Ministero dello Sviluppo Economico

G7 2017
ITALIA

ITA
ITALIAN TRADE AGENCY
ICE - Agenzia per la promozione all'estero e l'internazionalizzazione delle imprese italiane

Under the auspices of the Italian G7 Presidency

MAKING THE DIGITAL ECONOMY AND SOCIETY INCLUSIVE, OPEN AND SECURE

Multistakeholder Conference
Turin, 25th September 2017

G7 ICT and Industry Multistakeholder Conference

Executive Summary of the fours sessions’ debate

Session 1 - SMEs and the digital transformation

Background

The Next Production Revolution is now. The combination of new digital and non-digital technologies is reshaping the way goods and services are produced, distributed and sold. Companies have both opportunities and challenges ahead. SMEs are especially threatened by the growing competition, but at the same time they can play a new role thanks to their better integration into global value chains. Policies to further promote knowledge transfer capabilities of universities and research organizations, and also from larger to smaller companies, to the benefit of start-ups and SMEs, as well as solutions to improve technical and managerial skills of the workforce, will be critical for bridging the divergence between innovators and laggards. This would ensure more innovation-driven and inclusive growth.

Key issues

- ❖ How can the Next Production Revolution contribute to a fair, inclusive and sustainable economic development?
- ❖ How can policies avoid the increase of a performance gap between economic sectors and between large companies and SMEs?
- ❖ How should research and technology transfer programmes be organized to increase cooperation between SMEs, start-ups and universities?
- ❖ What are the enabling factors for start-ups to engage with large manufacturing enterprises on a faster commercial track?
- ❖ What are the social challenges in designing policies that sustain the uptake of digital manufacturing?

Conclusions

1. **Impact of digital technologies**: 90% of data in the world today have been created in the last two years at the rate of 2.5 quintillion bytes/day and the number of connected devices is exponentially increasing. As a consequence, Machine Learning and Artificial Intelligence will significantly affect industrial and marketing processes and managerial practices. There will be substantial benefits for SMEs which can rent algorithms from the cloud while machines can learn from data. As a result, we need to be prepared to acknowledge that part of the intellectual work will be replaced by machines.

Session 1 - SMEs and the digital transformation

Conclusions

2. **The need to develop policy frameworks to promote knowledge transfer from universities and research organizations, and from larger to smaller companies and vice versa.** Universities should educate and train talented people and it is well recognized that in most competitive areas of the world there are always outstanding universities able to attract talented students, researchers and also entrepreneurs. But emerging technologies, from additive manufacturing to robotics, from artificial intelligence to blockchains, from neurotechnologies to synthetic biology require to develop a multidisciplinary and cross-cutting approach. As a consequence, new paradigms for research organization and education will be required.
3. **The need to develop policies for reducing gaps and increasing sustainability of emerging technological paradigms from a social, cultural and economic point of view:**

   a. a new emphasis on the transformation of work and the creation of new skills is needed. Competence Centers are an example of collaborative entities which can foster the creation of proper ecosystems to conceive and design new education processes, in order to actively manage the loss of jobs, by creating new opportunities on a large scale;

   b. SMEs should have access to knowledge associated with new technologies and to data needed for creating and sustaining business, in order to avoid divergence among countries and sectors, especially in fast growing fields.

Challenges

→ **understand the new paradigm** of man-machine collaboration and promote policies and regulations to make this new form of interaction beneficial to people and to society

→ **open education** as widely as possible to include all, through flexible pathways and innovative thinking in order to enable all to adapt to yet unknown developments

→ **create Multidisciplinary International Competence Centers** to promote and foster knowledge sharing among universities, research organisations, large and small companies as well as start-ups

→ **use public sector open data** to rethink education models, by promoting adequate investments in Digital/IT technical and executive competences. Important changes in regulation are needed and expected by using a multistakeholder approach.

Session 2 – Datafication, free flow of information and sustainable growth

Background

As the Internet continues to evolve and goods and services produced get more and more digital, the amount of data originating from governments, businesses and citizens is quickly increasing. At the same time, the ability to collect, process and exploit the wealth of data created in cyberspace, including personal data, may favour concentration and greater information asymmetry and invites new thinking on how to preserve fundamentals such as privacy and cybersecurity. **A multi-stakeholder and international approach is needed to ensure the free flow of information**, and to put in place policies, grounded in respect of the rule of law, that reinforce the Internet's openness and its distributed and interconnected nature, while respecting applicable frameworks for privacy and data protection, and strengthening digital security.

Key issues

- Big data: what are they useful for, what are the risks and benefits?
- Is there a real risk of new monopolies and oligopolies on data?
- Do citizens and consumers have trust in seeing the flow of their data - especially personal – going beyond the border of their own country? Is it a real problem?
- What is needed to ensure that data can freely circulate in a secure ecosystem?

Conclusions

Data does more than just enhance efficiency: **it provides a new perspective on reality** i.e. a better understanding on how the world works. The phenomena of datafication can be compared to the 18th century movement, the enlightenment. Datafication is nothing more than enlightenment 2.0: according to the best estimates, the amount of data passed from 0,02 billion in 1987 to 276 billion GB in 2007 – an increase of a hundred-fold - and is now pervasive in the whole society. Thanks to this knowledge, humanity has the opportunity to rethink how to make sense of the world but under one condition.

Session 2 – Datafication, free flow of information and sustainable growth

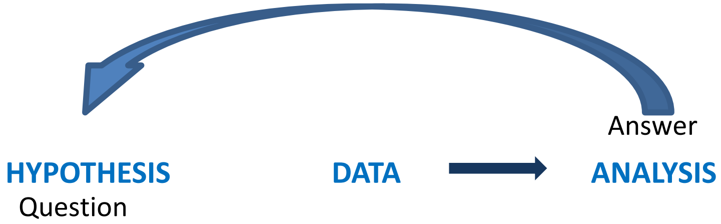
Conclusions

WHEN ONE COLLECTS DATA, HE NEEDS TO KNOW IN ADVANCE WHICH QUESTIONS HE WANTS TO ANSWER

If this precondition is not fulfilled, this person might get the wrong data.

QUESTION → **DATA** → **ANSWER**

So the crucial assumption is: **are we asking the right question?**
What almost everybody does is to start from data this way:



The new perspective
The interesting thing is that **data can be used** in the era of datafication **to stimulate new questions** not just to answer to the existing ones.

At the same time, the value of data is changing. It could be compared to an iceberg where one can only get the data above the sea level. But by revising the data over and over again, **one can capture the hidden value** of the data that is below the water line.
Data will undoubtedly help individuals to personalise their needs. For example, thanks to data it will be possible to customize treatment for an individual's specific needs and he will not be obliged to take an amount of medicine conceived for the average person.

Session 2 – Datafication, free flow of information and sustainable growth

Conclusions

Issues for governments

Looking at the role of data, **on what issue regulatory frameworks should focus**?
The answer is not easy because of the **changing role of data**.
Again, one must ask the right questions:

1. Who has access to data?
2. Who benefits from data?
3. Are markets more competitive with data?
4. Where is innovation generated? If innovation is generated by data who has access to data and who does not?

Session 2 has revealed that if humanity fails to find the answers to these questions concerning the regulatory framework, **datafication risks to empower just the powerful**.
Governments will keep some data non available because of national security issues but they need to understand that the free flow of information is a key element to enable the transition to the digital economy. At present, governments have to solve the problem of the geolocation of their data.
Likewise enterprises and citizens, governments must be reassured that data their is protected. To achieve this goal, International cooperation is the only way to put in place efficient legal frameworks and to spread trust in the digital economy. For this reason, G7 countries have the opportunity to raise and tackle these issues and make progress.

Issues for industry

As nowadays business is distributed, supply chains extend around the globe, people need to work together with the support of performing data systems.
Businesses use data to improve their efficiency and cloud computing is often the answer to access to advanced technologies: by bringing their own data to clouds, enterprises get back several services, on a low-cost basis. This is particularly important for SMEs's inclusion in the digital economy.
Therefore, as enterprises need data, they also need the free flow of information accross borders. According to the firm's perspective, **the issue is not where the data sits or is stored but if data is available, especially through cloud computing**. The message to governments is **to avoid creating artificial barriers to communication**.

Session 2 – Datafication, free flow of information and sustainable growth

Conclusions

Issues for end users/consumers

People are keen to use the digital tools and technologies to share information only if they are reassured about the protection of their data.

The key question: is datafication creating more value?

When it comes to dealing with data and new technologies, people feel they have to be put at the center of the decision making process. In fact, most of the data collected comes from individuals. Often, individuals do not even know that they are sharing personal data concerning their habits, their health, their customer journey, their leisure time, their driving of vehicles, etc. In return, people receive a lot of services for free.

It is important to underline that datafication should not serve only innovation but it should also enrich people's lives. Machine Learning technology helps to build machine translation and objects recognition technologies, especially to improve life for blinds and deafs.

Datafication in fact creates more value but when it comes to set clear rules, policy makers should pay attention to the collection of data from users because they are **engaged in a value exchange** and their perspective should be taken into account. **Data can be collected explicitly or implicitly**, in particular with IoT collecting deeply personal data.

Is it possible (and appropriate) to try to answer to the following questions:

- how can end users retain some control over this exchange?
- how to recover the value back to the end user?
- once the firm has collected information what is its responsability back to the end user?

As users cannot actually do much about it, we are assisting to a backlash of the digital technologies around the globe.

What would be the message to data handlers?

→ **increased accountability**

→ as users do not have the choice in the transaction of data collection, there should be an **ethical responsability**, holding the protection of that data which cannot be arbitrary. The absence of protection is having impacts on the real life of people as data breaches are more and more frequent.

«I, AS END USER, NEED TO HAVE MORE OPPORTUNITY TO PROVIDE MEANINGFUL CONSENT»

Session 2 – Datafication, free flow of information and sustainable growth

Conclusions

What are the models which can inspire an International debate on common policies?

First Example

In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU.

On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the Regulation will enter into force on 24 May 2016, it shall apply from **25 May 2018**. The Directive enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by **6 May 2018**.

The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy.

Second Example

Compared to the EU regulation, Canada has a different concept. A Canadian firm that wants to transfer its own data is responsible for maintaining the integrity of that data. In fact, businesses that engage in the collection, use, disclosure and management of personal information in Canada need to be cognizant of the regulatory framework governing the privacy landscape in order to stay compliant. The data protection regime in Canada is governed by the following four private sector privacy statutes:

a. the Federal *Personal Information Protection and Electronic Documents Act* (PIPEDA)

b. Alberta's *Personal Information Protection Act*

c. British Columbia's *Personal Information Protection Act*

d. Québec's *An Act Respecting the Protection of Personal Information in the Private Sector* (collectively, Canadian Privacy Statutes).

While PIPEDA governs the inter-provincial and international collection, use and disclosure of personal information, it also applies to organizations that collect, use and disclose personal information during a commercial activity that takes place within a province. In addition to these four statutes, Canada has also enacted anti-spam legislation (CASL). Effectively navigating this regulatory system is crucial for companies to maintain legislative compliance with respect to the Canadian Privacy Statutes.

Session 3 – Securing the cyberspace for business

Background

The increasingly wide use of ICTs implies growing risks of cyber incidents that can cause severe disruptions to social activities and major economic damage to businesses. Digital security is a multifaceted policy area, therefore a whole-of-society perspective needs to be adopted, to create the conditions for all stakeholders to effectively manage digital security risk. Governments need to further develop national digital security strategies, and business should include cybersecurity in their risk management strategies. Security standards, cybersecurity frameworks, interoperability and certification schemes, as well as efforts to make cybersecurity less onerous while providing more effective defences, are all strategic points to be addressed.

Key issues

- ❖ How to improve **cybersecurity culture**, in particular for SMEs and citizens? Are there any initiatives in the G7 countries in this field?
- ❖ To simplify the spreading of a culture of defence from cyber attacks, are domestic firms adopting a cybersecurity "common language" among their employees? To which extent domestic companies employ a **cybersecurity framework** to rationalize and plan their security needs? Can the alignment of cybersecurity frameworks adopted by different countries create the basis for an international agreement or regulation?
- ❖ To which extent domestic companies are aware that "**cybersecurity means business**"? To which extent is the risk related to cybersecurity a point of discussion within the executive board?
- ❖ What are the impediments for governments **to raise the level of reliability and safety of the cybersecurity product** as they do for most of the products like cars, trains, aircrafts, etc?
- ❖ One of the most critical points to boost effective cyber risk management processes within a company is **the growth of cyber insurance markets**. What could be the policy and incentives that could help this market take off?
- ❖ One of the main answers to cyber attack campaign is **quick information sharing among public and private sector** as well as **effective early warning systems**. What is the state of the art of this capacity building within G7 countries and at global level?
- ❖ Attacks are carried out through devices with software vulnerabilities. These devices can either become part of an information system managing critical activities for the society or be used to attack a third party. At the moment an efficient and **cost-effective certification scheme does not seem to exist**. Are G7 countries addressing this issue?

Session 3 – Securing the cyberspace for business

Conclusions

Today, the economic and social systems of advanced countries are strongly dependent on cyberspace, meant as the combination of thousands of networks, billions of devices and huge data systems needed to provide essential services to citizens by governmental bodies, Critical Infrastructures, enterprises and the public sector. Blocking business operations, overstepping critical infrastructure services, intellectual property theft, or breach of critical information for company business are examples of the major threats an industrial system has to face. 80% of European companies have experienced at least one cyber-security incident. Figures point out an ongoing attack to the industrial sectors of the G7 countries. In the future, inter-dependency between cyberspace and industry will grow due to several running digital transformation processes such as distributed ledgers, smart cities, industry 4.0, artificial intelligence pervasive robotics just to name a few. This will greatly widen the attack surface of a company.

This session has considered all such aspects by discussing which are the practical and concrete steps the G7 can take to contribute to preserving cybersecurity in domestic or global enterprises. In particular, the dialogue has been centered around the following issue: **how to make cybersecurity less onerous while providing more-effective defenses**.

This means:

- conceptualizing cybersecurity as **a risk management process to be embedded in any public or private organization**

- **using international cooperation to align national cybersecurity programmes** at the political level and **cybersecurity risk management frameworks in private and public sectors**. Alignment of frameworks can boost the adoption of information/processes sharing capability.

Session 3 – Securing the cyberspace for business

Conclusions

Among the multidimensional actions that a national cybersecurity programme has to carry out, **effective public-private partnership has been considered of paramount importance.** The cyber threat cannot be confined either to the public or the private sectors. The attack vectors are the same and they act in the same way, regardless of the targets being public or private. In addition, many public services are managed by private companies.

This is why it is strategic to:

- **develop public-private partnerships to share information and align security processes with the aim to anticipate, detect and recover from an attack**

- foster **International cooperation as key to network all these partnerships** because public-private partnerships have been built mainly in specific market sectors and on a domestic base. The activation of these networks is fundamental to raise the level of security of G7 countries.

Session 4 – Towards a beneficial A.I. in digital society

Background

The development of A.I. technologies has the potential to improve people's lives by helping to solve some of the world's greatest challenges and inefficiencies. The technology progress and the staggering growth of computational power, transmission and storage capabilities, combined with the advancement of machine learning algorithms, is making it possible for machines to work alongside humans in solving complex tasks, opening the way to solutions that have the potential to deeply transform our way of living.

Over the next ten years, given the rapid diffusion of A.I. technologies, we will witness **the transformation of a range of industries**, we will be able to solve complex global challenges such as those related to the environment, urbanization and health, but we will also be faced with a raising number of questions on how to best govern the changes brought by this major technological revolution. To **take advantage of this opportunity, we need new shared ethical values**, that must be elaborated and disseminated and we need to raise awareness of both the future benefits and challenges of A.I.

This effort needs the involvement of all stakeholders - citizens, researchers, policy makers, entrepreneurs, consumers - to build a common understanding and fair development of these technologies.

Key issues

- Which **ethical and social implications** do AI solutions have? How do we achieve a collective awareness of these implications?
- Do we have the tools today **to avoid transforming a great opportunity into a potential threat**?
- How can we encourage **the evolution of A.I. systems with a human centric approach**?
- What should **the role of governments and regulatory bodies** be? How can they direct technological efforts towards global shared goals without curbing them?

Session 4 – Towards a beneficial A.I. in digital society

Conclusions

With 30 billion dollars of investments in 2016 - according to the 2017 McKinsey report on A.I. - A.I. today appears to be out of its past winters. A.I. finally came out of the research labs and universities to have an impact on industry and society. These investments are unevenly distributed geographically – the great majority occurs in U.S. and China based companies - and also across industries as early adopters being mainly the high tech companies.

Despite this success, A.I. might live a new harsh season but not because of technological limitations but because of **the challenge of social acceptability**. In the last century, it took generations to adopt technology whilst at present innovation speeds up the taking on of the new technologies within a few years. However, their impact is absorbed slowly by the society: **disruptive innovation needs to be understood and taken in by citizens, enterprises and policymakers**, and finding a new equilibrium requires time and planning.

Food for thought

The first necessity is **to develop digital skills among citizens and workers to adapt to innovation** and such education requires policy frameworks involving all the stakeholders.

The challenge of making A.I. socially acceptable is not only represented by the loss of jobs. A.I. is already creating jobs in the sphere of creativity and analytics. It is important **to monitor and to be able to intervene at local level** where the impact of job losses might be greater compared to large cities. The benefits of A.I. will be felt more at a global with disruptive effects on environment, transport, distribution, production, health, etc.

Another challenge is **how humans, robots and intelligent programmes can work together side by side**, while still being so different: humans are self directed by goals, use common sense reasoning, base their decisions on values, etc. Machines have more computing power, they are better with math and statistical reasoning, and they can cope with larger sets of data.

Current technology is still very far from human cognition, and even when it gets closer, technology will have to deal with problems such as how to consider the differences in non-universal values and cultures.

Furthermore, it would be more appropriate to use the term "**Augmented Intelligence**", rather than "Artificial Intelligence" to highlight the fact that **intelligent machines are complementary to humans** and can support humans in doing tasks, rather than substituting them. The human-machine teamwork will be successful only if machines can be trusted by humans and the interaction becomes natural. This requires machines to behave ethically especially in the decision making process.

Session 4 – Towards a beneficial A.I. in digital society

Conclusions

Thus, the question is **how intelligent software can provide explanations and justifications on what it is doing and why**.

Another related issue is the **certification of the intelligent software**, as it occurs already with the software of different sectors. It is rather difficult to certify a product that learns and changes its specifications depending on the received data.

The recent main success of A.I. is the development of Machine Learning techniques called Deep Learning. Machine Learning applies statistical reasoning to very large sets of data to extract patterns and make predictions by discovering correlations. However, in this case, these algorithms do not have an explicit model of the field on which they can reason to give causal explanations. In addition to Machine Learning, A.I. also covers areas such as knowledge representation, reasoning, planning, and decision making, where programmes are based on explicit models of the world they work on. Nowadays, research on Machine Learning focuses on accuracy, i.e. on creating algorithms with better performances compared to the human ones.

In the future, the research challenge for scientists will be **to build algorithms that provide explanations, and are not just blackboxes.** The key for governments, industries and practices is to deploy A.I. sensibly with sufficient checks and balances.

Finally, it is interesting to make a **distinction between embodied A.I. and non embodied one**.
The first is related to robots: physical machines governed by intelligent algorithms.
The second to cognitive systems providing services, on the web for example.
In both cases, A.I. is planned for routine work.
Humans are embodied intelligences. This intelligence is deeply rooted in the body - and not only in the brain - and the body is a biochemical system: human intelligence does not exist without it. For example, the neurons of the brain that understand language are strictly correlated to the neurons that govern the movements of the body. Building a system like the human mind integrated with its human body is impossible with the current technologies. For this reason, the risk of an Artificial Intelligence taking over the world is not conceivable at present.
Such remote risk and other real risks are monitored by several multi-stakeholder initiatives, private and public, such as the *Partnership on A.I.* and *OpenAI*, where governments, citizens, industries and other stakeholders gather together to discuss risks and opportunities, to identify regulatory needs, to create social awareness, and to make A.I. beneficial to all.