

Ensuring AI takes a human first approach

Alfredo M. Ronchi

Politecnico di Milano, Piazza Leonardo da Vinci 32, Milano, 20133, Italy

Tel: +39 393 0629373, Email: alfredo.ronchi@polimi.it, ORCID [0000-0003-1230-4338](https://orcid.org/0000-0003-1230-4338)

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. The goal 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 due to lives spent in cyber-bubbles, cyber-mediation of human relations, citizens experience the world thanks to a cyber device mediated approach. 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. A short description of the "dark side" follows. The following section, starting from the description of the actual scenario introduces the growing interest in reshaping the digital landscape, as we know it now, into a more human centred and ethics domain. A potential benefit is evident ensuring the opportunity to deploy a human centred environment instead of a cyber centric web of procedures and duties. To shape this approach a strong interdisciplinary approach is required: SSH, STEM, Biz, Cyber, Psychological skills and more.

Keywords: Digital Transformation, Artificial Intelligence, Digital Humanism, Cyber Crimes

Preamble

This chapter, even if well focussed on AI technology, requires extending the vision to a brief overview on cyber technology and its recent evolution both on the technological and exploitation side. The key aspects outlined in the title cannot be adequately described if not include in the overall scenario, 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 raise some concerns.

If on one side the whole architecture is based on cyber tech, with all the potential risks it implies as we will outline later, on the other side cyber-world rules 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.

The fluid context

In the last decades periodically, we received some messages strengthening their impact on society as a mix of incumbent dangers, crisis and more recently an ongoing full reshaping of society on the one hand due to technology advancements and geopolitical changes, a kind of imminent "new global order", on the other hand, global warming, exponential growth of world population, lack of food and water, several pandemic crisis, conflicts and more have had a profound impact on society, that combined with an evident lack of values and beliefs, generated a widespread feeling that there was something wrong [1 - Eckersley -1995]. Several concepts and movements like "politically correct", "cancel culture" [2 - Vogels – 2023, 4 - Dudenhoefer 2020], "last generation" and more deeply contributed to increase this feeling.

Some thinkers foresaw the endpoint of the Anthropocene the faith of anti-humanism, not due to a political program but as philosophical idea. The flip side, Transhumanism glorifies some of the same things that anti-humanism decries, scientific and technological progress like genetic engineering and nanotechnology, the supremacy of reason. Others are adamant that 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. Furthermore, the economic model carried out in the recent past shows its limits [3 - Imad A. Moosa, 2023] as well as globalisation that was its side effect. Nowadays more often we consider de-globalisation [4 WEF, 2023] as a scenario and the re-discover of local "values" and "identities" [5 - ECB, 2023].

Digital and Society

One of the key events that have characterised the recent period is the so-called digital transformation considered the natural evolution of the current society in the light of a pervasive technology like digital technology. This ongoing process has impacted at different levels different countries. Some countries invested relevant resources to quickly implement this transformation, others behaved differently. These technologies and much more the following ones become, in the new century, something to frame humans breaching privacy, sometimes even human rights [6 – Zuboff – 2019].

In 2020 citizen [7 - CoE – 2001] faced a turning point due to the pandemic, this phenomenon had an increasing impact on society as soon as the practical effects of a faraway event become a kind of local nightmare restricting the human rights of citizens at different levels in different countries. Citizens around the world faced relevant changes, the web of interconnections among different countries and enterprises showed its fragility outlining critical links in some "global" supply chains. Digital media and services played a leading role in informing and reshaping citizens' behaviours, some of the imposed modification of habits become a new "normal" and survived after the end of the crisis.

A relevant part of digital transformation relies on software platforms, mainly "global" platforms, a market sector not yet regulated, a "grey zone". Platforms are mainly private, and the key ones are concentrated in few countries creating a kind of "oligarchy" [8 – Ronchi, 2019]. The "control buttons" of our daily life are often outside the control of our nation state. The increasing dependence from service platforms, that terminated the activities of the previous added value chains, may cause serious troubles in case of problems in accessing them both due to malfunctions, hackers' attacks or 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 pandemic was surely a significant stress test for the network infrastructure all-over the world, major part of the business activities was turned into on-line activities to ensure "business" continuity; government services, justice, health systems, cultural institutions, education not forgetting supply chains re-arrangements and more took advantage from digital technology. Government processes quickly transformed documents and citizen data into streams of data; sometimes under the pressure of critical events, this process was not designed to guarantee security. At the same time an increasing number of "digitally divided" [9 – Pimienta - 2014] were forced to "go digital" generating a wider and suitable "market" for cyber

criminals¹. The desire of decision makers to go digital [10 – Ronchi, 2020] posed the basis to create a cyber-based society relaying on “digital”, this pillar is quite fragile, potentially subject to malfunctions, hackers’ attacks and suitable for top-down discrimination.

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. 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.

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. This aspect it is not globally relevant nowadays in some countries but already impacts some critical services and infrastructures such as health and basic assets provision.

Metaverse [11 - Ronchi, 2022] and virtual reality are inter-twined, but they are not the same. Digital technology till now has mainly acted as a human insulation technology.

On the social side western citizens are wrapped in their own personal cyber-sphere in a kind of symbiotic relation. They experience the world thanks to a cyber-device mediated approach; the “new reality” is the one delivered by devices. The 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 [12 – 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.”

As it can already happen today even if a cyber wallet is not yet fully implemented as well as national crypto currency, no access to the digital infrastructure means: no ID, no social security, no bank accounts, no certificates, and more. 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. Goodbye Privacy!

Recently the European Commission and the European Central Bank boosted the project to create an official digital Euro potentially active since 2026 now postponed to 2028. Of course, due to its origins this cannot be considered a crypto currency it can be considered a kind of digital voucher digitally managed by the European Central Bank and subject to a full digital control.

The alleged total dependence from the cyber domain represents a significant weakness as often happens in science fiction movies like “The Net²” that draws a not completely unreal scenario of identity theft or “Enemy of State³” depicting similar situations. This scenario was recently enriched by the rapid diffusion of artificial intelligence generating some more concerns.

Moreover, the environmental impact of digital technologies, including energy and water consumption, due to data centres and blockchain operations, as well as electronic waste from

¹ “During the current corona crisis, we see an increasement of cyberattacks. Therefore, everyone and especially older people should raise their awareness for such attacks” (Hans-Wilhelm Dünn, President, Cyber-Security Council Germany e.V. – WSIS 2020).

² American action thriller movie 1995 directed by Irwin Winkler

³ American political action thriller movie 1998 directed by Tony Scott

rapid device turnover raises questions about the sustainability and resilience of our current technological trajectory. Consequently, can cyber technology be considered green and resilient [13 – Ronchi 2024]? Who will “pay” for this surplus of energy, clear water and waste? Recalling one of the above sentences – “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”.

The dark side of cyber

We usually consider “security” as a seamless part of our life, apparently something effort and zero-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”⁴. Then security it is no more a zero-cost “commodity”, we need to invest some resources to reach a certain level of “insecurity”⁵. 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. As already outlined, 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 analytics⁶, risk assessment, probability⁷, and projections.

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).

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.

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. It is true that

⁴ 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.

⁵ Quoting Salman Rushdie Iranian / British writer recently suffered an attempt to kill him in NYC.

⁶ E.g. Ronchi Alfredo M., (2018), TAS: Trust Assessment System, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018

⁷ Risk assessment and probability cover even natural risks scenarios that can impact security (e.g. critical infrastructure).

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.

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.

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.

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 infrastructure⁸. Recently on the World Economic Forum 2024, Jeremy Jurgens⁹, 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 infrastructures¹⁰. 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 disseminating sensitive information online to improve their Facebook or Instagram or Tik Tok profiles or to download latest games on their smartphones or 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. In relatively recent times one of the reactions was Cyber Humanism.

⁸ This to do not mention Wanna Cry and the registered domain iuqerfsodp9ifjaposdfjhgosurijfaewrwer gwea.com

⁹ “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.

¹⁰ The one we know as GAFAM (Google, Amazon, FaceBook/Meta, Apple, Microsoft) and NATU (Netflix, Tesla, Airbnb, Uber)

Digital Humanism

The interest for a human centred approach to digital technology dates back long time, in the digital scale of time, some steps were the study on interaction design (SIGCHI) or the report to the G7 in 2001 “On Culture in a world-wide information society” [14 Ronchi 2001] together with the active contribution to UNESCO IFAP, IGF and WSIS [15 Ronchi 2023] working groups dealing with cyber ethics and digital technology impacts on society.

The omnipresent digital technology was considered one of the building blocks of a “new global order”. Hence, one of the main vectors of this change was associated to the so-called Digital transformation (DT). The incredibly rapid success of the “Internet”, mainly due to e-commerce, information services, and social media, gave a boost to the globalization trend, a shift toward uniformity, jeopardizing diversities, broadcasting the vision of cyber majors. Social media, global content providers are “training” young generations offering a *pensée unique* approach¹¹, this will impact future generations and their cultural identity.

Among the key actors promoting a humanistic reshaping of the digital world we find the Technical University of Vienna, and its team Digital Humanism stating that “Technology profoundly shapes the world we live in, and the stakes are high. Digital Humanism deals with digital technology development and policies based on human rights, democracy, inclusion, and diversity.” As Klaus Schwab wrote in 2016 in the preface of Shaping the Fourth Industrial Revolution, “*The world is at a crossroads ...*”¹², a paradigm shift driven by a convergence of cyber, nano, and bio technologies. Since the ubiquitous rise of cyber technology driven by the Internet and later boosted by the pandemic, innovation and development become progressively less humans centred. The “cyber” aspect currently exerts the most profound influence on society, affecting privacy, freedom, labour, security, behaviour, and beyond. That presents both unprecedented opportunities and challenges. Shoshana Zuboff's “The Age of Surveillance Capitalism” [6 -Zuboff – 2019] highlights several concerning aspects of digital technologies. While the digital world promises freedom and innovation, we now face visible drawbacks such as the monopolization of information spaces, proliferation of misinformation, concentration of power among online platforms, escalating cybersecurity threats, privacy infringements, market disparities, and the commodification of human experience for commercial exploitation. Ranjit Makkuni, former chief researcher at Xerox PARC actually Director, Sacred World Design Laboratory wrote “The Betrayed IT Revolution” stating that in the 1980s “*computational tools were envisioned as a tool for creativity and leisure Nearly 50 years later, that vision had become a nightmare, with deep impacts on the society*”.

Reshaping the digital landscape

“While digital technologies bring strong advantages coming along with a promise of freedom and innovation, negative aspects have also become visible in the last years. These include the monopolization of the information space, increasing levels of fake news and disinformation, strong power of online platforms, cyber threats and crimes, privacy breaches, strong market disparities as well as an economic order that claims human experience as free raw material for commercial practices of extraction, prediction and sales” [6 - Zuboff, 2019].

Digital transformation is a complex process shaped by all the actors of the digital ecosystem having different capabilities (governments, institutions, policy makers, business, startup developers, investors, NGOs) to integrate their work and activities in a global sustainable

¹¹ *pensée unique* based on a single cultural model

¹² Klaus Schwab. “Shaping the Fourth Industrial Revolution”, World Economic Forum 2016

scenario respecting human rights. To understand the implications of decisions and guide them, different approaches can be considered¹³:

Human-centred design. This approach involves designing digital solutions that are based on the expectations, needs, wants, and limitations of the end-users at each stage of the design process. It emphasizes involving users in the design process, understanding their perspectives, and iterating based on their feedback. This approach could be used to ensure that digital solutions are designed to reinforce digital humanism and not undermine it.

Multi-stakeholder approach. This approach, positively experienced on WSIS, involves engaging a diverse range of stakeholders, including ICT experts, ethnologists, sociologists, and experts in fundamental rights, in the development and implementation of digital solutions. This approach could be used to ensure that digital solutions are developed in a cross-disciplinary and collaborative manner and considering a broad range of perspectives.

Ethical frameworks. This approach involves using ethical frameworks¹⁴ to guide the development and implementation of digital solutions. This approach could be used to ensure that digital solutions are developed in a way that respects and promotes fundamental rights and values.

Impact assessment. This approach, long time neglected or limited to the marketing dimension, involves assessing the potential impact of digital solutions on society, including their potential benefits and risks. This approach could be used to identify potential gaps or issues that need to be addressed to ensure that digital solutions reinforce digital humanism and do not undermine it.

Capacity building. This approach, essential in a DT scenario, involves building the capacity of digital actors, such as data scientists, start-ups, and investors, to develop digital solutions that promote digital humanism. This approach could be used to develop training and education programs, as well as resources and tools, to support the uptake of best practices.

No single approach can bring about the expected benefits and mitigate or prevent risks. A combination of approaches is necessary.

Vision and Approach

Current vision aims to embed ethical, inclusive innovation into the technological landscape. By bringing together stakeholders from information communication technologies (ICT), science technology mathematics (STEM), industry/business, humanities, and social sciences, it aims to tackle the diverse societal impacts of digital transformations. This interdisciplinary collaboration ensures that proposed technological advancements are accessible, made transparent and beneficial, reducing inequalities and promoting inclusivity for all societal groups. At the heart of this approach is the empowerment of end-users and workers as “human beings”. Actively involving them in the development lifecycle of technologies, fostering a participatory design process. This approach not only enhances the relevance and adoption of these technologies but also ensures that they align with real-world needs and ethical standards. Through this engagement, it cultivates a sense of transparency and ownership among providers and users, which is crucial for the widespread acceptance and success of technological solutions. The commitment also extends to fostering social innovation, particularly in critical sectors such as healthcare, mobility, and public administration, which are vital in the upcoming digital domain. It aims to create frameworks and tools that encourage innovation, ensuring that it results in practical improvements in everyday life while adhering to ethical practices.

The approach promotes innovation that is both technologically advanced and socially acceptable and ensures that this innovation aligns with the values of inclusivity data access and fairness. It focuses on preparing society for upcoming transitions by enhancing skills and competencies that encourage

¹³ This list of capabilities refers to one of the implementation proposals concerning Digital Humanism

¹⁴ such as the European Union's Charter of Fundamental Rights.

adaptability and resilience among citizens. In addition, it addresses the risks that come with digital transformations, such as for instance, digital gaps, skills mismatches, top-down control, and security vulnerabilities. Targeted interventions are designed to effectively mitigate these risks, ensuring a safe and fair digital future. It achieves this by developing transparent guidelines, information on ownership and authors rights and best practices for the ethical deployment of technology, prioritizing the respect of individual privacy and user rights and societal values.

The roadmap

At the heart of methodology is the establishment of an Interdisciplinary Working Group (IWG) that brings together experts from various fields, including ICT, STEM, HSS, Biz/Econ and the whole wealth of Humanities. The next step will be to activate the interdisciplinary working group mapping and analysing of the state of art of digital humanism as it is conceived in Europe and in other countries to capture the common basis. Each expert will start from his/her own knowledge and understanding of the relation between the digital world and humanism, avoiding any “pre-casted” approach to the topics usually generating the bandwagon effect, keeping the “door open” to different “culture” and standpoints encouraging out of the box thinking.

This group is responsible for guiding the activities towards innovative solutions that are both technologically advanced, ethical, transparent and socially responsible. Keeping in mind the potentially different approaches and stand points due to different cultural identities. By incorporating diverse perspectives, the IWG ensures that provided solutions are comprehensive and address the multifaceted challenges of digital transformation.

An applicable methodology can be summarised as follows:

- Mapping and analysis of the state of digital humanism approaches world-wide. Shall provide a comprehensive overview of digital humanism, including its conceptual foundations, current practices, challenges, and opportunities. This activity aims to establish a solid understanding of the field, analyse case studies, and develop methodologies for promoting human-centred digital transformation across various sectors and contexts.
- Next step is a cross-disciplinary collaboration in the field of digital humanism - aims to establish an international network of digital humanism researchers, practitioners, and experts, who will collaboratively analyse, deploy, and disseminate key principles of human-centred digital transformation. It will map and network digital humanism research, forming an extended network and a core expert group. These experts will analyse case studies, define the principles for human-centred digital transformation, and implement them in living labs. A comprehensive map and database will be created to identify ongoing research initiatives and key players in the field of digital humanism. Concurrently, a set of guidelines and best practices will be developed for integrating digital humanism principles into various sectors and contexts. This will be achieved through collaborative analysis of case studies and investigation frameworks. A systematic data collection process using online surveys and interviews will be conducted to gather information about ongoing research activities and key players. The results of this data collection will be merged with those achieved by previous activities to create a comprehensive and up-to-date resource for the field of digital humanism.
- Once defined the Digital Humanism guidelines the development and implementation of digital solutions can start. First actions will address data protection, privacy, informed consent, and related issues, along with the complexities of balancing open-source practices and intellectual property rights (copyright and copyleft) in contemporary research and practice, by delving into critical data governance and ethics issues and examining existing research and practice, to enhance guidelines for data protection, privacy, informed consent,

and related matters. This set of activities will focus on ethical principles, considering both procedural ethics and ethics in practice. These principles will be connected to the practical challenges of digital humanism guidelines. To ensure a tight connection between digital humanism and evolving digital technologies an annual symposium will be foreseen fostering collaboration and knowledge exchange, while policy guidelines will provide actionable recommendations for to ensure the integration of digital humanism principles in digital transformation initiatives.

- The awareness and capacity building of digital actors seeks to develop a robust monitoring and evaluation framework for digital humanism initiatives. This framework will help measure the progress and impact of digital products and services aligned with digital humanism principles. By empowering stakeholders with knowledge and skills, creating innovative tools, providing targeted training, and contributing to the creation of a digital humanism platform collecting, among the others, tested templates and success stories. To complement this platform and activate the shift toward digital humanism a digital humanism mentorship and impact evaluation programme will be setup. It involves setting up structured mentorship programme that connects seasoned digital humanism experts with emerging talents. The programme will offer tailored guidance, regular progress reviews, and collaborative projects, with a comprehensive impact evaluation to measure its success in advancing digital humanism expertise and advocacy. The Mentors will be selected from the pool of participating stakeholders: Ethical technology experts in the fields of ethics, technology, and social responsibility, Human rights advocates who are passionate about protecting human rights and promoting social justice, Policymakers who are involved in shaping technology policies; Business leaders who are committed to ethical and sustainable business practices; Academics: Researchers and professors who specialise in the ethical implications of technology.
- The Mentees will be selected from the pool members of the value chain: Students: Undergraduate and graduate students who are interested in pursuing careers in technology or related fields; Early-career professionals who are starting their careers in technology or related fields; Entrepreneurs who are starting their own technology businesses, Non-profit organizations who are working to promote ethical and responsible technology; Government officials who are who are involved in developing technology policies.

To support this methodology, the involved parties will adopt a flexible and adaptable project management structure to address the complexities of digital technology projects. This will prioritise stakeholder engagement, including end-users, policymakers, industry leaders, and civil society organisations, to ensure that outputs are socially viable, transparent, and widely accepted. A collaborative approach, combined with targeted training and outreach, will build capacity and promote the adoption of project's outcomes. In addition to these participatory activities, it incorporates a range of supportive measures and analytics, including targeted training sessions, dissemination events, and KPI measured public awareness campaigns. The described activities are designed to build capacity among stakeholders, promote the widespread adoption of the project outcomes accompanied by a high reach, relevance and impact on the public discussion. The target is to achieve measurable and sustainable transformative transparent and trustworthy outcomes, creating a profound impact on technological and societal landscapes.

To wrap up

Taking in consideration the actual trends and looking at the potential scenario in a mid-term perspective one of the main concerns is to be framed in a cyber centric society very similar to the one often depicted by Sci-Fi movies. The high risks related to the single pillar holding the full framework on one side concern us about potential crisis on the other side gives to the - framework "architects" an unprecedented power to rule on citizens.

This foreseeable scenario elicited the necessity to reshape the existent cyber framework involving all actors of the digital ecosystem (governments, institutions, policy makers, business, startup developers, investors, NGOs) to integrate their work and activities in a global sustainable scenario respecting human rights. More in general there is a need to reshape our technological landscape putting again humans in the focus. To mitigate risks such as monopolization of the information space, increasing levels of fake news and disinformation, strong power of online platforms, cyber threats and crimes, privacy breaches, strong market disparities, a robust framework grounded in ethical principles is imperative. The described methodology adopts a horizontal and holistic approach that combines ethical considerations with extensive stakeholder engagement to develop a collaborative framework centred on transparency and human well-being.

References

- [1.] Eckersley Richard, 1995, Values and visions: Youth and the failure of modern Western culture, Youth Studies Australia 14(1):13-21
- [2.] Vogels Emily A. et Al. (2023) Americans and ‘Cancel Culture’: Where Some See Calls for Accountability, Others See Censorship, Punishment, Pew Research Centre - <https://www.pewresearch.org/internet/2021/05/19/americans-and-cancel-culture-where-some-see-calls-for-accountability-others-see-censorship-punishment/>
- [3.] Imad A. Moosa, 2023, The Western Economic System, In book: The West Versus the Rest and The Myth of Western Exceptionalism, Palgrave Macmillan
- [4.] Deglobalisation: what you need to know, World Economic Forum 2023 <https://www.weforum.org/agenda/2023/01/deglobalisation-what-you-need-to-know-wef23/> and Deglobalisation? The reorganisation of global value chains in a changing world <https://www.oecd.org/publications/deglobalisation-the-reorganisation-of-global-value-chains-in-a-changing-world-b15b74fe-en.htm>, OCSE
- [5.] Risk or reality? European Central Bank – 2023 <https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog230712~085871737a.en.ht>
- [6.] Zuboff Shoshana (2019), The Age of Surveillance Capitalism. The Fight for the Future at the New Frontier of Power, ISBN 978-1610395694, Public Affairs
- [7.] Council of Europe (2001) New information technologies and the young. Council of Europe Publishing, Paris
- [8.] Ronchi A.M., (2019), e-Citizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer (D)
- [9.] Pimienta D (2014) Redefining digital divide around information. Literacy and linguistic diversity in a future context of access provision, internet and socio-cultural transformations in information society. Interregional Library Cooperation Centre, Moscow. ISBN:978-5-91515- 061-3
- [10.] Ronchi Alfredo M., (2020). Digital transformation, proceedings ICC New Delhi, Cyberlaw ISBN:978-0-385-50386-0
- [11.] 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
- [12.] Deglobalization: The New Normal?, ISPI <https://www.ispionline.it/en/publication/deglobalization-new-normal-32758>
- [13.] 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>
- [14.] Alfredo M. Ronchi et al., Report to the G8 (2001) On Culture in a worldwide information society — <https://re.public.polimi.it/bitstream/11311/690095/1/Future%20OnLine%20Culture%20G-8%20report.pdf>
- [15.] Ronchi Alfredo et Al. (2023), Can cyber tech be resilient and green?, WSIS 2023 Outcome Document, <https://www.itu.int/net4/wsis/forum/2023/Agenda/Session/161>
- [16.] Egger O. at al. (1996) Internet behaviour and addiction, Swiss Federal Institute of Technology