New Normal: are we ready for it?

Mid-and Long- term impact of ICTs on society: an interdisciplinary analysis

Preamble: It is not under question the added value and the achievements due to digital technology; the aim of this session is to carefully consider potential risks and drawbacks to minimize or counterbalance them.

Digital transformation is reshaping society impacting lifestyles. Are we facing a significant turning point toward a “New normal”? We are increasing leaving the analog, face to face, paper-based world to enter the intangible digital mediated one. The panel analyses the present, mid-, and long-term impacts of this transformation. The pandemic accelerated this process pushing citizens go digital, sometimes forgetting some wise principles. The result is a cyber-based society relaying on “digital”, this pillar is quite fragile, potentially subject to attacks and suitable for top-down discrimination. In the “analogue” world we had different pipelines and “channels” to carry out our activities, thanks to different tools and means, in the cyber world the entire activity depends on a single “bottleneck”: cyber technology. If this pillar fails, does not work properly, or is turned off, our life will have to face problems that are sometimes unpredictable. Without cyber tech we will lose our digital identity, bank account, social security, service provision, news, and much more. Consequently, the more we digitise, the more the attack surface expands, the more vulnerable we will be to hackers and hybrid threats.

The economic model carried out in the recent past shows its limits as does globalisation that was its side effect. Nowadays we increasingly consider de-globalisation as a scenario and the rediscovery of local “values” and “identities”.

A significant part of digital transformation relies on platforms and standards and related “owners”. In the digital transition, despite antitrust laws, there is a potential risk of falling under the control of few key players creating a kind of “oligarchy”.

The Internet distributes all-over the world “homogenised” content that can jeopardise cultural identities. Citizens increasingly live in cyber-bubbles, have cyber-mediated human relations, they experience the world thanks to cyber devices mediated approach, and can be biased by mainstream on opinion dynamics and by nudging.

It is true that platforms open the "global" market to small and micro businesses by offering them a "window" on the globe, but it is equally true that access to global service platforms creates a shortcut between supply and demand shortening the traditional added value chain. This may cause serious troubles in case of unavailability of access to the platforms either due to malfunctions, hackers’ attacks or in the event of a top-down decision to selectively deactivate the service. A plan B in such a situation, if not present, will require long time to implement.

We usually view “security” as an integral part of our lives, seemingly something cost-free, without needing to invest or worry about it. This seems to be true until we face small or large problems. Then we start to worry about security, it is no longer a zero-cost "commodity", we need invest some resources to reach a certain level of "insecurity". The concept of “security” it is not an absolute and permanent status, but we can identify it as a “dynamic balance”. We draw attention to the dual nature of “cyber” which many times contributes to improving resilience but due to its pervasive attitude it can be the target of attacks and generate the "perfect storm".

We are surrounded by “critical infrastructures” managed by cyber components which, in the event of attacks, can create greater or lesser impacts on our daily lives. We don’t just mean the typical critical infrastructures like communication, energy, water, health, transportation, and last but not less important nowadays, financial services. Thanks to the appreciation of citizens and their role as everyday “tools” we consider information services, social media, geo-positioning, home automation, smart cities, safety, and security devices, and more. It will not be

surprising if in a few years key service platforms as GAFAM will be considered critical infrastructures.

The pervasiveness of cyber technology, the internet and the quick deployment of emerging number crunching applications is emphasizing energy consumption, at the same time the rapid pace of innovation in the field of consumers' devices produces significant amount of waste to be recycled or disposed. Consequently, can cyber technology be considered green and resilient?

Since more than two decades we have been wrapped in our personal cyber-sphere in a kind of symbiotic relation. Citizens experience the world thanks to an approach mediated by cyber devices; the "new reality" is the one provided by devices. Metaverse and virtual reality are inter-twined, but they are not the same thing. So far, digital technology has mainly acted as a human isolation technology, computer mediated human relations or even a "loneliness relation" with your terminal, a smart phone, gaming console or laptop.

According to the current perspective the Metaverse will progressively create a clone of our environment, but it will not limit itself to this goal, creativity will extend this limitless universe beyond the imagination. Cyber-loneliness, one of the foreseeable risks, is a sort of addiction to this "parallel life" that trains users to shift from Real- to Meta-life blurring the boundary between them, this can happen as much as the number of services and duties will be "moved" on the other side of the Alice's mirror. Meta-life may propose a new normal that once accepted in the Meta-life could be accepted in the real life (e.g. restriction of human rights).

Will genetic engineering and nanotechnology allow us to escape human limitations, will general artificial intelligence design improve itself to overcame human intelligence? While AI will benefit citizens, businesses, and public interests it will create risks to fundamental rights, potentially liberating humans' beings from ethical dilemmas. AI should be as neutral as possible to cover techniques that are not yet known/developed.

The new ethics calls into question personal free will and freedom of choice; traditional cultural regulators of social relationships and processes are being replaced by automated social algorithms (growing role of algorithms and ML). The extensive use of artificial intelligence, machine learning and big data, in addition to various ethical issues, can led to some significant drawbacks. We feed ML systems mainly with big data from Western countries, sometimes both due to the opacity of the algorithms and the inability to predict the "patterns" identified by the system we receive risky or not useful outputs. Citizens are increasingly using AI "bots" to carry out different activities ranging from writing a poem to creating a deep fake. How can we identify a human "product" from a machine product? Lawyers are already animating the debate together with other interested parties (e.g. IPR issues).

If on the one hand the entire architecture is based on cyber technology, with all the potential risks it entails on the other hand the "rules" of the cyber-world have can express a power that none of the "rules" of history have never had. Information and big data are the assets to be analysed, influenced, reused.

Furthermore, time ago we started discussing about the Global Digital Compact, this was one of the key topics of the WSIS Forum 2023 together with AI tools and their developments. The aim of the debate is to outline a shared vision on digital cooperation providing an inclusive global framework for a sustainable digital future.

The challenges for the upcoming years are the ways to sustain the human's role and the inviolable right to freedom and personal privacy in an era of unlimited collection of information. Once again, the need to find a proper balance between humanities and technologies is omnipresent. Social sciences and humanities must establish a tight cooperation in the design or co-creation of cyber technologies always keeping humans in the focus.