Pertinax, February 2011

The Franco-German tandem and the euro crisis
Wolfgang Glomb, February 2011

*2011, World Youths**
Fondation pour l'innovation politique, January 2011

The European opinion in 2011
Dominique Reynié, January 2011

Public service 2.0
Thierry Weibel, January 2011

*The state of the right: Bulgaria**
Antony Todorov, December 2010

The return of sortition in politics
Gil Delannoi, December 2010

The People's moral ability
Raymond Boudon, November 2010

Academia in the land of capital
Bernard Belloc and Pierre-François Mourier, November 2010

*Achieving a new Common Agricultural Policy**
Bernard Bachelier, November 2010

*Food Security: a global challenge**
Bernard Bachelier, November 2010

The unknown virtues of low cost carriers
Emmanuel Combe, November 2010

Political Innovation 2011
Fondation pour l'innovation politique, November 2010

Overcoming the Defense budget issue
Guillaume Lagane, October 2010

*The state of the right: Spain**
Joan Marcet, October 2010

The virtues of competition
David Sraer, September 2010

Internet, politics and citizen coproduction
Robin Berjon, September 2010

*The state of the right: Poland**
Dominika Tomaszewska-Mortimer, August 2010

*The state of the right: Sweden and Denmark**
Jacob Christensen, July 2010

What is the police up to?
Mathieu Zagrodzki, July 2010

*The state of the right: Italy**
Sofia Ventura, July 2010

Banking crisis, public debt: a German perspective
Wolfgang Glomb, July 2010

Public debt, public concerns
Jérôme Fourquet, June 2010

*Banking regulations for sustainable growth**
Nathalie Janson, June 2010

Four proposals to renew our agricultural model
Pascal Perri, May 2010

2010 regional elections: where have all the voters gone?
Pascal Perrineau, May 2010

The European opinion in 2010
Dominique Reynié, May 2010

*The Netherlands: the populist temptation**
Christophe de Voogd, May 2010

Four ideas to boost spending power
Pascal Perri, April 2010

*The state of the right: Great Britain**
David Hanley, April 2010

Reinforce the regions' economic role
Nicolas Bouzou, March 2010

Reforming the Constitution to rein in government debt
Jacques Delpla, February 2010

A strategy to reduce France's public debt
Nicolas Bouzou, February 2010

Catholic Church policy: liberty vs liberalism
Émile Perreau-Saussine, October 2009

*2009 European elections**
Corinne Deloy, Dominique Reynié and Pascal Perrineau, September 2009

The Nazi-Soviet alliance, 70 years on
Stéphane Courtois, July 2009

The administrative state and liberalism: a French story
Lucien Jaume, June 2009

*European development policy**
Jean-Michel Debrat, June 2009

Academics: defending their status, illustrating a status quo
David Bonneau and Bruno Bensasson, May 2009

Fighting age discrimination in the workplace
Elise Muir, June 2009

*Stemming the protectionist tide in Europe**
Nicolas Bouzou, March 2009

Civil service vs civil society
Dominique Reynié, March 2009

The European opinion in 2009
Dominique Reynié, March 2009

Working on Sundays: Sunday workers' perspectives
Dominique Reynié, January 2009

Retrouvez notre actualité et nos publications sur fondapol.org

*The titles marked with an asterisk are available in English.

THE FONDATION POUR L'INNOVATION POLITIQUE NEEDS YOUR SUPPORT

To reinforce its independence and carry out its mission, the Fondation pour l'innovation politque, an independent organization, needs the support of private companies and individuals. Donors are invited to attend the annual general meeting that defines the Fondation orientations. The Fondation also invites them regularly to meet its staff and advisors, to talk about its publication before they are released, and to attend events it organizes.

As a government-approved organization, in accordance with the decree published on 14th April 2004, the Fondation pour l'innovation politique can accept donations and legacies from individuals and private companies.

Thank you for fostering critical analysis on the direction taken by France and helping us defend European integration and free economy.

DIGITAL SOVEREIGNTY – STEPS TOWARDS A NEW SYSTEM OF INTERNET GOVERNANCE

By Farid GUEHAM

Just how omnipotent will GAFA become in terms of accessing and processing our personal data? The convenience of voluntary servitude comes at a price – the exposure of our habits, purchasing and health.

Since the Wikileaks revelations, the commodity of data has become a resource coveted and envied by governments and companies. A new ecosystem has sprung up in response to the unbridled race for this prized commodity pitting the 'circles' of citizen, government and corporate sovereignty against one other. Is anyone capable of imparting a message of individual freedom without hitting a wall of powerful multinationals?

At a time when the European Union is refining its data protection policy, the rules of a fledgling system of governance are being shaped every day by a new balance of power. The issue of personal data protection, a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, both in and outside of European territory, has refocused attention on the urgent need to define an international framework of sovereignties.

With the European Commission's recognition of the Privacy Shield on 12 July 2016 and the Safe Harbour framework pledging equivalent protection of data outside the European area, a new system is emerging in a fierce and competitive environment reflecting the sudden yet necessary realisation that the age of the Internet with its innate freedoms has come to an end.

11, rue de Grenelle • 75007 Paris – France • Tél. : 33 (0)1 47 53 67 00 • contact@fondapol.org