ARE WE LOOKING FOR A "NEW NORMAL"?

Ronchi Alfredo M. – Politecnico di Milano, Italy
Secretary EC MEDICI Framework Foundation
alfredo.ronchi@polimi.it.

Abstract

The paper provides an overview on the "new normal" or "near future society" starting from the most significant events that characterised the evolution and pervasiveness of cyber technology. The impact on security and privacy due to the acceleration of the digital transition during the pandemic and the decision makers wills to go digital sometimes forgetting some wise principles. The goal is to digitise as much as possible reaching a cyber-based society relaying on "digital", this pillar is quite fragile and subject to attacks or suitable for top-down discrimination. Additional potential drawbacks concerning loneliness due to lives spent in cyber-bubbles, cyber-mediation of human relations, citizens experience the world thanks to a cyber device mediated approach, the pandemic busted these effects, the "new reality" is the one delivered by devices, mainstream influence on opinion dynamics and nudging, these are some of the additional aspects considered. Here it comes the potential role of the Metaverse. Accordingly with the actual perspective the Metaverse will progressively create a clone of our environment, but it will not be limited to this goal, creativity will extend this universe without limits apart from imagination. The Metaverse today offers a simplified representation of the "reality" as conceived by programmers. There is an increasing interest in promoting the metaverse as a kind of "new frontier" a territory potentially rich of opportunities for the forerunners. Key players are putting their flags on this territory in a kind of gold rush.

Cyber-loneliness, one of the foreseeable risks is a kind of addiction to this "parallel life" training users to shift from real to Meta-life blurring the border between them, this may happen as much as the number of services and duties will be transferred on the other side of the Alice's mirror. Metaverse can propose a new normal that once accepted in the Meta-life might be accepted in the real life. The same of course is valid for information and opinion dynamics, especially if perceived as real and trustable.
Leveraging on laziness and relaxation citizens spend less time outside home, they have shopping online, they buy food and drinks directly delivered on their table, "meet" friends on Zoom or WhatsApp, interact with the "outer environment" though the mediation of social media and video clips. 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 information gathering. Once again, the need to find a proper balance between humanities and technologies is omnipresent.

This is not a complete overview on the key aspects and trends that appeared in recent times, off course taking into consideration each single technology and trend there are not specific concerns and technology seems simply to ease our daily life but getting much more in depth of each single innovation or putting together all the visible "tiles" of the "new normal" mosaic we can be concerned. In addition, a limited number of companies concentrated in a few areas of the world control the network and key platforms, may we call it oligarchy?

Introduction

We are facing a significant turning point concerning the “Tangible and intangible impact of information and communication in the digital age”, this paper will outline some of the significant changes and concerns due to this impact.

As Klaus Schwab wrote in the preface of his book “Shaping the Fourth Industrial Revolution” in 2016 “*The world is at a crossroads. The social and political systems that have lifted millions out of poverty and shaped our national and global policies for half a century are failing us. The economic benefits of human ingenuity and effort are becoming more concentrated, inequality is rising, and the negative externalities of our integrated global economy are harming the natural environment and vulnerable populations the stakeholders least able to absorb the cost of progress.*” [1 - Schwab 2016]

The turning point we are facing can be termed, in relation to the previous ones, the Fourth Industrial Revolution; the first in the middle of the 18th century enabled the mechanization of activities thanks to steam energy, the second added electric energy to the scenario, the third was activated by computers and the creation of huge datasets, the fourth is based on a portfolio of enabling technologies ranging between cyber, nano and bio. The present document will focus on the cyber one that seems to have the most relevant impact on a large part of society involving privacy, freedom, labour, security, behaviour, etc.

To have a clear vision of the "new reality" and its trend, it is necessary to consider the way in which wealth is generated, no more based on labour and production of physical goods. We will start from the technological evolution together with some relevant events and the impacts that these aspects have had and will have on society. Since some decades we were concerned about the future of “labour”, concerns probably initially represented by the disappearance of some professional roles, e.g., typist assistant, and the never-ending quest for cheaper production costs moving from country to country, the shift from a well-defined set of curricula and skills addressing the needs of production toward a new set of often undefined skills of soft skills required by “services”, “gig economy”, and technology re-invented jobs.

Since a couple of decades, we faced the even improving role of digital procedures and tools reshaping the activities to evolve in the so-called digital transition or probably more meaningful “digital transformation”. “Transformation” gives a better understanding about the outcome; society will be deeply impacted by this process. The economic model carried out in the recent past shows its limits as well as globalisation that was its side effect. Nowadays more often we consider de-globalisation as a scenario and the re-discover of local “values” and “identities”. We do not like anymore the same sandwich or merchandise all-over the world. Therefore, in the western world there is an evident lack of values and beliefs, a clear feeling that there is something “wrong” so in such an uncertain environment without clear references young generations are discovering new “gurus” and trends. The “cancel culture” movement together with the “politically correct” re-evaluation of history and facts in the light of today’s trends and thoughts. The negative impact of man on nature considered the origin of main disasters is generating a widespread feeling of risk for the survival of humanity. Global warming, increasing level of oceans, lack of food and water and last but not the least the pandemic sometimes interpreted as the self-defence reaction of nature. All these aspects impacted society as a mix of incumbent tragedies and an ongoing full reshaping of society, a kind of imminent “new global order”.

Some thinkers foresee the actual extinction of Homo Sapiens, the faith of anti-humanism, begins not with a political program but with a philosophical idea. The flip side, Transhumanism glorifies some of the same things that anti-humanism decries—scientific and technological progress, the supremacy of reason. Genetic

engineering and nanotechnology will allow us to escape human limitations such as mortality and confinement to a physical body. General artificial intelligence design will improve itself to think faster and deeper, then the improved version would improve itself, and so on, exponentially. Both trunks of thoughts basically consider humans' disappearance, on one side extinction on the other cyborg.

This set of concerns capable of generating uncertainty for the future has prompted human beings to seek new development models based on the mitigation of climate change, zero environmental footprint, circular and green economy, and more. The omnipresent digital technology was considered one of the building blocks of this "new normal" even thanks to the relevant contribution that this technology provided on one of the recent crises: the pandemic. Hence, one of the main vectors of this change was associated to the so-called Digital Transition or Digital transformation (DT or DX).

The roadmap of our digital future

Digital transformation is considered the natural evolution of the current society in the light of a pervasive technology like digital technology. Thanks to Tim Berners-Lee and Robert Cailliau, close to the end of the 1980s, the web technology was born at Conseil Européen pour la Recherche Nucléaire (CERN) to ease the information exchange among physicists. In 1995 flourished on the consumer and home markets even thanks to Microsoft motto "Where do you want to go today" outlining the idea of a small world entirely connected online and the move of computers out from the technological corner and nerds' community. Personal computers since that time (1995) moved from the sleeping room of nerds to the living room and kitchen. Internet and Web technology gave to citizens the opportunity to reach multitude of people before reachable only by radio and television, this "one to many" or "many to many" exchanges of ideas opened a completely new scenario both in positive and negative sense. Social media completed the transition toward a completely new way of human relations, probably less solid, empathic, and trustable.

Digital technology is intertwined with almost all the life sectors. Since the dawn of digital technology, the number of application and solutions based on such technology had a surprising rate of growth. Transistors, originally conceived to fight against deafness, were the sparkling light of several new devices, followed by integrated circuits. Computers became ten times smaller and powerful being ten times cheaper. The extended use of computers overlapped more and more any activity generating an impact of society. Let's underline that innovation per se without an impact on society, possibly positive impact, is useless.

Nowadays there is no field of human knowledge that doesn't take advantage or is based on digital: information and communication, education, government, health, energy, mobility, etc.

The full settlement of such pervasive technology is termed digital transformation (DT or DX), governments, international organisation, private companies are all together promoting and facilitating this switch from analog to digital. We are increasingly leaving the analog, face to face, paper-based world to enter the intangible digital mediated one.

We all agree on the meaning of the term "transformation" but "digital" has different meanings. "Digital" is a word that means many things to different people, one might think of going paperless; another might think of data analytics and artificial intelligence; another might picture agile teams; and yet another might think of open-plan offices. A comprehensive definition of the term digital transformation should be the integration of digital technology into all areas of activity, from business to public sector, fundamentally changing how we operate and deliver value to customers or citizens.

As a general assumption the adoption of digital technology represented a true competitive advantage, literally “Competitive advantage refers to factors that allow a company to produce goods or services better or more cheaply than its competitors. These factors allow the productive entity to generate more sales or superior margins compared to its market competitors.” If this is in a nutshell the aim of DT what about the impact on society? Digital Transformation is an opportunity or a nightmare?

Side effects of Cyber Tech Pervasiveness

The incredibly rapid success of the world wide web, mainly due to e-commerce and social media, gave a boost to the globalisation trend, a shift toward uniformity, jeopardising diversities, and cultural identities.

As a follow up of the diffusion at citizens level of web technology and related services, starting from the first decade of the twenty-first century, several Governmental Agencies, Institutions and Private Enterprises from all over the world, both in industrialised and developing countries, invested time and resources on e-Services [2 – Ronchi 2019].

The key element of this success was the cyber element called “platform”, the main component of any kind of service or information delivery. Platforms are mainly “populated” by users, even if they do not pay any fee, considered as customers. They, as “customers”, increase the market value of the platform in the media market because of the advertisements and the ability, among the others, to analyse data and resell customers’ profiles.

This development has been deeply influencing Society. Citizens have been increasingly using the platforms exploring the new possibilities to buy and sell goods online, book their travels and vacations. They also enjoyed social media and several other services, unthinkable before the Internet, from extremely vertical services to crowd services [3 – Surowiecki 2004] or funding. Platforms were the real “silver bullet” that created major opportunities and a real impact on society and economy. A relevant part of digital transformation relies on platforms and standards [4 – Ronchi 2020]. These aspects are directly linked with the “owners” of such platforms and standards.

This can be considered a kind of monopoly not yet regulated - a kind of grey zone. Platforms are mainly private, and the key ones are concentrated in few countries creating a kind of “oligarchy”. The “control buttons” of our daily life are often outside the control of our nation state. So, in the digital transition, despite antitrust laws, there is a potential risk to fall under the control of few key players, Google have a share of around 85.53 percent of the global search engine market, and advertising, Meta stated that 3.81 billion people were using at least one of the company's core products (Facebook, WhatsApp, Instagram, or Messenger), and Amazon holds 37.8 % of the market share[1]. Again shall we call it ”oligarchy”? This aspect was recently outlined by the censorship action of some platforms that cancelled user profiles and entire video channels opening the discussion on the balance of the rights between the owner and the user of the platform.

An additional remark is warranted here. If, on the one hand, the diffusion of platforms creates new opportunities, as it happens with small enterprises or craftsmen, on the other hand, this “kills” several existing businesses. Besides, the platforms open the “global” market to small and micro enterprises offering them a “window” on the globe, and, further, the access to global service platforms creates a shortcut between the offer and demand that cuts out a major part of the traditional added value chain, thereby replacing malls with platforms. This as we will outline later, apart from the disappearance of several working positions, may cause serious troubles in case of unavailability of platforms access both due to malfunctions

[1] Source of data: http://www.statista.com

or hackers' attack and in case of top-down decision to selectively switch off. A plan B in such a situation, if not present, will require long time to be implemented. The role of cyber technology and key services in our everyday life increases, at the same time and even more increases the vulnerability and risk of cyber-attacks.

The dark side of networking

We usually consider "security" as a seamless part of our life, apparently something cost-free, no need to invest or care about it. This seems to be true till we face minor or big problems. Pickpockets take our wallet, thief stole our car or take some of the goods we have at home, hackers kidnap our data or any other event that infringe our "convincement" of "feeling safe[2]".

Then, we start to be concerned about security, it is no more a cost-free "commodity", we need to invest some resources to reach a certain level of "insecurity" quoting Salman Rushdie[3]. Why we say, "level of insecurity"? Because there is not total security or better "*There is no such thing as perfect security, only varying levels of insecurity.*" The concept of "security" it is not an absolute and permanent status, but we can identify it as a "dynamic balance" between a specific "asset" or "assets" to be secured, the specific context, sometimes for a specific time span, the range of potential threats, and more. We pose the focus on the double nature of "cyber" many times it contributes to improve resilience but because of its pervasive attitude it can be the target for attacks and generate the "perfect storm".

As the general concept of security evolved through time even the concept of national security evolved as well as homeland security and, the same happened in case of potential targets and threats. State actors face a very complicated scenario trying to match with the current and future developments of threats based on intelligence, information flow analytics[4], risk assessment, probability[5], and projections. Many times, in this complex and risky scenario, the best or less harmful solution is to refer to the game theory and how to maximise the gain minimizing risks, that doesn't mean to choose the maximum absolute gain. This may led to choices motivated by contradicting goals.

We already faced several relevant attacks due to hackers, some targeting Governmental or Law Enforcement Agencies and Institutions, some targeting critical infrastructures, others targeting big companies. Financial markets may be influenced or tilted by cyber-attacks. Smart cities and grid models must carefully consider cyber security issue, as much as we install IoT and other cyber devices and services as much the risk to be cyber-attacked increases. This mainly because such devices were and are many times not designed to be "secure". The early generations of IoT devices were designed before the Internet and the deployment of hordes of hackers.

What about industrial machinery today fully computerised, or critical infrastructure management; in a cyber warfare scenario it might be enough to dispatch on the network a tag like "sunrise" to collapse the whole target infrastructure[6]. Recently on the World Economic Forum, Jeremy Jurgens [7], foresaw the possibility a global cyber-attack that will take us back to the stone age. Of course, even this message might be a fake news.

---

[2] We did different studies together with our partners from behavioural psychology including tests based on VR simulation of different environments recalling increasing level of insecurity.

[3] Iranian / British writer recently suffered an attempt to kill him in NYC.

[4] E.g. Ronchi Alfredo M., (2018),, TAS: Trust Assessment System, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018

[5] Risk assessment and probability cover even natural risks scenarios that can impact security (e.g. critical infrastructure).

[6] This to do not mention Wanna Cry and the registered domain iuqerfsodp9ifjaposdfjhgosurijfaewrwer gwea.com

[7] "Geopolitical instability makes a catastrophic cyber event likely in the next two years": WEF Managing Director Jeremy Jurgens on the Global Cybersecurity Outlook Report 2023.

We all remember some examples of cyberattacks to lock machineries or energy pipelines. We are surrounded by "critical infrastructures" managed by cyber components that, in case of attacks, may create mayor or minor impact on our daily life. We don't mean only typical critical infrastructures like communication, energy, water, health, transportation, and last but not less important nowadays financial services; due to citizens appreciation 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 surprise if in few years big service platforms as GAFAM will be considered critical infrastructures[8]. In addition, there is a clear need to reconsider supply chains and their resilience. As a first impression the whole cyber environment including CCTV, IoT, tracking tools will ease everyday life and improve security but on the other side the alleged total dependence from the cyber domain represents a significant weakness blending with the widespread lack of digital literacy and cybersecurity awareness among citizens.

The actual trend is to transfer to the digital domain as much as possible any "traditional" process and document, so in a glimpse government procedures and citizens documents and data will flow in the format of bit streams, sometimes, under the pressure of critical events, this process wasn't designed to ensure security. The impact of Digital Transition on cybersecurity due to the boost caused by the pandemic and the increasing number of "digitally divided" citizens forced to "go digital" generated the need to foster a diffuse culture of cybersecurity since the primary schools. On the pandemic cyber technology offered a valuable contribution to ensure "business" continuity; government services, justice, health sector, culture, education not forgetting supply chains and more, they all switched to online procedures.

Governments are planning to transfer, or complete the transfer of, key documents and certificates in digital format thanks to QR codes or digital wallets installed on smart phones collecting documents (ID, Social Security, Medical Folder, Driving licence, Bank Account, ID Pay, etc.), and certifications (vote certificate, vaccinations, etc). All the rest of our personal data are already stored somewhere in our country or abroad thanks to our "buddies" like our smart phone or smart watch. It is true that probably our present and future after the pandemic is and will be different mainly due to the progresses in digital transition and the outcomes of the experience on smart working and video conferencing: less travels, less need to provide offices, and more. The increasing number of different passwords we learned to manage every fifteen days is now almost obsolete, bio metric is gaining more and more relevance in the sector of secure identification, from fingerprints to eye and, more recently, face, even if early face recognition systems tested on the field shown some weaknesses.

The survived "almost" traditional documents will be soon enforced by cross validation thanks to our digital ID. In the "analogue" world we had different pipelines and "channels" to perform, thanks to different tools and means, our activities, in the cyber world the whole activity depends on a single "bottleneck": cyber technology. Consequently, the more we become digitalised, the more we are vulnerable to hackers and hybrid threats. Of course, the overall scenario includes many other aspects and "shades".

Can cyber technology be considered green and resilient?[9]

"Resilience", a keyword recently discovered by governments and media, one of the key sectors is critical infrastructure resilience or cyber disasters resilience. Therefore, even if we use cyber-ranges and simulations

[8] The one we know as GAFAM (Google, Amazon, FaceBook/Meta, Apple, Microsoft) and NATU (Netflix, Tesla, Airbnb, Uber)

[9] This is the title of a workshop organised by MEDICI on the WSIS Forum 2023, participants from different organisations and institutions debated on these topics and agreed on the outcome available at https://www.itu.int/net4/wsis/forum/2023/Files/outcomes/draft/WSISForum2023_OutcomeDocument_20230731.pdf

of any potential cyber-attack there are always new threats due to the creativity of “cyber warriors”. There is a strong need to identify back-up solutions and procedures. Nowadays the key concept is “holistic security”, a “global” approach to security integrating all the different aspects and problems. There is a diffuse need to foster a “culture of cyber-security” starting from kids disseminating sensitive information online to improve their Facebook or Instagram or Tik Tok profiles or to download latest games on their smartphones of tablets. Apps are asking the permission to access our address book, phone, camera, mike and more, they basically take almost full control of what we consider our vault hosting business information, bank account, digital identity, etc.

The almost total dependence from cyber technology represents a significant weakness blending with the widespread lack of digital literacy and cybersecurity awareness among citizens. If this cyber pillar will fail, malfunction or be switched off for any reason, our life will suffer sometimes unpredictable problems, no cyber and consequently physical identity, no bank account and social security, no service delivery, no news, and connection with other “entities”.

The increasing diffusion of cyber devices offers an extended attack surface that requires a similar dissemination of awareness and knowledge. In addition to the blooming of cyber devices, the Internet, block chains, 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?

Impact on Society and Ethical aspects

Digital technology in general had and still have a strong impact on society and the pandemic accelerated and amplified such impact especially on young generations. Social media, global content providers are “training” young generations offering a “unified global” approach, this will impact future generations and their cultural identity. Leveraging on laziness and relaxation citizens spend less time outside home, they have shopping online, they buy food and drinks directly delivered on their table, “meet” friends on Zoom or WhatsApp, interact with the “outer environment” though the mediation of social media and video clips. These aspects are even more evident in young generations that add to the social media the gaming dimension. Of course, such trends are even amplified by other media such as television and news.

Considering the ontology point of view Cyber Technology is a new entity, a new class of objects. Cyber data can be duplicated without any difference (cloned) and transferred on the fly through networks. These properties made cyber objects difficult to manage on the legal side and even created some ethical problems. Philosophers and experts in humanities debated for a long time to identify the “original” in digital data. One of the assumptions is that original data are the ones just created in the computer’s memory. Nevertheless, in the early times of Xerocopies “originals” use to be signed in blue or green ink to make the reference document easy to identify.

In the age of “digital originals” the issue of “authenticity” and “originals” has been amplified and several tools and standards were created to solve the problem in contracts, reports, instructions, technical drawings and more. One of the latest solutions is based on blockchains, nice to be back thanks to innovation. Nevertheless, in many cases, there is a real or virtual lack of legislation, virtual because situations apparently new can lead us back to the original.

Probably the standpoint of humanities was considered because the web technology has opened the use of the Internet to the multidisciplinary group of users. Information Ethics was one of the issues [7 – IFAP]. On

the first phase of the WSIS (World Summit on the Information Society) held in Geneva in 2003, a specific working group was created. This later became a WSIS Action Line that has brought out C10 "Ethical Dimensions of the Information Society" [8 – UNESCO WSIS] and some other relevant documents, like the "Code of Ethics for the Information Society". The existence of knowledge "silos" unable to cooperate because of the different knowledge backgrounds and skills has been recently broken. Therefore, in the last decade, philosophers and humanists started to professionally deal with computer scientists and innovators [9 – Stuckelberger 2018]. These scholars usually considered the medium and long-term impacts of technologies on society. The emerging technological trend in autonomous vehicles, robots, machine learning and artificial intelligence may pose significant ethical problems to innovation.

Since more than two decades we are wrapped in our personal cyber-sphere in a kind of symbiotic relation. Citizens experience the world thanks to a cyber device mediated approach; the "new reality" is the one delivered by devices. A short and uncomplete list of impacts on society[10] due to DT may include freedom of expression[11], opinion dynamics & social networks[12], decision making[13], business[14], and commerce[15].

More impacts

As already outlined in a previous document[16] "cyber-loneliness, one of the foreseeable risks is a kind of addiction to this "parallel life" training users to shift from real to Meta-life blurring the border between them, this may happen as much as the number of services and duties will be transferred on the other side of the Alice's mirror. Meta-life can propose a new normal that once accepted in the Meta-life might be accepted in the real life. The same of course is valid for mainstream information and opinion dynamics, especially if perceived as real and trustable."

Opinion formation is a complex and dynamic process mediated by interactions among individuals in social networks, both offline and online. Social media have drastically changed the way opinion dynamics evolve, in any case, they provide a reservoir of data for the study of opinion dynamics on social networks. Social media have become a battlefield on which opinions are, often violently, exchanged. In turn the behaviour of social media has become an important early indicator of societal change. In the "new reality" there is a concrete and present risk to manipulate opinions thanks to digital media as well as to impact the decision-making process.

The extensive use of Artificial Intelligence, Machine Learning and Big Data, apart from several ethical issues, can led to some relevant drawbacks. As an example, let's consider "nudging". The progress of AI has made it possible to develop much more powerful nudge mechanisms thanks to the effectiveness of statistical and inferential AI systems. The impact of AI powered technology on human autonomy is huge. AI-enhanced nudges reinforce the ability to achieve the designer goals using cognitive biases, emotional impulses, and other human behavioural mechanisms both intentionally and unintentionally.

---

10 Refer to [10 – Juul 2019], [11 – Martins 2009], [12 – Peralta 2022]

11 A typical infringement of freedom of expression is the establishment of a "commission" in charge for the fight against fake news, the one owning the "truth", the risk in an "information society" is to cancel debates, silence alternate views and take a dangerous drift towards the "Pensée unique" or single thought in addition to the "single training".

12 The potential role of digital media in shaping the opinions, they represent a relevant part of how we perceive reality and interpersonal relations.

13 let's consider "nudging". The concept of nudge is already used in digital systems even if the nature of the mechanisms that characterise it is not always consistent, and some uses overflow into practices already prohibited by current legislation.

14 Traditional digital technology offered the opportunity to create and test 3D models turning physical object into digital data sets the fourth industrial revolution enables the reverse from digital data sets we can print out in 3D physical objects.

15 An outcome of the merge of big data analytics and behavioural psychology is Internet of Behaviours (IoB) [13 – Joinson 2004]. A very rough description of the IoB is the mash-up of three disciplines: Cyber Technology, Data Analytics, and Behavioural Psychology (Emotions, choices, augmentations, and companionship) [14 – Egger 1996].

16 Ronchi A. (2022). Metaverse and shared immersive virtual realities, proceedings IV International Conference
Tangible and Intangible Impact of Information and Communication in the Digital Age, UNESCO IFAP Moscow, Russian Federation

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 information gathering. 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 designing or co-creation of cyber technologies always keeping humans in the focus.

The post DT "New Normal"

This is not a complete overview on the key aspects and trends that appeared in recent times, off course taking into consideration each single technology and trend there are not specific concerns and technology seems simply to ease our daily life but getting much more in depth of each single innovation or putting together all the visible "tiles" of the "new normal" mosaic we can be concerned. If on one side the whole architecture is based on cyber tech, with all the potential risks it implies, on the other side cyber-world rules have can express a power that no one of the "rules" in history had, information and big data are the assets to be analysed, influenced, reused. Some authors call them "the new oil" but this type of "oil" can be used, abused, and misused many times.

Furthermore, more recently we started to discuss about the Global Digital Compact, this was one of the key topics on the WSIS Forum 2023 together with AI tools and their developments. "The Global Digital Compact that would set out principles, objectives and actions for advancing an open, free, secure and human-centred digital future, one that is anchored in universal human rights and that enables the attainment of the Sustainable Development Goals." The aim of the debate is to shape a shared vision on digital cooperation by providing an inclusive global framework for a sustainable digital future. We hope that the outcome of this debate will fully represent what is expressed in the statement above.

References

1 *Klaus Schwab. "Shaping the Fourth Industrial Revolution", World Economic Forum 2016*

2 *Ronchi A.M. (2019). e-Services: Toward a New Model of (Inter)active Community, ISBN 978-3-030-01842-9, Springer (D)*

3 *Surowiecki J (2004) The Wisdom of crowds: why the many are smarter than the few. Doubleday, Anchor.*

4 *Ronchi Alfredo M., (2020). Digital transformation, proceedings ICCC New Delhi, Cyberlaw ISBN:978-0-385-50386-0*

5 *Ronchi A.M., (2019), e-Citizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer (D)*

6 *Ronchi A.M. (2019 D) e-Democracy: Toward a New Model of (Inter)active Society, ISBN 978-3-030-01595-4, Springer (D*

7 *(IFAP), Information Ethics, http://www.unesco.org/new/en/communication-and-information/intergovernmental-programmes/information-for-all-programme-ifap/priorities/information-ethics/*

8 *UNESCO and WSIS, Ethical dimensions of the Information Society (C10), http://www.unesco.org/new/en/communication-and-information/unesco-and-wsis/implementation-and-follow-up/unesco-and-wsis-action-lines/c10-ethical-dimension-of-the-information-society/*

9 *Christoph Stuckelberger, Pavan Duggal (2018), Cyber Ethics 4.0: Serving Humanity with Values, ISBN 978-88931-265-8, Globethics net*

10 *Juul, J. S. and Porter, M. A. (2019). Hipsters on networks: How a minority group of individuals can lead to an anti-establishment majority. Phys. Rev. E, 99:022313.*

11 *Martins André C.R. et Al., An opinion dynamics model for the diffusion of innovations, Physica A 388 (2009) 3225–3232*

12 *Peralta Antonio, et Al. (2022), Opinion dynamics in social networks: From models to data, Handbook of Computational Social Science*

13 *Joinson Adam (2004) Internet Behaviour and the Design of Virtual Methods, http://www.joinson.com/home/pubs/02%20Virtual%20methods021-34.pdf*

|4 *Egger O. at al. (1996) Internet behaviour and addiction, Swiss Federal Institute of Technology*

15 *Ronchi A. (2022). Metaverse and shared immersive virtual realities, proceedings IV International Conference Tangible and Intangible Impact of Information and Communication in the Digital Age, UNESCO IFAP Moscow, Russian Federation*