PRIVACY IN THE DIGITAL WORLD:
BEYOND COMPLIANCE, TOWARDS TRUST
Wavestone is a new consulting brand, formed by the merger of Solucom and Kurt Salmon’s European business (excluding Consumer Goods and Retail Consulting activities outside of France) in 2016.

Wavestone’s vision is to enlighten and guide our clients in their strategic, value-adding decision-making by capitalising on our functional, industry and technological expertise. Our firm combines the expertise of 2,500 people across 4 continents. Wavestone is also the first truly independent consulting firm in France.
Digital data is now a key tool for all organisations. The emergence of new technologies makes it possible to process increasing amounts of data and extract more of the associated benefits.

However, such capacities also spark fear among citizens and regulators, which must be taken into account in order to ensure the success of digital transformation.

In this context, the principle of privacy is evolving, as is the role it can play in current digital transformation.

At Wavestone, we believe it is crucial that both private and public organisations know how to use and handle personal data in order to become digital champions, whilst maintaining a relationship of trust with their employees and customers. For us, transparency is pivotal for maintaining this relationship of trust.

In this publication, we have sought to shed light on the various facets of this complex subject. In so doing, each organisation may determine its own position in the face of privacy challenges in the digital world.

Enjoy!

“Data is at the heart of the digital revolution. Trust and transparency will be key factors for enabling its success”

FRÉDÉRIC GOUX
Partner
We would like express our sincere gratitude to Tine A. Larsen and Milad Doueihi for having provided us with two interviews for this publication. We would also like to thank Armand de Vallois, Jean-Christophe Procot, Hervé Commerly, Pauline Rouaud and Julien Douillard for their contributions to this document.
06 / Preface

08 / What does privacy mean in a digital world? An exclusive survey conducted by Wavestone

22 / Which legal frameworks should be implemented on an international scale?

30 / Respect for privacy in digital transformation: key challenges and principles

44 / The future of digital privacy
Privacy in the digital world: going beyond compliance and making a success of your digital transformation
In this publication, we seek to provide readers with an understanding of the concept of privacy in the digital age, both from a general public and regulatory perspective.

We hope that our insights will enable large organisations to confront the challenge of privacy in a digital world by aligning their programmes with the increasing expectations of states and citizens.

1. **IN A DIGITAL WORLD, WHAT LEVEL OF PRIVACY?**

   We used a survey to ask this question to citizens, whether European, American or Chinese. Overview of the results of this survey, followed by the first part of the interview of Milad Doueihi, philosopher.

2. **WHICH LEGAL FRAMEWORK AT AN INTERNATIONAL LEVEL?**

   Protection of personal data is now regulated throughout the world and is increasing exponentially. Overview of the main approaches, supplemented by an interview with Tine A. Larsen, President of the Luxembourg regulator.

3. **RESPECTING PRIVACY IN DIGITAL TRANSFORMATION: KEY CHALLENGES AND PRINCIPLES**

   Based on the analysis of concrete projects in different business areas, we provide the keys to implement a strategy of trust and transparency with end clients and consumers. The breakdown is illustrated by the testimonies of Armand de Vallois, Jean-Christophe Procot and Hervé Commerly, experts from Wavestone.

4. **WHAT ARE THE NEXT CHALLENGES?**

   Personal data will be at the heart of the next digital evolutions, especially through algorithms. Such evolutions must be anticipated now, and are at the core of our consideration enriched by the second part of the interview of Milad Doueihi, philosopher.
In the digital world, citizens, irrespective of their country of origin, are increasingly concerned about respect for their privacy. They trust few organisations; namely traditional players such as banks. Their most important priority? Having control over the data they entrust. Their biggest fear? New technologies leading to a world of increased surveillance.
AN INTERNATIONAL SURVEY ABOUT HOW CITIZENS PERCEIVE PRIVACY

The results presented in this paper form a synthesis of the survey as a whole. Detailed results and analysis are available on: www.wavestone.com/insights

The results of this survey should not be viewed as scientific evidence. Rather, it is representative of global and national trends in the perception of privacy by individuals. The survey considers the responses of 1,587 participants, between July and August 2016, across 6 countries.

Among the majority of respondents were younger generations, often perceived as “digital” citizens and more intrigued by the subject of privacy in a digital world.

A CONSISTENT VISION ON AN INTERNATIONAL SCALE

The countries selected for the survey, namely France, Italy, Germany, China, the United States and the United Kingdom, were selected on the basis of their socio-economic environments and the diversity of regulatory frameworks concerning privacy protection. These elements can influence the perception and opinion of citizens regarding the protection of personal data.

However, despite initial contextual differences, we observed through collected responses that the theme of privacy is perceived in a relatively similar way across the surveyed countries.
Indeed, there are differences and particularities: notably in how German respondents place particular importance ahead of their counterparts on the definition of privacy relating to personal freedom. Responses from the United States demonstrate less confidence in public institutions.

Generally, however, there is greater global awareness among individuals about privacy and personal data topics. This can be explained by the borderless nature of data and the digital world, with the digital citizen expecting his or her privacy to be respected regardless of borders.

This observation reinforces the importance of respecting privacy in digital projects, regardless of the country and population in question.

**What is your definition of privacy today?**

*(Figures correspond to the number of persons who selected each answer)*

- **Have control over who can get information about you**: 1092
- **Not having to disclose what you consider to be a matter of privacy against your will**: 1012
- **Have control over the type of information collected about you**: 976
- **Not being observed or disturbed by others**: 858
- **Have "your" moments, on your own, without being monitored by others**: 732
- **Not being monitored at the office**: 537
- **Not being systematically identified in public spaces**: 520
- **Other**: 16

**FROM FREEDOM TO CONTROL: EVOLUTION OF THE MEANING OF “PRIVACY”**

Privacy is traditionally seen as the possibility for an individual to retain some form of anonymity in his or her activities and to have the ability to isolate oneself in order to best protect his or her interests. It is intimately linked to the notion of freedom.

However, analysis of the survey results shows that this notion tends to disappear in favour of the control of information.

We have proposed to our respondents to select one or more definitions that relate to either notion.
It is also important to provide customers and employees with assurance that they have control over their data. This is possible by providing individuals with simple and autonomous means of access.

**ALL PERSONAL DATA ARE VIEWED AS SENSITIVE IN THE EYES OF CITIZENS**

When questioned about the level of sensitivity, the panel showed slight differences in their responses. Citizens considered most of the proposed types of data as sensitive. They did not perceive that leakage of certain data types could have serious or even irreversible consequences (e.g. health data), in contrast to other data types (e.g. financial data), for which most countries have already implemented regulatory frameworks which protect individuals (for example, rapid reimbursement in the event of fraud).

The most frequently selected responses relate to control. This pattern is confirmed by observing the intermediate proposals. For example, “having control over the type of information collected about you” is a more widely selected response (more than half) than “having moments alone, without being monitored by others”, relating to freedom.

**According to you, what are the most sensitive data?** (rating from 1 to 5)

- Financial data: 4.13
- Health data: 4.02
- Personal data (name, age): 3.96
- Behavioural data: 3.87
- Contact details: 3.87
- Family status data: 3.85
- Data on devices and IT network used: 3.83
- Localisation data: 3.83
- Audio or video data: 3.28
- Lifestyle data: 3.14
- Other: 0.45
This demonstrates that, regardless of the type of personal data handled by a project, special attention must be given at least to the communication of protection levels.

**TRUST VARIES GREATLY FROM ONE SECTOR OF ACTIVITY TO ANOTHER**

We asked respondents to indicate which type(s) of organisation(s) they trusted the most with regard to using their personal data for previously authorised use.

We can differentiate between three main groups of actors. Firstly, the actors grouped under the category of “institutions” command the highest level of trust among respondents. This includes public institutions, semi-public institutions or entities from the traditional economy with which individuals have historically shared a relationship of trust. This is particularly the case given how such

---

### Which organisations do you trust?

<table>
<thead>
<tr>
<th>Organisation Type</th>
<th>China</th>
<th>France</th>
<th>Germany</th>
<th>Italy</th>
<th>United Kingdom</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks</td>
<td>51%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medical organisations</td>
<td>45%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public organisations</td>
<td>45%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment/credit card companies</td>
<td>34%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insurance companies</td>
<td>29%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energy suppliers</td>
<td>24%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport operators</td>
<td>14%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telecommunication operators</td>
<td>13%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local shops or online shops</td>
<td>13%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>11%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web companies</td>
<td>10%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technological companies</td>
<td>9%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social media</td>
<td>6%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**More than 25%**

- Banks, Health, Public institutions, Credit card providers, Insurance

**Between 10 and 20%**

- Energy, Transportation, Telecoms, Retail

**Less than 10%**

- Web companies, Social media, Technological companies
institutions have processed sensitive data throughout their history (medical data, etc.). We also find significant differences within this category, with more than half of respondents claiming to trust banks with the processing of their data. Image and reputation are therefore crucial for banks, which serve to meet customer expectations in the aim of retaining their position as the number one trusted partner.

Secondly, an intermediate category encompasses the actors of daily life such as transport operators and energy suppliers. Such B2C actors carry out swift digital transformation and benefit from the existing relationship of trust.

Thirdly and finally are actors in the digital economy, whether web giants or technology firms.

The social media paradox: lowest in confidence but highest in use

Mistrust towards such companies can be attributed to the amount of data they collect and use on individuals, as well as recent high-profile prosecution cases related to such use. However, this result reveals a paradox. Despite this evident lack of trust, individuals continue to frequently use the services provided by these actors, due in part to a lack of alternative, as well as the information entrusted seeming to be, often wrongly, harmless and insignificant in the eyes of the individual.

Banks are the number one trusted partners - a place to be cherished!
NEW TECHNOLOGIES RAISING FEARs

The panel highlights four technologies most likely to put their privacy in danger, according to respondents. What do they all have in common? Making it possible to collect data without this activity being under the control of the persons concerned. This would, for certain individuals, equate to a form of surveillance.

On the other hand, technologies which provide citizens with the ability to choose the data they share, such as connected objects or Cloud services storing private information, are considered less risky in terms of privacy and therefore do not feature as any of the four technologies.

Although not traditionally thought of as “sensitive”, data on individual behaviours and actions are now viewed as a significant stumbling block between customer expectations about the respect for privacy and the increasingly personalised customer relationship.

In your opinion, which technologies can threaten your privacy? (rating from 1 to 5, from the least to the most threatening)

<table>
<thead>
<tr>
<th>Technology</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public WIFI to surf on the Internet</td>
<td>3,87</td>
</tr>
<tr>
<td>Drones recording images, videos and sounds in a public space, and the behavior of people</td>
<td>3,79</td>
</tr>
<tr>
<td>Technologies for capturing moods, opinions and how people behave when using Internet</td>
<td>3,78</td>
</tr>
<tr>
<td>Cameras recording images, videos and sounds in a public space, and the behavior of people</td>
<td>3,75</td>
</tr>
</tbody>
</table>
Measures to improve the security of the data provided: increasing the level of security of online accounts such as strengthening passwords, changing passwords regularly, checking access rights and being more attentive when sharing personal information over the Internet...

In addition to such measures, we find more extreme solutions. This ranges from the complete closure of accounts on social networks, exclusive use of trusted and tested sites or technologies, to deleting history and cookies with every use of search engines.

While these individual initiatives can contribute to increasing the protection of privacy, they may conflict with new uses and innovation promoted by organisations, thus limiting or even preventing the personalisation of the customer relationship.

Over the last years, have you changed your behavior to better protect your privacy and limit the sharing of your personal data?

<table>
<thead>
<tr>
<th>Yes</th>
<th>Don’t know/No opinion</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>0%</td>
<td>52%</td>
</tr>
</tbody>
</table>
Respecting privacy is a concern for three-quarters of respondents. Chinese respondents were by far the most concerned about the subject (97%). The United States and France share similar responses to this question despite different visions on the subject. Germans seem less worried about the topic, 35% of them don’t feel concerned about their privacy, which contrasts from their other answers. Opinions were more dubious on this question in Italy and the United Kingdom.
To what extent do you feel that you have control over your private information?

Generally, respondents estimate that they only have partial control over their personal information. The proportion of respondents thus represent a markedly similar percentage in five of the countries surveyed (between 68% in France and the United Kingdom and 75% in Germany).

The United States is to be analysed separately, insofar as more than a third of respondents claim to have complete control over their personal information.
In general, do you think that public or private organisations use the information you provide only for a purpose you have authorised?

By country

<table>
<thead>
<tr>
<th>Country</th>
<th>Yes</th>
<th>No</th>
<th>Don't know/No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>283</td>
<td>48%</td>
<td>37%</td>
</tr>
<tr>
<td>France</td>
<td>307</td>
<td>64%</td>
<td>15%</td>
</tr>
<tr>
<td>Germany</td>
<td>252</td>
<td>59%</td>
<td>24%</td>
</tr>
<tr>
<td>Italy</td>
<td>247</td>
<td>59%</td>
<td>21%</td>
</tr>
<tr>
<td>UK</td>
<td>253</td>
<td>45%</td>
<td>29%</td>
</tr>
<tr>
<td>US</td>
<td>245</td>
<td>49%</td>
<td>16%</td>
</tr>
</tbody>
</table>

A first group stands out, more than 60% on average of French and Italian respondents join their German counterparts in claiming not to trust that organisations use their data exclusively for the purposes announced at the time of collection. Even if they entrust them with their data.

These responses contrast with those of Chinese and American respondents, who demonstrate a stronger tendency to trust public and private organisations.

It should also be noted that this is a complex issue for several respondents. Thus, one in five respondents are not commenting.
To what extent do you agree that existing laws provide a reasonable level of protection for your privacy?

This question triggered a wide range of responses among the respondents. Half (51%) of respondents somewhat or completely agree with the statement that existing laws protect their privacy, while one-quarter (25%) somewhat or completely disagree. Almost a quarter (22%) of respondents were unable to decide.

More than two-thirds of Chinese (80%) and US (70%) citizens somewhat or completely agree, whereas in both countries, national regulations are less developed than in Europe.

About one-third (38% and 31% respectively) of citizens in France and Germany tend to somewhat or strongly disagree, underlying the need for even more regulation.
The first part of our interview with Milad Doueihi, American philosopher and Chair of Digital Humanities at Paris-Sorbonne University, placing privacy in the context of a more global evolution of digital culture and its impact on privacy.

Is the notion, or indeed value, of private life still relevant today?

It is relevant, but not as we understand it. Private life does not carry the same meaning as in the past, even the recent past. What has changed, with social networks or the Internet in general, is the scale of metadata and logs.

There is a massification in the production of data and this data is now analysed to identify, to follow – that is not to say to spy on – people. Thus, the cultural landscape in which we go about our private lives and the way that individual, public and collective actors perceive it, has changed.

So the challenge of today would be to redefine the notion of a private life in a digital world?

Yes. It is interesting to redefine because it has been subject to many modifications. Some studies show that adolescents, at a particular moment in time, agreed to share more information which their parents would have considered as private. Gradually, behaviours of this type have become more commonplace. What would be interesting to see would be embedding this alteration of private life into the alteration of digital data itself.

Such evolutions in digital technology, as you mentioned, involve progressing from a fixed digital culture to one of mobility in which people enter the public space and interact with others. Has such evolution also changed our relationship to others and our own private lives?

Absolutely. Mobility can be interpreted in different ways. Firstly, there is essential type of mobility through transitivity

Find the full interview on our website: www.wavestone.com/insights
There is a massification in the production of data and this data is now analysed to identify, to follow – that is not to say to spy on – people.

between support and tools. We see this today with a kind of continuity (moving from a tablet to a phone to the computer) which did not exist previously. Secondly, a significant amount of data and metadata logs contain geo-location information, transmitted by mobile phones. Finally, the third type of mobility could be related to platforms which collect data. This is the case for the Cloud, for example, which complexifies jurisdiction surrounding the framing of data, calling the need for supervision of data transfers through devices such as safe harbors or privacy shields.

Returning now to the notion of digital identity, it was introduced by the digital revolution and can be differentiated from civil identity. Has this changed our relationship with others and has it redefined what we are willing to share about our identities?

The first phase of digital identity was straightforward: aggregation of our online presence. However, due in part to mobility, the massification of data and the emergence of digital sociability has evolved. We have witnessed a paradigm for personalised recommendations, which harness the elements of the digital identity. This modifies the context of social or economic pertinency, shifting how we view and understand confidence and trust. It is one of the most important success factors which arise with this new form of digital identity. The association of tabular choices, suggested by algorithmic platforms deriving their choices from the analysis of interactions, will produce recommendations. We therefore witness a shift from an era defined by measurement to an area of social precision, of pertinence. This modifies the perception of our relationship to others.
Since the introduction of digital privacy in legislative literature, regulations have become increasingly stringent. The European Union is the engine driving this trend with the General Data Protection Regulation (GDPR), although other countries have not faltered behind as we witness a global effort in establishing regulation for the handling of personal data.
AN INCREASINGLY INTERNATIONAL REGULATORY FRAMEWORK

The concept of privacy, as understood in history, can be understood across several centuries of legislation. It began taking shape in 1948, inscribed in Article 12 of the Universal Declaration of Human Rights: “No one will be the object of arbitrary interference in his private life (...). Everyone has the right to be protected by law against such interference or attacks”.

Regulation around the protection of personal data is a more recent phenomenon. It is directly linked to the development of information technology and the increased collection of data by organisations. In addition, the market value of data adds a further layer of complexity with the emergence of an international regulatory consensus.

Sweden was the first state to establish legislation on the subject in 1973. In France, the “Loi Informatique et Libertés” was enacted in 1978, following debates over the Safari project, aimed at creating a centralised database of information about individuals.

Without reviewing each national law and its timeliness, an analysis of the initiatives implemented on regional scales provides a holistic view of the main privacy trends.

EUROPEAN UNION: THE STATE PROTECTING ITS CITIZENS

The European Union was the first institution to establish legislation on the subject in 1995 with the publication of Directive 1995/46/EC. This first attempt at creating legislative harmony on an institutional and European scale has been followed by the implementation of numerous principles,
defined in the law of various Member States, including the establishment of supervisory authorities. This legislation is rooted in the “Guidelines for the Protection of Privacy and Transborder Flows of Personal Data” published by the OECD in 1980, which were non-binding.

In April 2016, the European Union elected to strengthen its legislation with the General Data Protection Regulation (GDPR), which, unlike the 1995 directive, will be directly applicable in the law of the Member States of the European Union. Its implementation is planned for May 2018, when organisations must ensure their compliance with the requirements of the regulation. Developments will soon take place in e-privacy in the near future, aligning traditional requirements on privacy with more recent developments and innovation, thus addressing the topics of secrecy and correspondence in the digital age. Through such literature, the European Union will adopt the position as a protector of citizen data.

US: MAKING PEOPLE AWARE OF THEIR RESPONSIBILITIES

There is no specific regulation nor regulator within American law which oversees the collection and use of personal data at a federal level. Instead, the United States operates under a combination of laws
In 2016, the United States and the EU drew up a new arrangement, the Privacy Shield, designed to offer better protection for data transfers which apply to certain sectors or states. Some regulation covers specific categories of personal data, such as financial data or health-related data, while others regulate activities which exploit such data, such as digital marketing. In addition to such regulations, best practices developed by federal agencies and industrial groups are also used as a means of auto-regulation. The Fourth Amendment of the US Constitution can also be referenced for the protection of personal privacy. Finally, laws around consumer protection, while they do not regulate personal privacy, forbid practices around the disclosure of personal data. Nevertheless, American citizens display a certain degree of flexibility regarding the distribution of their personal data.

As shown by the evolution of “Safe Harbor”, differences exist between the American and the European vision. This legal mechanism was implemented to ensure the protection of data transfer between the EU and the USA until October 2015, thereafter invalidated by the Court of Justice of the European Union (CJEU). According to the CJEU, the level of data protection offered by the United States was no longer satisfactory in light of the information leaked by Edward Snowden regarding the global surveillance programme operated by the American government. In February 2016, the United States and the EU drew up a new arrangement, the Privacy Shield, which came into force in August 2016 and is designed to offer better protection for data transfers.

ASIA: A SITUATION UNDER DEVELOPMENT

With respect to data protection, we can categorise Asian countries and territories in two ways. Some are relatively mature on the subject, including South Korea, Singapore, Hong Kong or Taiwan. Until recently, China did not have any specific personal data protection legislation. However, in November 2016, new regulations applicable to operators from June 2017 were implemented. This new regulation will integrate widely agreed principles on respecting personal privacy and will require the storage of personal data on Chinese territory.

On the other hand, other countries in the area are yet to implement regulations regarding the protection of personal data on a large scale, despite on-going debates.
REST OF THE WORLD: REGIONAL INITIATIVES UNDER DEVELOPMENT

In Africa, the first legislation on the subject was implemented in 2001, in Cape Verde. In 2004, Burkina Faso was the first state to establish a national regulator. At the regional level, the African Union Convention on Cybersecurity and Personal Data Protection, signed by 18 countries in 2014, incorporates notions derived from European legislation, with no legal binding.

In the Middle East, states such as the United Arab Emirates (UAE) and Saudi Arabia do not have specific legislation regarding the protection of personal data. Specific to these countries is the application of Sharia law, stating that damage can be claimed if the disclosure of personal data leads to abuse or damage.

In South America, several countries implement independent regulators. Moreover, they benefit from constitutional guarantees regarding personal data protection. This is particularly the case in Uruguay and Argentina, two countries recognised by the European Union as providing sufficient levels of data protection.
Interview with Tine A. Larsen, president of the National Commission for Data Protection (NCDP) of Luxembourg

How has the role of a supervisory authority like the NCDP evolved over the past few years? Will the role change again under the new GDPR?

The role of the NCDP is constantly evolving as it must address the changes driven by developments in information technology. The last 15 years have witnessed the emergence of social networks, Cloud computing and an exponential increase in collected data. It is now easier than ever to acquire the necessary IT resources to process such data. The NCDP must adapt its role when facing these new challenges. In addition, citizens are more and more conscious of their rights and the necessity to better protect their privacy in an increasingly digital world. The new European regulation reinforces the supervisory role of the NCDP, allowing the NCDP to stricter impose administrative fines which must be effective, proportionate and deterrent.

In your view, why have the topics of privacy and data protection become so important for the general public over the last few years?

With the “computerisation” of our society over the last two decades, the development of blogs and social networks and the internationalisation of nominative data flows have radically changed the game. The exchange of personal data has become a global phenomenon, corporate IT infrastructure is increasingly outsourced to the Cloud and the Internet is the most widely used tool in our daily lives. Moreover, the volume of personal data has witnessed an explosion indicated by the unprecedented rise of data storage centres across the world. The development of new technologies such as artificial intelligence and data mining techniques will also considerably increase data processing and analysis capabilities.

Find the full interview on our website: www.wavestone.com/insights
From a citizen point of view, if you ask a young person what is their most important possession, the majority will answer “my smartphone”. This object, coupled with data servers hosted across the Internet, holds information about most aspects of their lives and the associated data. Citizens wish to benefit from services generated by the global collection of data (personalised services, social networks...) whilst preserving their privacy.

Is there any difference in perception between European regulators over what is at stake and the future application of GDPR?

To implement GDPR, European legislators will benefit from experiences from the application of the 1995 directive. The transposition of the directive by the Member States generated national legal literature marking differences between each country, which did not contribute to the uniform application of the principles of data protection at the European level. The choice of regulation as a legal instrument rather than a new directive is justified by the desire to avoid discrepancies between Member States and to contribute to the emergence of a Digital Single Market.

What should we retain from GDPR and the main developments it brings to citizens, companies, administrations and public entities?

This new regulation clearly prioritises addressing the concerns of citizens, consumers and indeed all stakeholders involved in the field of data protection.

It is built upon transparency, requiring companies to use easily understandable and accessible language in all communications with individuals. The list of information which must be communicated has also been considerably extended. The conditions for obtaining prior consent were clarified, including for children and adolescents. Finally, individuals benefit from new rights such as the right to erasure (right to oblivion) and the right to portability allowing for better control over what happens to personal data.

The regulation not only affects the way companies can be held accountable, but links the processing of personal data to the entirety of the sub-contracting chain. We can expect a net decrease in declarative constraints to the NCDP. But the consequence of this reduction places the expectation of robust accountability measures by companies, whilst offering them increased
freedom in the implementation of their personal data management policy. At all times, such companies must be capable of demonstrating the relevance and adequacy of technical and organisational measures implemented to guarantee data protection.

Administrative and public entities must also be compliant with the requirements of the new regulation. However, the literature allows Member States to legislate in the relevant public authority domain, such as for national security. To support stakeholders in the implementation of the regulations, data protection officers will become mandatory, while only compulsory in certain situations for companies.

Numerous digital initiatives have taken off in recent years (Big Data, IoT, Blockchain). What risks do these technological advancements carry for citizens?

A very important risk is the generalisation of automated decision-making based on the increasingly detailed digital profiles of individuals. Technologies are shaping a society where algorithms will soon dictate all decision-making. This context raises questions about the human aspect as well as the quality and reliability of data found in digital profiles. However, this is not just about risk. Such technologies also hold fruitful opportunities for improving the quality of life of citizens. For example, the blockchain system has become an integral component of finance in the economy of Luxembourg.

One benefit of the new regulation is that it avoids specific mention of technologies and rather concentrates on risk management principles and techniques linked to data protection. However, risks will indeed evolve with technological advancement. It will therefore be necessary to maintain efficient and appropriate risk management strategies.

Is the impacts of innovation well understood by citizens?

As with every new technology, we always find discrepancy between its introduction into society and the perceived risks or disruption this technology will create. However, with data protection principles applied from conception and by default, European legislature will in any case require that the creation of new devices and services will consider data protection requirements from the offset. In the same way that passenger safety is central to the manufacturing of cars, data protection will serve at the core of technological advancement.
Ensuring the respect of privacy in a digital world not only requires integration into every project, but integration into every company culture. This approach will also facilitate compliance with new regulations in the respective countries.
MANY PROJECTS AIM AT DIGITALISING BUSINESS PROCESSES AND CUSTOMER RELATIONSHIPS IN ORDER TO OPTIMISE EXISTING PROCESSES, INTRODUCE CUSTOMER PROXIMITY OR OFFER NEW SERVICES

The following examples, based on Wavestone’s consulting experience, illustrate such trends.

Historically, postmen, meter readers and service technicians have worked with paper (address databases, meter-reading or maintenance documentation). Work is organised according to the tasks to be performed and can usually be operated alone and independently throughout the day, before information is collected and consolidated at the end of a work shift.

The dematerialisation of such paper-based processes is intended to help organisations or agents in their activities by collecting data, better organising the work to be performed and sequencing tasks.

This digitalisation process occurs in different sectors for specific purposes. For example, in the energy sector, smart meters create innovative opportunities around energy saving and fraud management through the collation of consumption data. In the insurance sector, accumulating data on customer preferences enables the personalisation and customisation of services and the development of additional offerings.

Such developments require the collation and manipulation of masses of personal data.

CYBERSECURITY ALONE IS NOT SUFFICIENT FOR PROTECTING DIGITAL PRIVACY

To protect personal data so crucial to the digital market, organisations will pursue cybersecurity measures, such as secure transfer protocols or data encryption. However, we may question if such measures are sufficient, while concerns over data misuse, profiling and automated decision-making intensify. An IT security-oriented approach alone is not sufficient. To address the fears over the respect of privacy, it is essential for organisations to reassure individuals by guaranteeing the non-manipulation of data without their prior knowledge and against their will.
FOUR MAJOR PRINCIPLES

The following guiding principles are to be applied in the collation and use of personal data.

1. Communicate transparently and explicitly, informing individuals on the data that is collected about them even if not directly obtained from those concerned. Our survey essentially illustrates this meaning of privacy to citizens: what kind of information is accessible about me, and to whom? It also means sharing the reasons behind data collection and the intended usage. Under no circumstances should data be collected without the purpose of collection disclosed to the persons concerned. Recent sanctions from regulators have illustrated that such activity is always exposed in the media, with heavy reputational impact and lost customer confidence often the damaging consequences. Building a relationship of trust takes years, whereas losing it only takes minutes.

2. Minimise the collection and storage of personal data. Less data collected about an individual means a lower risk of unauthorised and non-compliant use. For existing data, it is possible to process data while minimising risks through the use of “declassifying” techniques such as anonymisation, pseudonymisation (replacing direct identifiers with “codes”), randomisation (randomly generated data which retains the statistical value but conceals the origin) or generalisation of data sets.

Regarding data sharing and exchange, mathematical methods facilitate the exchange of data between two organisations, whilst ensuring data anonymity. When selecting such methods, it is important to assess their limitations. A poorly executed “sensitivity reduction” can still directly lead to the source of original data. For example, this can involve deleting the name but keeping the date of birth, place of birth and address.

Such methods enable organisations to optimise the customer relationship in two ways: by providing a better understanding of the digital customers’ profile and by demonstrating respect for customer privacy. This is the path chosen by Apple through the concept of differential privacy to differentiate from competitors Google and Microsoft.

3. Ensure individuals are in control of their personal data not by generating value through the access to data, but rather by providing individuals with control over their data, allowing services to develop based on their needs.
Use cases for self-data are also subject to research in the insurance sector, with some insurance companies contemplating the complete removal of client spaces to instead install them on self-data Cloud platforms. The insurer will then have access to the data belonging to his client but is no longer in ownership of that data.

Beyond self-data, such trends may even lead to the “Green Button” mechanism where individuals explicitly validate access to their data at any time. This principle, albeit difficult to implement in practice, can be restricted to particularly sensitive data, such as health data.

4. Implement a win-win model by clearly demonstrating the benefits generated by collecting and using data, not only for the organisation but also for individuals. Such benefits can be shared with customers through various means, such as additional services, rebates and compensation.

This approach may even drive the ease in adoption of new uses in an environment where increases in market share carry significant impact.

Ultimately, we are able to identify several levers in motion for building an honourable circle of trust when using an individuals’ data with respect and for the purposes of increasing the level of confidence.

This approach, labelled “self-data”, can be applied in the context of an energy consumption optimisation project, an example of which is to ask customers to indicate the temperature in their homes to record the potential cost savings associated with heating reduction. An individual will then be informed of the potential cost savings by autonomously using and managing a self-data Cloud platform, connected to his personal equipment to enable the cross-analysis of data through consultation of his digital thermometer and energy bills.
What changes have occurred over the last few years in the mass retail sector?

Over the last decade, we have shifted from a distribution model focusing on costs and volume to a model based upon understanding our customers. Mass distribution is thus a thing of the past, as it completely overlooks the interests of the customer relationship. Nowadays, our model gathers and stores knowledge about our customers, allowing us to develop closer proximity with the customer and loyalty programmes which support the frequency and consistency of their purchases.

How should organisations handle such changes?

In recent years, awareness by business stakeholders of the opportunities that come with the high potential of customer data has increased. Nevertheless, resources must be used wisely in supporting the efforts of organisations to get closer to their customers. Data must be collected, handled and reconciled against frameworks which correspond to customer expectations and regulatory requirements.

For example, the “opt-in” option is a good way to ensure that customers are well informed and accept the collection and processing of their data.

Increasingly, rewards are used as a means for encouraging customers to accept the disclosure of their data. However, this model has its limitations. It is essential to ensure that services are of interest to customers and contribute to the ease of their lives, as well as ensuring that individuals have agreed to provide their data.

Do you have some examples of projects which created apprehension?

The introduction of RFID chips (integrated technology which enables the identification and follow-up of objects or people) in electronic tagging is a good example.

Many projects have been launched in the textile industry based on optimising production costs, inventory automation in stores and warehouses as well as the ease of chip insertion into clothes. It is crucial to have real-time knowledge of stock levels and to have reliable information in an omni-channel context, where it
is increasingly common to see online purchases made ahead of in-store collections.

RFID chips can also contribute to data production based on customer journeys and the actual product itself, for example calculating ratios to record the number of times a product has been tried on in a fitting room compared to successful purchases of that product. This type of information is essential in the context of fast fashion in the textile industry.

However, such chips are also a cause for concern. For example, salesmen can “potentially” connect a customer to a product (the RFID chips use unique identifiers) and track their activity over the duration of their shop visit (the chipset remains activated).

**How did you address these concerns?**

We implemented what we call “Privacy By Design”, which goes beyond strict principles regarding chip use (identification and follow-up of products, not customers) and incorporates several other principles:

- A visible marker showing that clothes are equipped with a RFID chip
- Training sales teams so they are better qualified to respond to customer queries, such as informing customers that chips may be removed by cutting the tags attached to a product, a service offered in stores, or declaring that the company in question will never connect a customer and a chip
- Dedicated webpages for communicating all information required to understand the chip and the data it collects

These are some examples of best practices which are applicable to all projects involving the treatment of sensitive data. We must lead by example when handling and informing individuals about how to handle such data. It is therefore crucial to reassure customers and answer their questions so as to anticipate and alleviate their concerns.

“Increasingly, rewards are used as a means for encouraging customers to accept the disclosure of their data”
How is the concept of privacy between employees and employers perceived?

It is a concept that has changed significantly over the last few years. The privacy concerns of employers about their employees is that they often do not devote enough time to their work. For employees, the notion of privacy is goes hand in hand with flexible working conditions such as flexible hours, reduced surveillance and teleworking arrangements. Employees also value a limit on the amount of information that the employer can gather about them.

On the basis of this concept of privacy and to improve employee privacy, employers increasingly seek to support employees in their personal lives through well-being services such as laundry and daycare services, company restaurants and complementary insurance. However, providing such support also requires that the employer knows more and more about the private life of employees, such as the composition of their family and eating habits linked to religious beliefs.

What explains such concerns?

It should be understood that employers are increasingly interested in collecting data to improve understanding of their employees. Employees are increasingly reluctant to communicate this information, especially the younger workforces. Employers wants to retain their employees for longer, facilitate their decision-making and help them to perform more effectively and efficiently in the professional and personal lives. The employer collects such data not directly communicated by the employee themselves but from third parties, such as social networks, previous employers, managers, and data inputs from work tools.

Both employees and customers are concerned by this development. It would almost say that, by definition, employees suspect employers of attempting to monitor their every move. The employee is then left to wonder how it is possible to retain control over privacy if employers collect all this information about them,
Do you have an example of a recent project which echoed such concerns?

The plan of the French government plan to introduce a tax withheld at source. An employee’s salary withheld is an example of this. The aim is to simplify an individual’s life by avoiding deferred payments which can lead to difficult situations. For example, tax collection methods for the state can be improved with a reduction in income set by the employer as an indication that an employee is no longer able to pay the tax rate of the previous year. However, citizens are quick to express concerns about the information their employer holds about them. As well as financial information, a tax return can contain additional private information such as marital status, children, ancillary income and any assistance provided to persons with difficulties. The objective should be therefore to ensure that the purpose of the data collected will be limited to tax purposes and that access to such data will be controlled. The employee wants to ensure that his or her data will not be used for any purposes other than that previously agreed to, such as modifying a salary due to learning the employee’s ancillary income.

What developments have taken place in human resources management that will impact the protection of personal data?

Several major trends have emerged:

/ Big Data in recruitment activities, particularly sourcing, which should be supervised in order to ensure legitimacy when collecting data

/ The multiplication of decision-making for career managers (for example, the creation of succession trees or the identification of key personnel) for automated decision-making, a sensitive topic for regulators

/ Mobility, with an increasingly frequent introduction of new professional mobile terminals which do not facilitate the separation between the data produced in private settings and data produced in professional settings. The question of the “right to disconnect” is also alluded to regularly.

“Employees are increasingly reluctant to communicate this information, especially the younger workforces”
Principles around respecting digital privacy should establish an enticing corporate culture for customers

Beyond simply complying with different regulations, not necessarily the most effective means to building trust in the digital customer relationship, the best practices described below have proved in our experience to be most effective with respect to change management.

**Best practice n°1**

Formalise a company-wide ethical charter

A company-wide ethical charter will provide a strong basis for building respect for privacy. Sharing this charter throughout the organisation will reinforce key organisational principles of transparency and trust. It can be written as part of the implementation of binding corporate rules (BCR), in efforts to establish frameworks treating more important issues than simple data transfers. By introducing a selection of simple yet effective rules to follow, such as the introduction of prior consent by default, an organisation can develop its principles and company philosophy. The charter will aim to cover all personal data, whether from customers, partners or employees. Beyond a binding regulatory aspect, it will above all ensure that organisations look to develop their treatment of such issues in an increasingly digital world. Its adoption at a corporate level combined with an effective communication campaign will ensure the message is disseminated across to all employees. It will also contribute to the corporate social commitments of the organisation.

**Best practice n°2**

Establish a privacy ethics committee

To handle the most complex issues at an operational level, a privacy ethics committee will be implemented. This committee may be attached to existing organisations responsible for ethics and professional conduct. Composed of members of various business lines, including (but not limited to) IT, HR, compliance, legal and customer relations, the committee will be chaired by a member of senior management. It will arbitrate situations experienced in particularly data-sensitive projects and handle any received complaints. It will also serve as part of the communication strategy on the subject of respect for privacy.
Facilitate the implementation of “Privacy by Design” by the business lines

Respect for privacy in the digital world is a relatively new concept, yet to be fully embraced and implemented by organisations. A dedicated operational effort should be made to equip the relevant teams with simple and effective tools to integrate such concepts into projects. A privacy impact assessment of projects (based on the types of data collected and how it is proposed to be processed) using a matrix is a strong lever for privacy by design, which helps to prioritise projects in terms of key business stakes. For “high impact” projects, risk analysis methods or communication kits for customers or employees can be implemented.

Integrate respect for privacy into business objectives and monitor their application

In order to create an honourable circle of trust within the organisation, business and / or project manager objectives will be determined. Objectives will be based on the monitoring of simple indicators put in place to ensure that respect for privacy is reflected in each business project. For
In addition, GDPR is highly regarded as an international benchmark standard, where it is viewed that ensuring compliance with GDPR will facilitate compliance with other international regulations.

Beyond compliance on a European scale, this programme will also have a regulatory function in monitoring regulatory developments across different countries, as well as developing the GDPR programme itself to ensure a more widely applicable level of compliance.

Best practice n°6
Equip the CIO with tools to protect and monitor data

In order to process data and protect collected data, investment in IT-related solutions are necessary. Such investments will be towards implementing solutions such as anonymisation, data encryption and management of access rights. Investments in cybersecurity, particularly for detecting and responding to incidents related to obligations around customer notification, will also contribute to efforts in challenging cybercrime more broadly.

Best practice n°5
Conduct a compliance programme focused on (but not limited to) GDPR

This programme will organise all the tasks aimed at ensuring compliance with different legal and legislative literature linked to the protection of personal data. The biggest priority over the next two years (by May 2018) will be the implementation of the EU regulation, General Data Protection Regulation (GDPR). This is largely due to the substantial financial impact that non-compliance (fines of up to 4% of global consolidated turnover) can inflict.

example, we can measure milestones or achievements such as evaluating the risks of data processing or the application of measures required for transparency, such as communication with customers. The control and regular reporting of such indicators will contribute to best practice governance with respect to privacy. Incentives may even be introduced by the ethics committee; such as awards for projects demonstrating the most respect towards privacy.
Best practice n°7 Communicate clearly and widely to anticipate concerns and reassure

Concerns that emerge from digital innovation and development require early communication in order to reassure individuals and gain their support for change. Such communications should be transmitted globally, demonstrating the social commitment of organisations with respect to privacy. For example, this may include incorporation into CSR policy, as well as within each project. The reasons for data collection, data processing and the measures taken to ensure safety can be communicated, without the use of legal or technical jargon. Such communications must be prepared to respond to issues or questions raised by customers and employees. Such interactive aspects will be integrated at the project or processing design stage.

Best practice n°8 Remain vigilant and know how to adopt innovation

It is evident that regulatory, technological and use frameworks centred around the subject of protection of digital privacy are changing rapidly.

In order to capitalise on such innovation, observation of regulatory developments and intelligence processes will be necessary. Such initiatives will support approaches based on the rapid adoption of relevant innovation, ensuring effective structural positioning over time.

ORGANISATION IS KEY FOR IMPLEMENTING BEST PRACTICES

Depending on the purpose of organisations and the nature of their actions, the implementation and facilitation of the aforementioned best practices may be conducted by teams responsible for ethics, compliance, legal issues or even supporting the CIO. European regulation requires the appointment of a Data Protection Officer (DPO). Such a role is essential for ensuring compliance by an organisation. Above all, it ensures that the principle of respect for privacy is ingrained within the DNA of an organisation. The impact of a Data Protection Officer’s actions will correspond to his or her reporting lines and the communication made around his or her appointment.
FOCUS:
GDPR COMPLIANCE PROGRAM
AND KEY CHALLENGES

In the situation where an organization has to comply with the GDPR, it will be necessary to initiate a specific compliance program to be aligned with the requirements of the directive. With regard to the large number of those requirements, numerous challenges must be undertaken through several major streams:

/ Global program steering, including the creation of group guidelines interpreting the regulation in the specific context of the company, the coordination of local tasks and the implementation of change management;

/ Compliance with the customers’ and employees’ data requirements, including the production of the inventory of data processing, risk analysis and the associated remediation plan, as well as the roll-out of the consent, information and rights exercise principles;

/ Implementation of the accountability, containing the implementation of audit and control plans, the construction of the Privacy by Design process, reporting to top management and regulatory authorities, as well as the reporting of data breaches;

/ Management of the IT evolutions, comprising the roll-out of portability, cleanse and anonymization solutions.

These challenges require a well defined program organization and an established associated governance: what are the respective roles of the DPO, of the compliance function, of the legal function, of the CIO, of the CDO (Chief Digital Officer), and of the support business lines and functions? This organization will need to be able to centrally pilot, coordinate and equip the program to enable the local implementation of the compliance by the teams directly in touch with the processing.
What would be the 3 challenges to be tackled first and foremost?

**1.** The implementation of Privacy by Design, a pre-requisite to improve over time. It is the obligation to perform risk analyses related to the privacy of individuals (discrimination, dissemination of confidential data, etc) before implementing the most sensitive processing, and with each modification of the processing. Companies will have to adopt appropriate security measures in order to mitigate such risks. Concrete actions to be conducted include an update of the project methodology to identify sensitive processing as soon as possible, as well as the definition of a risk analysis method to be introduced. Support can be found in the practical guides developed by the regulatory authorities, including the CNIL’s “The study of the impact on Privacy”), which will need to be simplified and adapted to the context and specific needs of the company.

**2.** The notification of data breaches, a challenge for the client relationship. The regulation introduces an obligation to report data breaches to the competent authorities. The notification of such data breaches to the concerned individuals is only mandatory if the company is unable to prove that it has taken appropriate steps to make such breaches inconsequential. Hence the benefits gained from a properly carried out risk analysis and from the definition and implementation of appropriate measures. To meet this requirement, two processes will have to be developed or overhauled: the first one is a detection and alert process for data breaches, which will integrate the reporting to the authorities, and a new client relationship process to ensure that, when compulsory, the correct actions will be taken to notify the clients (by email, registered letter, press release...) and to manage subsequent interactions with all stakeholders (questions, complaints...), which will often be dealt with via the implementation of dedicated call centers and the quick training of the relevant parties.

**3.** The adoption of the principle of accountability. Every company will now need to be able to demonstrate its compliance with the regulation. This requirement will be reflected by the implementation of a personal data management framework policy; an associated organization; operational procedures covering the topics of the regulation (information, respect of the rights of the people, transfer to sub-contractors...). The company will also need to be able to prove the application of such policies, and, consequently, to implement audit and control processes.
The future evolution of digital technologies and how they are used, particularly for automation and artificial intelligence, will place even greater importance on personal data. How do we prepare for such developments?
Algorithms and associated digital services do not appear today as neutral and independent actors.

It is therefore necessary to develop trust, at the risk that new proposed services will not be accepted by individuals.

This move is anticipated by major Internet companies such as Amazon, Google, Facebook, IBM or Microsoft, the latter of which recently announcing a partnership to develop artificial intelligence for the benefit of citizens and society, with the immediate involvement of an ethics committee.

... TOWARDS BUILDING TRUST FOR THE FUTURE

For all organisations and companies concerned, trust must be a criteria of differentiation in customer relationships and human resources management.

Meeting the challenge of building digital trust should therefore not be seen as a regulatory or security issue. Rather, it should be seen as an in-depth transformation of the customer and employee relationship and the way in which digital technology is used. This change must be deeply rooted in the foundation of organisations and businesses.

Protecting privacy in today's digital world means doing digital differently.

PROTECTION OF DIGITAL PRIVACY: BEYOND COMPLIANCE...

We have seen on an increasing scale that digital transformation raises concerns related to data protection, as well as to the legitimacy of the purposes for which data are used.

Digital technology is perceived as accelerating, informing and increasing the reliability of the decision-making process. In the future, automated use cases of technology will emerge: for automating financial investment decisions, predicting diseases and finding their cures, autonomous vehicles, not to mention the arrival of robots in everyday life.

However, in order to address this level of automation, it will be necessary to collect data directly or indirectly (via the Internet, from partners, etc.) from individuals. This data will have to be increasingly interconnected in order to facilitate these new uses.

The multiplication of this correlated data combined with the emergence of automation through the use of algorithms understandably provokes fear in individuals about the decisions over which they have no control.

To capitalise on the next stage of the digital revolution, employees and customers will thus have to be prepared to partially or fully delegate decision-making.

Such delegation, as Milad Doueihi claimed, involves the action of entrusting a third party.
The second part of our interview is with Milad Doueihi, American philosopher and Chair of Digital Humanities at Paris-Sorbonne University, placing privacy in the context of a more global evolution of digital culture and its impact on privacy.

In the world of digital technology, the word “algorithm” comes up often. Do algorithms produce unbiased choices or are they like people, with a digital identity?

There is type of a fetishism surrounding algorithms. We have witnessed a shift from the era of data to what we could call algorithmic governance. We are governed, shaped and spied on by algorithms, whether from large corporations or intelligence services. In my view, an algorithm is a digital cultural “being” because it is built by people who make decisions informed by economical or cultural factors, which are mostly implicit. Moreover, such algorithms can produce unexpected or not necessarily programmed results. There is certainly an element of the unknown in the results.

Nowadays, we are faced with the choices suggested by these algorithms, which anticipate what we will be interested in. For example, Facebook will prioritise showing our closest friends’ posts. Does this lead to a restriction of our freedom in exchange for a little more convenience?

Other forms of individual autonomy appear because of increasing levels of automation through algorithms and the gradual removal of classical intermediaries. What is crucial to me is understanding the links between autonomy and automation. Instead of questioning liberty, we should be questioning autonomy. Autonomy is now a method of delegation. We agree to delegate through an established trusted third-party: for example, a friend. Nowadays, we are witnessing a transformation in the way we are autonomous in public spaces, as well as in private and confidential spaces, which is particularly striking to me. The boundary between the two is difficult to determine and maintain.
“Yet, through the blockchain, we will transfer our trust from banks and states and into the hands of the colossal computing and calculation power of machines. This signifies a major shift in delegation”

Can we delegate in a trustworthy manner with current Web tools and digital technologies in general?

In my view, we should master the tools we use and monitor the transparency and loyalty of the algorithms on which they are built. We should understand how algorithms produce recommendations before a decision is made. There is a form of reciprocity between individuals, their interactions and the way that the algorithm functions.

In your view, how should the consequences of digital cultural evolution and private life be taken into consideration by governments and the business world?

Data and its management has become a real factor of trust between people, communities and societies. I believe that states, as is already the case in Europe, should contribute to protect the personal data of its citizens. Such data is meant to be protected by a “jurisdiction embassy”. This means applying rules governed by the citizens’ country of origin and not the country where the data is stored or processed. Sovereignty is at the heart of the problem. In fact, we must surpass the classical juridical sovereignty of states, which is a territorial sovereignty. The data characterising a citizen’s identity should be accompanied by legal frameworks not restricted to location but which are intrinsic to a citizen’s country of origin.

Another solution which seems realistic to me and which can be applied in firms, as well as on a national scale, is to have explicit and accessible customer policies on the way data is handled. We have the right to access, control and appeal the content of our data within legal boundaries. Yet, this principle is not consistently applied.

To conclude, could you share with us what you believe could affect the evolution of digital in years to come, especially related to privacy?

Blockchain seems interesting to me, because it helps to automate and erase the human factor, often considered the weakest element of the chain. Yet, through the blockchain, we will transfer our trust from banks and states and into the hands of the colossal computing and calculation power of machines. This signifies a major shift in delegation.