Cyberworld and Jurisprudence: looking for a golden balance

Alfredo M. Ronchi
Politecnico di Milano, Piazza Leonardo da Vinci 32, Milano, 20133, Italy
Tel: +39 393 0629373, Email: alfredo.ronchi@polimi.it

Abstract: This 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. It is not under question the added value and the achievements due to cyber technology (societal, intellectual, etc.); we look at cyber technology from the humanities side. Posing our focus on processes that have led to governance agreements. Starting from internet governance, ongoing digital transformation to reach AI Governance Ethics and a selection of experiences carried out by international organisations, nations and single states. Digital transformation is reshaping society impacting lifestyles. The desire of decision makers to go digital, sometimes forgetting some wise principles. The goal to digitise as much as possible reaching a cyber-based society relaying on "digital", this pillar is quite fragile, potentially subject to attacks and suitable for top-down discrimination. Additional potential drawbacks due to lives spent in cyber-bubbles, cyber-mediation of human relations, citizens experience the world thanks to a cyber device mediated approach, mainstream influence on opinion dynamics and nudging. Here it comes the potential role of the Metaverse. 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.

Keywords: Digital Transformation. E-Services, Human Rights, Laws, Regulations, Privacy, Cyber Ethics, Artificial Intelligence, Machine Learning.

Setting the scene

"The world is at a crossroads ... "[1] we are facing a significant turning point based on a portfolio of enabling technologies ranging between cyber, nano and bio. This document will focus on "cyber" and the impacts of this sector on society and its regulatory/legal framework.

The omnipresent digital technology was considered one of the building blocks of this "new global order" hence, one of the main vectors of this change was associated to the so-called "*digital transformation*" (DT). Digital procedures and tools are reshaping, since a couple of decades, citizens' activities; society will be deeply impacted by this process.

Side effects of Cyber Tech Pervasiveness

Thanks to the diffusion of web technology governmental agencies, institutions, and private enterprises from all over the world invested time and resources on e-Services [2 – Ronchi 2019]. The key element to deliver such services is the cyber element termed "platform". Online services have profoundly affected Society. Citizens are 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, including crowd services [3 – Surowiecki 2004]. A relevant part of digital transformation relies on platforms and standards [4 – Ronchi 2020] and it is intertwined with the "owners" of such

[1] As Klaus Schwab wrote almost twenty years ago in the preface of his book "Shaping the Fourth Industrial Revolution" [1 - Schwab 2016].

platforms and standards. This can be considered a kind of monopoly not yet regulated - a “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 “private” key players.
It is true that platforms open the “global” market to small and micro enterprises offering them a “window” on the globe, but at the same time platforms create a shortcut between offer and demand that cuts out a major part of the traditional added value chain. This apart from the disappearance of several working positions, may cause serious troubles in case of problems in accessing platforms both due to malfunctions or hackers’ attacks and in case of top-down decision to selectively switch off the service. A plan B in such a situation, if not present, will require long time to be implemented.

The dark side of networking

We usually consider “security” as a seamless part of our life, apparently something requiring zero- efforts and cost, in our mind there is no need to invest or care about it. This seems to be true till we face minor or big problems that break our “conviction” of “feeling safe[2]”. Then security it is no more a zero-cost “commodity”, we need to invest some resources to reach a certain level of “insecurity”[3]. 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 much the role of cyber technology and key services in our everyday life increases, as much at the same time and even more increases the vulnerability and risk of cyber-attacks.

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. 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. 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.

[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] Quoting Salman Rushdie Iranian / British writer recently suffered an attempt to kill him in NYC. 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.
[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).

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). 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 transformation 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. The survived "almost" traditional documents will be soon enforced by cross validation thanks to our digital ID. 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 [5 – Ronchi 2024].

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". Some of the recent events show the possibility to hack a huge number of IoT devices generating impressive large-scale problems/disasters.
The early generations of IoT devices were designed before the Internet and the deployment of hordes of hackers.

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. This pillar is quite fragile and subject to attacks or suitable for top-down discrimination. If this pillar will fail, malfunction or be switched off our life will suffer sometimes unpredictable problems, no cyber and consequently no digital identity, no bank account and social security, no service delivery, no news, and connection with other "entities".

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]. On the World Economic Forum 2024, 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.
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 as critical infrastructures. 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. There is a diffuse need to foster a "culture of cyber-security" starting from kids

[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.

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

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. Nowadays the key concept is "holistic security", a "global" approach to security integrating all the different aspects and problems. The more we become digitalised, the more the attack surface will extend, the more we are vulnerable to hackers and hybrid threats.
There is a need, again, to agree on a "global" regulatory framework concerning the whole cyber universe ranging between IPRs to cybercrimes.

Impact on society and ethical aspects

Social media, global content providers are "training" young generations offering a "unified global" approach, this will impact future generations and their cultural identity. This is surely one of the first impacts on society potentially shaping a "standard citizen" at least in the western world.
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 [6 – 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" [7 – 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 [8 – 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.

Metaverse and cyber loneliness

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. 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. Metaverse [9 - Ronchi, 2022] and virtual reality are inter-twined, but they are not the same. Digital technology till now has mainly acted as a human insolation technology, computer mediated human relations or even a "loneliness relation" with your terminal, a smart phone, gaming console or laptop. It happens that friends sitting around a table at breakfast or lunch do not interact among them but watch their smartphones sending messages or browsing the web sites. A short and

uncomplete list of impacts on society due to DT may include freedom of expression[9], opinion dynamics & social networks[10] [10 – Juul, 2019] [11 – Martins, 2009] [12 – Peralta, 2022], decision making[11], business[12], and commerce[13].
The Metaverse today [13, 14 – Weiser, 1993, 1994] offers a simplified representation of the "reality" as conceived by programmers. 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. As already outlined in a previous document[14] "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 [15 – ISPI 2023] 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, they 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.

Artificial Intelligence and Machine Learning

Among the different technologies offered on the shelf of digital transition one of the most promising and concerning is surely Artificial Intelligence (AI) and its rich set of sister applications.
We don't know if the concerns often related to AI, considered a potential cyber-Leviathan dominating humanity thanks to its high "intelligence" far exceeding any human one, is due to the term that was associated long time ago to the early studies and applications in this field. The term artificial intelligence generates the idea that this technology will compete and exceed the human one thanks to the ability to self-improve even recursively.
Apart from the nightmares often generated by Sci Fiction movies like, War Games, Eagle Eye or even Lucy[15], this set of technologies has generated the need to regulate both the development and the deployment of its applications. Both experts in the field and governmental bodies are asking to issue specific regulations and laws, one of the most relevant voices in this field was due to San Altman "OpenAI's Sam Altman Urges A.I. Regulation in Senate Hearing" [May 2023]

[9] 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".
[10] The potential role of digital media in shaping the opinions, they represent a relevant part of how we perceive reality and interpersonal relations.
[11] 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.
[12] 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.
[13] 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].
[14] 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
[15] Science fiction movies already proposed similar scenarios e.g. Wargames (1983 American techno-thriller film directed by John Badham) or Eagle Eye (2008 American action-thriller film directed by D. J. Caruso), Lucy (2014 French Sci Fi movie written and directed by Luc Besson)

or a newspaper level “The world wants to regulate AI but does not quite know how” [The Economist - Oct 24th, 2023].

The key questions concerning similar problems are:
- How to achieve precautionary/protective regulatory goals regulating AI design. Use & autonomy without stifling a jurisdiction’s competitive advantage?
- At which level does ought AI be treated “as IF” a morally considerate agent & how would that impact regulatory options? (assigning legal personality does not address the issues Mc Donald’s is a legal person, but is not morally considerate)
- Should issues arising from any eventual authentic emerging moral considerateness be integrated into regulatory approaches now?

To better understand the range of concerns and the willingness to regulate a short list of shared and contrasting underlying concerns is:
- Security (homeland/national & defence secrets, military, space, weapons, infrastructure, financial systems, personal information, political processes/elections, commercial secretes, biosecurity),
- Discrimination and BIAS in health, any selection process, procurement, justice, policy, regulation, broadly anything AI may be involved with,
- AI Moral responsibility – feel released from a personal ethical analysis and related responsibilities,
- Information - Oversight – Misinformation, disinformation, disapproved information filtering, nudging, opinion formation,
- Privacy, human rights & civil liberties protections
- Commercial advantage e.g. promoting national industry – via different methods
- Protection of System and Information Integrity programs from being hijacked
- Consumer protection – liability for harmful products

Some of the ad hoc approaches to the concerns are:
- Mixed frameworks national security, commercial advantage, justice, biosecurity,
- Shared preventative (but generally not extending to precautionary) focus-too late for after the fact liability to be effective.

Possible integrating framework:
- Traditional commercial liability for programme creators (downside v/s preventative effectiveness),
- Environmental law preventative frameworks (down sides v/s competitive or innovative advantage),
- Graduated “AI” focused liability as with other independent actors.

Ethics and Artificial Intelligence

To contextualise the topics described in the next paragraphs it is proper to start from the two terms composing the title of the present paper: Ethics and Artificial Intelligence.
Ethics, in a very basic definition, is one of the branches of philosophy that concerns human behaviour. The term Ethics finds is root / etymology in the ancient Greek term “ἦθος,” (ethos), this term refers to the characteristic spirit of a culture, era, or community as manifested in its beliefs and aspirations.

The term Ethics is often associated with the term Moral as in the case of ethics as Moral Philosophy, the philosophical study of the concepts of moral right and wrong and moral good and bad. Ethics subject consists of the fundamental issues of practical decision making, and the ultimate value and the standards by which human actions can be judged right or wrong.
The term Moral is often associated with religions, cultures, professions, or virtually any other group that is characterized by its moral outlook (e.g. Medical Doctors, Biologists, Judges, Engineers). Philosophers developed their approach to ethics as part of their theory starting from the early stages of thinkers. At the Roman age we can mention the treaty "De finibus bonorum et malorum (*On the Supreme Good*)" [16 – Cicero 45 b.c.].
How it happened that ethics entered the cyber domain? Since the origin of computer science there was apparently no relation between this branch of human knowledge and philosophy, ethics and more in general humanities. Computer science seemed to do not impact on society at least not enough to generate interests or concerns by humanists, something happened at the birth of the World Wide Web. Since the early stages, the WWW attracted knowledgeable people from a wide range of cultural sectors. At least since that time the humanism entered the world of computer science. A turning point was probably the World Summit on the Information Society held in Geneva ten years later in 2003 mainly thanks to the multistakeholder approach that involved in the process civil society and a large set of expertise including humanities, a specific interest was devoted to Cyber Ethics and to pursue a human centred approach [8 – Stuckelberger 2018].
Cyber Ethics become one of the relevant topics to be discussed and addressed, this led to the creation of a specific action line "AL10 Ethical dimensions the Information Society" that since that time, working in tight cooperation with other action lines, represents the humanism side of cyber technology. More recently thanks to the activity carried out both within the WSIS Forums and some research centres[16] the focus has been extended to the whole Digital Humanism.

Having introduced the first term, Ethics, we need to focus on the second one, Artificial Intelligence. Considering the ontology point of view Cyber Technology is a new entity, a new class of objects. In the last decade, philosophers and humanists started to professionally deal with computer scientists and innovators. 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.
After the previous interest in the 1980s, sometimes evoking the negative role of this branch of technology, the trend concerning the "reborn" AI and ML is generating concerns. If on one side AI will benefit citizens, business and public interests on the opposite side creates some risks for the safety of consumers and users, for fundamental rights, potentially releasing humans from ethical dilemmas. Some scholars suggest that the definition of AI should be as neutral as possible to cover techniques which are not yet known/developed. The overall aim is to cover all AI, including traditional symbolic AI, Machine learning, as well as hybrid systems.

How can be defined AI? On the legal side we can refer to the "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"
"The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial

16 Vienna manifesto : **tps://caiml.org/dighum/dighum-manifesto/**

intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action."
While "the term "AI model" means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs."

The European Commission provides a different definition of AI, EU Regulations adopt a risk-based approach to regulation. "'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;"
The European Commission clearly distinguish between "simpler traditional software systems or programming approaches ... that are based on the rules defined solely by natural persons to automatically execute operations. A key characteristic of AI systems is their capability to infer".

China is investing relevant resources to lead the AI domain. One of the definitions of AI due to Chinese researchers is "*Artificial intelligence (AI) aims to mimic human cognitive functions and execute intellectual activities like that performed by humans dealing with an uncertain environment.*[17]". The Chinese approach to this technology is in line with Chinese culture and foresees, in recent rules, that AI must always be under human control (since the advent of Generative AI as a precautionary approach). Positive duties for applications to promotes social cohesion, additional regulations prohibitions on algorithms that create division.

Benefits and drawbacks

No doubt that AI can benefit society performing an incredible number of duties including duties almost impossible to be performed by other means like big data analytics aimed to identify potential patterns, as it happens in health sector and biology, or decoding of ancient inscriptions in unknown languages. Concerns on AI start to focus if we consider potential bias (e.g. gender, culture, etc.), automated non supervised decisions, autonomous vehicles behaviours (land, air, water) in case of crisis and related responsibilities, impacts of general artificial intelligence, ethical data sourcing use, analytics and reuse, this to do not mention malicious use of AI to exploit resources, leverage on deep fakes and nudging, influence opinion dynamics and perform high-end social engineering. An additional aspect to be carefully considered is the quality and origin of data used to feed and train the system; these data will directly influence the outcome. Here it comes the role of supervised or not supervised systems and the opportunity to intervene as humans in the automatised decision making process. Automated decision systems based on AI are many times part of a network of sensors and actuators, the design of such solutions must carefully consider malfunctions of one or more devices and behave properly (e.g. alerting humans and activating risk mitigating procedures).

Safety and security standards for such devices are not set actually; a typical ethical dilemma refers to how will two cars behave in case of imminent collision. The algorithm must decide which one of the two can be sacrificed the one with a baby or the other with a grandfather?

17 Chen Shuang - School of Chinese Medicine, University of Hong Kong, Hong Kong 999077, China

which will be the decision of the algorithm and what about the implemented logic? There might be a "creative" solution due to human mind? How much technology and A.I. overlap moral and ethical aspects? This example depicts even the potentially different "logics" due to different cultural models (eastern / western). Among the others, a potential ethical concern could be the idea to solve serious ethical dilemmas simply referring to an AI proxy to receive suggestions on how to behave and feel released from a personal ethical analysis and related responsibilities e.g. in the health sector.
We feed ML systems mainly with big data from western countries this can lead, as happens in case of minoritized languages, to the disappearance of other "intelligences", how to remove biases in machine learning models that could potentially discriminate against under-represented groups. Citizens are increasingly using AI "bots" to carry out different activities ranging from writing a poem to creating a deep fake. If spell and grammar checkers have already created new dialects/languages, e.g. MS-English, AI is now generating one or, may be, multiple "creativities" accordingly with data that fed the system. On AI for Good international event the UNESCO session dealing with this problem proposed to create several AI systems fed with different cultural models to ensure equal opportunities to different cultures.
More at practical level GPT can support businessman creating an almost perfect contract but, due to its training, this will be generated accordingly with the US regulations. Nowadays we can compare this outcome with a similar one produced by DeepSeek, the Chinese competitor in the race to rule the AI domain.
Having timely identified the potential relevance of AI both at innovation and national soft power and security level, some country devoted a specific ministry to Artificial Intelligence[18].

Is there a need to create a global AI regulatory framework?

The following paragraphs will provide a short overview on relevant recent developments.

UNESCO

UNESCO launched the AI Initiative[19] and published different reports on this topic including UNESCO Generative AI, UNESCO Generative Ai in Education[20], and more[21].
IEEE published Ethically Aligned Design[22], a vision for prioritizing human well-being with autonomous and intelligent systems. Similar initiatives were due to GPAI The Global Partnership on Artificial Intelligence, OECD Artificial Intelligence and Robotics, and UNICRI United Nations Interregional Crime and Justice Research publication "Toolkit for Responsible AI Innovation in Law Enforcement[23]" or "AI for Safer Children".

18 The Vice President and Prime Minister of the UAE and Ruler of Dubai, Sheikh Mohammed bin Rashid Al Maktoum established the State Ministry of Artificial Intelligence and appointed as Minister Omar Sultan Al Olama. Under this Ministry United Arab Emirates are developing several initiatives to promote AI studies and expertise as "Learning Artificial intelligence" and "The National AI Strategy 2031"

19 https://www.unesco.org/en/artificial-intelligence/recommendation-ethics?hub=32618

20 https://www.unesco.org/en/articles/generative-artificial-intelligence-education-think-piece-stefania-giannini

21 https://www.unesco.org/en/artificial-intelligence

22 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9398613

23 https://unicri.it/topics/Toolkit-Responsible-AI-for-Law-Enforcement-INTERPOL-UNICRI

OECD

The OECD in 2019 published one of the first document providing some basic guidelines to regulate AI technology "Recommendation of the Council on Artificial Intelligence"[24] that become a key reference globally, including the definition of an AI system provided "Artificial Intelligence (AI) is a general-purpose technology that has the potential to: improve the welfare and well-being of people, contribute to positive sustainable global economic activity, increase innovation and productivity, and help respond to key global challenges. It is deployed in many sectors ranging from production, education, finance and transport to healthcare and security."
At the end of 2023, the OECD has decided to play its part, leveraging its unique cooperation infrastructure and convening power to support and foster a positive and proactive message about AI and privacy. The OECD active cooperation across borders, sectors, and areas of expertise is evident. The key role of OECD is to act as an observer and an historical partner of Global Privacy Assembly (GPA) that is a reference global network of Privacy Enforcement Authorities (PEAs) together with the Council of Europe (CoE).
In early 2024, the OECD formally launched the OECD.AI Expert Group on AI, Data, and Privacy, bringing together leading AI and privacy experts worldwide (data protection authorities, policymakers, industry, civil society, and academia). The OECD policy observatory published the 2024 OECD AI principles update[25]. The OECD Ministerial Council Meeting held the same year offered the opportunity to update the principles on AI governance established for the first time in 2019, the already mentioned first intergovernmental standard. The 2024 update considers new technological and policy developments, ensuring they remain robust and fit for purpose. The updated principles now address emerging challenges with an enhanced focus on safety, privacy, intellectual property rights and information integrity.
These principles defined the basis for innovative, trustworthy AI respectfully considering human rights and EU democratic values. Up to now we count 47 countries that adhere to these Principles.
The role of these Principles is to provide recommendations and guidelines to policy makers. This process allows the creation AI risk frameworks, building a foundation for global interoperability between jurisdictions.

The principles are based on shared values and can be summarized:
- Inclusive growth, sustainable development and well-being (Principle 1.1),
- Human-centred values and fairness (Principle 1.2),
- Transparency and explainability (Principle 1.3),
- Robustness, security and safety (Principle 1.4),
- Accountability (Principle 1.5).

Coping with these principles we find recommendations for policy makers such as: Investing in AI research and development (Principle 2.1), Fostering a digital ecosystem for AI (Principle 2.2), Shaping an enabling policy environment for AI (Principle 2.3), Building human capacity and preparing for labour market transformation (Principle 2.4), International co-operation for trustworthy AI (Principle 2.5).

[24] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
[25] Care of Juraj Čorba, Audrey Plonk, Karine Perset, Yoichi Iida

As stated by OECD "The Principles serve as a benchmark for responsible AI development and a critical checklist to address these rapid changes effectively, ensuring that AI continues to benefit society without compromising standards and safety."
In addition, as already mentioned, there are some core aspects such as interoperability of AI and the definition of AI systems and its lifecycle.

The typical life cycle is composed by: Design, Development, Deployment[26].
"*The **Design phase** consist in three main steps:*
Understand the problem: To share your team's understanding of their mission challenge, you first have to identify the key project objectives and requirements. Then define the desired outcome from a business perspective. Finally, determining AI will solve this problem. Learn more about this step in the framing AI problems section. (No AI solution will succeed without clearly and precisely understand the business challenge being solved and the desired outcome.)

Data gathering and exploration: This step deals with collecting and evaluating the data required to build the AI solution. This includes discovering available data sets, identifying data quality problems, and deriving initial insights into the data and perspectives on a data plan. (Data is the foundation of any AI solution. Without clearly understanding of the data required and the make-up of that data, a model cannot use it.)

Data wrangling and preparation: This phase covers all activities to construct the working data set from the initial raw data into a format that the model can use. This step can be time consuming and tedious but is critically important to develop a model that achieves the goals established in step 1. (Data preparation is often the hardest and most time-consuming phase of the AI lifecycle.)

*The **Develop phase** consist in two main steps:*
Modelling: This step focuses on experimenting with data to determine the right model. Often during this phase, the team trains, tests, evaluates, and retrains many different models to determine the best model and settings to achieve the desired outcome.
The model training and selection process is interactive. No model achieves best performance the first time it is trained. It is only through iterative fine-tuning that the model is honed to produce the desired outcome. Learn more about types of machine learning and models in Chapter 1. Depending on the amount and type of data being used, this training process may be very computationally expensive meaning it requires special equipment to provide enough computing power and cannot be performed on a normal laptop. See Chapter 5 to learn more about infrastructure to support AI development.

Evaluation: Once one or more models have been built that appear to perform well based on relevant evaluation metrics, test the models on new data to ensure they generalize well and meet the business goals. As this step is particularly critical, we discuss it in much greater detail in the test and evaluation section.

*The **Deploy phase** consist in two main steps:*

[26] Source "Center of Excellence AI Guide for Government: a living and evolving guide to the application of artificial intelligence for the U.S. federal government. https://coe.gsa.gov/coe/ai-guide-for-government/understanding-managing-ai-lifecycle/

Move to production: Once a model has been developed to meet the expected outcome and performs at a level determined ready for use on live data, deploy it into a production environment. In this case, the model will take in new data that was not a part of the training cycle.

Monitor model output: Monitor the model as it processes this live data to ensure that it is adequately able to produce the intended outcome—a process known as generalization, or the model's ability to adapt properly to new, previously unseen data. In production, models can "drift," meaning that the performance will change over time. Careful monitoring of drift is important and may require continuous updating of the model."

General remark: "*As with any logic and software development, use an agile approach to continually retain and refresh the model. However, AI systems require extra attention. They must undergo rigorous and continuous monitoring and maintenance to ensure they continue to perform as trained, meet the desired outcome, and solve the business challenges.*"
As it was demonstrated in different occasions the continuous monitoring and maintenance of AI and ML system is a key aspect to avoid unexpected behaviours and potential drawbacks, even if sometimes the outcome of the system is automatically transferred to operation without a human intervention it is many times wise to enable human involvement or even intervention to block unwanted results.

European Commission & Council of Europe

The EC join Research Centre explored the opportunity AI-generated synthetic data presents for privacy-safe data use.
In such specific field EU Regulations adopt a risk-based approach to regulation. AI should be as neutral as possible to cover techniques that are not yet known/developed.
On 17 May 2024, "the Council of Europe adopted the first-ever international legally binding treaty[27] aimed at ensuring the respect of human rights, the rule of law and democracy legal standards in the use of artificial intelligence systems. The treaty, which is also open to non-European countries, sets out a legal framework that covers the entire lifecycle of AI systems and addresses the risks they may pose, while promoting responsible innovation. This document was the outcome of two years of work due to an intergovernmental body, the Committee on Artificial Intelligence (CAI) composed by 46 CoE members states, 11 non-member states[28], the European union plus the private sector, civil society and academia, who participated as observers. The convention adopts a risk-based approach to the design, development, use, and decommissioning of AI systems, which requires carefully considering any potential negative consequences of using AI systems."
Few days later, on 21 May, the Council of the European Union adopted the EU AI Act, which once published in the EU Official Journal in June, became the first set of AI regulations that has undergone a full legislative approval process.
The EU AI Act is structured in 113 articles and counts 13 annexes, its holistic risk-based approach is suitable for any player in the field of AI from developers to deployers.
The EU vision on AI can be summarised as "beyond making our lives easier, AI is helping us to solve some of the world's biggest challenges: from treating chronic diseases or reducing fatality

[27] https://search.coe.int/cm#{%22CoEIdentifier%22: [%220900001680afb11f%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}
[28] Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, the United States of America, and Uruguay

rates in traffic accidents to fighting climate change or anticipating cybersecurity threats.[29]" Dealing with a fast evolving technology the key aspect in defining a framework is to find a golden balance between shaping the evolution and leaving to technology the freedom to evolve naturally.

United States: Federal executive, federal legislative & State Level (mixed)

At State level: basic requirements are non-discrimination /fairness concerns in States which have AI specific regulations, many states have no AI specific regulations, but ordinary consumer law could be applied in appropriate situations. On 7 September 24 California Governor Gavin Newsom signed three measures to remove deceptive content from large online platforms, increase accountability, and better inform voters. This enacted law criminalising deep fakes which could influence the current election, effective immediately for a period of 120 days before and 60 days after the election. "Safeguarding the integrity of elections is essential to democracy, and it's critical that we ensure AI is not deployed to undermine the public's trust through disinformation – especially in today's fraught political climate. These measures will help to combat the harmful use of deepfakes in political ads and other content, one of several areas in which the state is being proactive to foster transparent and trustworthy AI." [Governor Gavin Newsom].
This bill, to be known as the Defending Democracy from Deepfake Deception Act of 2024, would require a large online platform, as defined, to block the posting of materially deceptive content related to elections in California, during specified periods before and after an election.

At Federal level: October 20, 2023, Presidential Executive Order - Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. "Section 1. Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavour demands a society-wide effort that includes government, the private sector, academia, and civil society."
The executive order identifies eight guiding principles and priorities to advance and govern the development and use of AI:
(1) Artificial Intelligence must be safe and secure.
(2) Promoting responsible innovation, competition, and collaboration will allow the United States to lead in AI and unlock the technology's potential to solve some of society's most difficult challenges.
(3) The responsible development and use of AI require a commitment to supporting American workers.
(4) Artificial Intelligence policies must be consistent with my Administration's dedication to advancing equity and civil rights.
(5) The interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected.
(6) Americans' privacy and civil liberties must be protected as AI continues advancing.

[29] Artificial Intelligence for Europe

(7) It is important to manage the risks from the Federal Government's own use of AI and increase its internal capacity to regulate, govern, and support responsible use of AI to deliver better results for Americans.
(8) The Federal Government should lead the way to global societal, economic, and technological progress, as the United States has in previous eras of disruptive innovation and change.
The executive order refers to different "agencies"[30] involved in the application of AI technology e.g. Federal law enforcement agency[31], Sector Risk Management Agency[32].
With specific reference to AI in Critical Infrastructure and Cybersecurity to ensure adequate protection the following action shall be taken:
"*Within 90 days of the date of this order, and at least annually thereafter, the head of each agency with relevant regulatory authority over critical infrastructure and the heads of relevant SRMAs, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security for consideration of cross-sector risks, shall evaluate and provide to the Secretary of Homeland Security an assessment of potential risks related to the use of AI in critical infrastructure sectors involved, including ways in which deploying AI may make critical infrastructure systems more vulnerable to critical failures, physical attacks, and cyber-attacks, and shall consider ways to mitigate these vulnerabilities. Independent regulatory agencies are encouraged, as they deem appropriate, to contribute to sector-specific risk assessments.*"
This is simply one of the first actions to be taken, within150 days the Secretary of the Treasury shall issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks, within 180 days the Secretary of Homeland Security, in coordination with the Secretary of Commerce and with SRMAs and other regulators as determined by the Secretary of Homeland Security, shall incorporate as appropriate the AI Risk Management Framework, NIST AI 100-1, as well as other appropriate security guidance, into relevant safety and security guidelines for use by critical infrastructure owners and operators. Within 240 days of the completion of the guidelines described above. In addition, the Secretary of Homeland Security shall establish an Artificial Intelligence Safety and Security Board as an advisory committee. The Advisory Committee shall include AI experts from the private sector, academia, and government, as appropriate, and provide to the Secretary of Homeland Security and the Federal Government's critical infrastructure community advice, information, or recommendations for improving security, resilience, and incident response related to AI usage in critical infrastructure.[33]
There are more actions and duties duly described in the Executive Order; the description provided above will describe the approach of the White House in securing the nation against potential threats.

Nevertheless, yet there is no AI specific statute. The 2023 Senate Federal AI Risk Management Bill[34] is still pending. This bill directs federal agencies to use the Artificial Intelligence Risk Management Framework developed by the National Institute of Standards and Technology (NIST) regarding the use of artificial intelligence (AI).

---

[30] The term "agency" means each agency described in 44 U.S.C. 3502(1), except for the independent regulatory agencies described in 44 U.S.C. 3502(5).
[31] The term "Federal law enforcement agency" has the meaning set forth in section 21(a) of Executive Order 14074 of May 25, 2022
[32] The term "Sector Risk Management Agency" has the meaning set forth in 6 U.S.C. 650(23).
[33] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/
[34] Sponsor Sen. Moran, Jerry [R-KS] (Introduced 11/02/2023)

Exec order declares that AI regulation is a moral duty it:

- Directs application of the Defence Production Act 1950[35] to require that companies working on an AI model "that poses a serious risk to national security, national economic security, or national public health" to share the results of safety tests with the federal government to ensure those models are not used for malignant purposes.
- Directs that the Department of Commerce will devote "guidance for content authentication and watermarking to clearly label AI-generated content" which federal agencies will be expected to use.
- Instructs federal agencies to screen for bias in model related to housing applications, criminal justice settings and other institutions.

China: National Level

China invested relevant resources to lead the competition in the AI domain, as a direct consequence China is leading the way in AI regulation releasing new strategies to govern algorithms, chatbots and more. Early in 2021/2022 China developed & implemented detailed/binding AI regulation. These regulations foreseen duties on companies regarding content recommendations, rights for users recommended content. Worker protections against gig algorithmic scheduling were foreseen as well. The Cyberspace Administration of China, the National Development and Reform Commission, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the National Radio and Television Administration jointly released the Interim Measures for the Management of Generative Artificial Intelligence Services (the "AI Measures"), which is the first administrative regulation on the management of Generative AI services, which came into effect on August 15, 2023.

On September 2024 China has proposed new regulations that would make it mandatory labelling of AI-Generated Content that tries to clamp down on a surge in AI-related fraud.

Rules requiring watermarks identifying deep fakes, protecting people's "likeness rights" or harm the nation's image- creating/amending an Algorithm registry.

Regulation created in consultation w/academics, bureaucrats, journalists, researchers & technologies – public debate & advocacy, workshopping etc. factors of policy making.

Draft guidelines were published on September 14 and open for public comment one month as stated by the "Notice on soliciting opinions on the mandatory national standard (draft for comments) of "Network Security Technology Artificial Intelligence Generation Synthetic Content Identification Method"".

This marks the first time that the Cyberspace Administration of China has proposed specific rules regarding the labelling of AI-generated content.

All relevant units and experts: According to the standard revision plan of the National Standardisation Administration Committee, the Office of the Central Network Security and Information Technology Commission has organised and completed the draft of the national standard of "Network Security Technology Artificial Intelligence Generation and Synthetic Content Identification Method", which is now publicly soliciting comments. Please feedback your opinions to the drafting department of the organisation before November 13, 2024.

Transparency rights for citizens whose rights are affected by AI applications

[35] https://www.fema.gov/sites/default/files/2020-03/Defense_Production_Act_2018.pdf

Most recently rules that AI must always be under human control (since the advent of Generative AI- a precautionary approach). Positive duties for applications to promotes social cohesion, additional regulations prohibitions on algorithms that create division. Care taken to encourage production & not discourage development/innovation. Regulation requiring algorithm transparency.

Australia

The Australian Government's consultations on safe and responsible AI have shown that current regulatory system is not fit for purpose to respond to the distinct risks that AI poses. Governments, at international level, are introducing new regulations to address the risks of AI, with a focus on creating preventative, risk-based guardrails that apply across the AI supply chain and throughout the AI lifecycle. Australian Government is committed developing a regulatory environment that builds community trust and promotes AI adoption. They opened for consultation 4 September 24, Close 4 October 24) (AI risk categorisation criteria // EU's). We want your views on the proposed guardrails, how we're proposing to define high-risk AI, regulatory options for mandating the guardrails. The proposed approach to use AI safely and responsibly when developing and deploying AI in Australia in high-risk settings. They aim to address risks and harms from AI, build public trust, provide businesses with greater regulatory certainty. Strictly regulate High Risk, free rein to Low Risk to support development ($ 1.887,5 billion in 24 federal budgets). Proposed mandatory guardrails for AI in high-risk settings. Proposed Principles are as follows:

- Throughout their lifecycles, AI systems should benefit individuals, society and the environment.
- Throughout their lifecycles, AI systems should respect human rights, diversity & the autonomy of individuals (termed human-centred vision).
- Throughout their lifecycles, AI systems should be inclusive & accessible & should not involve or result in unfair discrimination against individuals, communities or groups (termed Fairness)
- Throughout their lifecycles, AI systems should respect & uphold privacy rights and data protection & ensure the security of data.
- Throughout their lifecycles, AI systems should reliably operate in accordance with their intended purpose.

There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI & can find out when an AI system is engaging with them. When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcome of the AI system. Those responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI system, and human oversight should be enabled.

Canada

With reference to the official documentation published by the Canadian Government, in September 2023, the Minister of Innovation, Science and Industry announced the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems. Development Focus ($2.4 billion in 24 federal budget) to encourage capability and infrastructure. Not waiting to "fall further behind", seeking economic benefit, capitalise on extensive clean energy grid. Artificial Intelligence and Data Act (AIDA) will introduce new

requirements for businesses to ensure the safety and fairness of high-impact AI systems every step of the way:
Design: Businesses will be required to identify and address the risks of their AI system with regard to harm and bias and to keep relevant records.
Development: Businesses will be required to assess the intended uses and limitations of their AI system and make sure users understand them.
Deployment: Businesses will be required to put in place appropriate risk mitigation strategies and ensure systems are continually monitored.
The idea is to have a flexible policy, where safety obligations are tailored to the type of AI systems. The more risks are associated with an AI system, the more obligations there will be.
These new regulations would build on existing best practices, with the intent to be interoperable with existing and future regulatory approaches. By drawing on common standards, the government is hoping to ease compliance. Consulting on best approaches with industry players (opened June 24, closed September 6, 2024).

Finland

Split focus (eventually) initially (2017) focused on business opportunities & competitiveness, economic benefits/growth, evolved through 2018 & 19 & 20 to include and supporting a high quality & efficient public service, and ensuring a functioning societal wellbeing of citizens (economic & other kinds of wellbeing).

Will a global regulatory framework for AI become a reality?

The willingness to create a regulatory framework devoted to Artificial Intelligence is already a reality, several conferences or spokespersons pertaining completely different sectors are concerned about the potential impact of AI on their activities and businesses. Some of them are concerned about the impact on job position and careers other are concerned about human rights or ethics or the possible full control on our lives and more. Regulatory bodies are usually concerned, facing emerging technologies not yet fully developed, to influence their development biasing the potential natural evolution. As it already happened in different digital "global" domains as IPRs, privacy or cybersecurity dealing with global impact the expectation is to release or promulgate a global regulation framework. Currently, each country or Institution is promoting or enacting its own solution. Sometimes approaches to the issue differs other times refer to similar principles. Some research groups propose to create an AI Agency graduated "AI" agency-based liability regulating with an "AS IF" fiction:

- Level Zero – non generative AI – Preventative programming restrictions along the lines of Environmental, Discrimination, Privacy Regulation, penalties based on harm/level of programming malfeasance,
- Level One – Generative or semi-independent AI, or AI as independent actor in the sense of other nonhuman independent actors with less "autonomous agency leeway". Animal law, preventive programming restrictions & responsiveness (//training' responsibilities) (NZ Animal Welfare Act 1999 has provision for Governor General to declare no listed entries as "animals"),
- Responsibility for harm lies with creator or custodian of "animal" – penalties lie with both AI and creator/custodians, confinement (redesign) or destruction for the former,

financial or custodial penalties for the latter, up through manslaughter and beyond, depending on programming malfeasance,

- Level Two – AI as independent actor in the sense of human independent actors – AI creating new AI – should this trigger morally based responsibilities and processes around control/penalties?

To summarize

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. Posing the focus on the legal side we need to understand if the "digital universe" that from ontology standpoint is quite different from the traditional world needs ad hoc laws and regulations or if the existing ones are applicable. For sure some specific features offered by this new normal require a specific, in many cases even global, legal framework.
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. The real impact of some of the emerging technologies such as machine learning and artificial intelligence are often emphasized by media, we must wait a little bit longer to assess the real impact of such technologies on society in specific fields such as employment or professional profiles [17 – Egger, 1996].
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 [18 – 19 – Ronchi 2019].

Bibliography

[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 Alfredo M., (2024). It is all gold that glitters? The new normal, Communication, Media, Design Vol 9, Num 1 2024 - https://cmd-journal.hse.ru/article/view/20977
[6.] (IFAP), Information Ethics, http://www.unesco.org/new/en/communication-and-information/intergovernmental-programmes/information-for-all-programme-ifap/priorities/information-ethics/Surowiecki J (2004) The Wisdom of crowds: why the many are smarter than the few. Doubleday, Anchor.
[7.] 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/
[8.] Stuckelberger Christoph, Duggal Pavan (2018), Cyber Ethics 4.0: Serving Humanity with Values, ISBN 978-88931- 265-8, Globethics.net
[9.] 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
[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.] Weiser, M. (1993). Some Computer Science Issues in Ubiquitous Computing. Communications of the ACM - Special Issue on Computer Augmented Environments: Back to the Real World, 36(7), 75–84.
[14.] Weiser, M. (1994). Creating the invisible interface. ACM Symp. User Interface Software and Technology UIST'94.
[15.] Deglobalization: The New Normal? ISPI https://www.ispionline.it/en/publication/deglobalization-new-normal-32758
[16.] Cicero Marcus Tullius, (45 B.C.), De Finibus bonorum et malorum. LOEB Classical Library. https://archive.org/ details/de nibusbonoru02cicegoog
[17.] Egger O. at al. (1996) Internet behaviour and addiction, Swiss Federal Institute of Technology
[18.] Ronchi A.M., (2019), e-Citizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer (D)
[19.] Ronchi A.M. (2019 D) e-Democracy: Toward a New Model of (Inter)active Society, ISBN 978-3-030-01595-4, Springer (D)