International Conference
"Ethics and Artificial Intelligence"
(Venice, June 24-25, 2022)

Medaglia del Presidente della Repubblica
(Medal of the President of the Italian Republic)

with the contribution of
TIM, Noovle

in collaboration with
The Aspen Institute
Aspen Institute Germany
Institut Aspen France
Academy of Sciences of Bologna Institute

Summary

by

Stefano Colloca, Lorenzo Iannarilli, Giuseppe Roberto Marseglia

The geopolitics of data and the role of cyberwarfare

Data governance, collection and processing are strategic practices whose impact affects endpoints ranging from business models to geopolitical balances. The framing of legislation that permits both citizen/consumer protections and data sharing procedures that optimize information and permit the extra-territorial reach of data governance is a highly complex and equally urgent issue.

Indeed, the related jurisprudence is in need of a radical update, which prompts an interesting reflection on the harshest penalty that ancient Roman law could impose: *damnatio memoriae* – a sentence condemning the convicted party to complete and utter oblivion. How times have changed: in today's world, oblivion is no longer a penalty but indeed a legal right sanctioned by the European Union in a set of laws that address concerns over citizens' dignity and privacy.

Actually, the European Union's regulatory efforts date back to more than twenty years ago. They began with the issuance of the ePrivacy Directive (2002) and the GDPR or General data protection regulation (2016), which are still in effect and have recently seen the addition of two important milestones. One of these is a proposal for regulating the use of Artificial Intelligence algorithms, known as the AI ACT (2021), and the other is for common regulations on data governance and sharing known as the Data Governance Act (2020). This latter advances the idea that, as regards the EU, digital sovereignty is not based on isolationism but rather on collaboration and receptivity toward other nations; that includes the free flow of data. It therefore lays the groundwork for the establishment of a digital territory common to the European Union, the United States of America and other states that may wish to join.

A further step forward in forging a trans-Atlantic digital pact was the recent Declaration for the Future of the Internet (2022) proposed by the White House and signed by 60 governments. The signatories commit themselves to the creation of a truly open, single global internet that fosters competition, privacy, respect for human rights and fundamental freedoms for all people, as well as the free flow of data and inclusive and sustainable connectivity that offers anyone access to the digital economy (prosumers).

Nevertheless, new technologies – in particular, everything that directly or indirectly concerns digital systems – place policy makers in front of more than a few trade-offs and difficulties.

In the first place, as the scientists at the MIT Media Lab describe in "The Moral Machine Experiment", the ethics involved are geography-specific; i.e.

since “cultural clusters” come into play when it comes to deciding what is good and bad or right and wrong, designing a one-size-fits-all cross-cultural regulation is a very tall order. Indeed, the regulatory approach of many governments has been highly variegated.

Nevertheless, finding a solution is becoming increasingly urgent. In 1983, in the midst of the Cold War, then-Soviet officer Stanislav Petrov identified what he correctly deemed a malfunction in the early-warning missile system and decided to disobey orders to launch a retaliatory strike – a decision that in all probability saved us all from nuclear war.

This early example of the critical importance of data and information management in making decisions capable of shifting the balance between nations, if updated to the present day – where the volume of data produced, the facility of accessing them and the speed with which they can be shared is so much greater than in the past – clearly underscores the fact that it is no longer possible to do without automated and intelligent data protection, certification, exchange and verification processes that, in turn, feed real-time decision support systems.

While up to the recent past information was mainly collected by intelligence operatives who risked their lives on a daily basis to do that job, today’s citizens often turn their data over spontaneously and free of charge when interacting with digital platforms, and clustering instruments make it possible to identify and very precisely predict user behavior.

Today’s socioeconomic context has also undergone some radical alterations. Starting in 2020, events that affected the entire world brought sweeping changes to people’s daily lives and priorities in a shift to what has been labelled the “new normal”.

The first major event of this season of change was the Covid-19 pandemic. In addition to dominating public health management, the pandemic forced people to stay closed up in their homes; a generation of young people had to be distanced from classrooms for over a year; scientists of the world scrambled to come up with treatments, prevention methods and containment policies against a single public enemy: the SARS-COV-2 virus.

At the same time, every government went in search of the tools with which to confront and manage the disease: oxygen tanks, masks, respirators and so forth. At this historic stage, information exchanges and data management acquired strategic importance for the security of nations that, on the one hand, feared being seen by the world as unprepared and trembled at predictions of the economic contraction that would follow the slump in consumption. On the other hand, they were confident that sharing data and

discoveries would contribute to ending the emergency more quickly – a process, what's more, that is still underway.

The second major event that shook global equilibria was the Russian Federation's invasion of Ukraine. Here too, data and information management has had a pivotal impact on the course of events at a multitude of levels.

Firstly, information is widely used as an indirect weapon in the wielding of soft power: targeted propaganda campaigns, the spread of fake news and the systematic censure of information sources associated with anyone considered an enemy.

Secondly, data and information are at the center of the digital battlefield in what is known as cyber warfare. The Russian Federation threatened Italy with reprisals after it supplied weapons to Ukraine; the threat was unique from the standpoint of history in as much as it consisted of the publication of confidential and sensitive data and information on prominent individuals and Italian leaders. Yet, it is not only people that are sensitive to IT attacks; on the contrary, in the majority of cases the targets are the computer systems of strategic infrastructures and firms, and their intention is to damage, cancel or commandeer access to data, interrupting business continuity and the efficient provision of services.

In terms of the persons involved and the indirect and direct damage done, today's cyber war has taken on dimensions comparable to those of traditional warfare. Yet, while for conventional battles such as naval ones, for instance, the specific skills and levels of preparation of different states are not in any way comparable. Being an essentially simpler undertaking, cyber war effectively levels the playing field, often facilitating the use of meticulously organized technical resources that are not necessarily a component of any official government program. The ethical/legal debate on the acceptability of using vaguely defined methods and/or independent groups to carry out cyber-attacks is inevitable.

Italy recently joined the ranks of others giving serious consideration of the issue of cyber security, making structural investments and undertaking institutional actions such as the creation of an authority and specialized team charged with overseeing the application of legislation. Moreover, a recent spike in ransomware attacks has not only affected the governance of strategic infrastructures but also the systems of small and medium-sized Italian businesses.

Considerable investments therefore have gone into both the communications and IT infrastructures that companies use "as-a-service",

and that ensure the protections typical of European law and of greater IT security in general. A remaining point to be considered, however, is the protection of intangible assets. Indeed, while strategic government assets are still understood to be those physical ones – sea and airports, power grids, logistical infrastructures and so forth –, the need to protect what are increasingly strategic digital assets has been relatively neglected.

Yet, a strong national strategy on the safeguarding of our intangible assets must necessarily go hand in hand with an equally effective push to boost digital literacy. Indeed, all too often cyber-attacks are abetted by the poor digital culture of their victims; and according to the European Commission's recently published Digital Economy and Society Index (DESI), Italy has a long way to go to catch up to other European countries.

Artificial intelligence and defense systems: the ethical dilemma

The application of artificial intelligence to military defense poses a number of ethical and regulatory questions, two of which appear especially relevant. The first concerns the correct dosage of AI, i.e. the balance between under- and over-use. Human organizations often pose unjustified obstacles and resistance to the use of innovative and transformative technologies. This is an example of under-use often seen sectors of the public administration such as healthcare, justice and education; yet, neither is the business world immune, despite the well-known fact that AI is principally what gives today's firms their competitive edge.

Opposition to the use of AI exists in the military sector as well, even though it is a technology capable of increasing the efficiency of many processes, especially in space defense. The military sectors where unjustified resistance is lower are those most recently created, and which could therefore provide a useful springboard for the spread of the digital transformation.

On the other hand, since AI remains a fallible technology, the automation it affords should not involve riskier military activities; indeed, the AI systems used by the military are also vulnerable to cyber-fooling or cyber-spoofing attacks. Thus, we could rephrase our first question: When is the use of AI ethically warranted?

Our second question concerns not only the amount or range but also the modalities of AI use. Indeed, AI systems are often allowed too much independence and if they are not monitored constantly by humans can have destructive consequences. That applies to AI use at every level but assumes

much greater resonance in the case of emerging highly automated weapons and autonomous weapons systems.

The arguments prepared by the United Nations Convention on Certain Conventional Weapons assert that international humanitarian law applies to all militarized conflicts and all weapons systems, which therefore includes autonomous weapons – meaning any weapon capable of independently identifying a target and attacking it without human intervention. Similarly, the Geneva Convention states that military commanders must take every precaution to protect civilians during any attack and evaluate conformity with international legislation on new weaponry and methods of military engagement. Article 36 of Protocol 1 (1977) additional to the Geneva Conventions of 1949 states: "In the study, development, acquisition or adoption of a new weapon, means or methods of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law". Although radically different from traditional ones, autonomous weapon systems are covered by the same legal principles. The central ethical dilemma is whether there is sufficient room for the "meaningful human control" required for taking every precaution to protect civilians. Of course, it is true that software and automated systems were invented and developed by humans, so in that sense they can be considered indirectly under human control. Nevertheless, that indirect control may not be enough when it comes to military applications – an autonomous system cannot be entrusted with deciding whether to kill human beings.

The design of autonomous weapons is causing a paradigm shift capable of radically transforming how wars are fought and how geopolitical relations are understood. The creation of independent machines with the capability and authority to kill human beings raises a multitude of additional ethical and legal red flags. What on this new scenario is meant by "significant" human control?

Finally, two additional ethical risks associated with the employment of autonomous weapon are disproportionality and non-reversibility. In the first place, international humanitarian law states that military attacks must be targeted and proportionate in such a way as to avoid civilian massacres. While on the one hand it is true that AI can contribute to making war less bloody by reducing the number persons killed or wounded unintentionally due to human error, on the other there is the risk that autonomous weaponry could strike indiscriminately and disproportionately. If, with regard to legal liability, the so-called principle of subjectivity is adopted – which requires a

psychic nexus between the agent of conduct and the conduct itself – then where is liability to be placed with regard to the act of an autonomous weapon, and who is to be held liable when an autonomous weapon mistakenly attacks a hospital or a school, for example? In the second place, autonomous weapons are devoid of human psychology, cannot feel pity and are incapable of aborting an operation as a result of compassion.

Their actions cannot be self-limited in the way that a human being's can under certain circumstances; indeed, it could be said that if war is inhuman, war conducted by autonomous weapons is, by definition, even more so.

Moreover, the possibility of equipping an automaton with the capacity to decide to change the intention of its actions raises two new issues. The central query at technical level concerns what such a decision would be based on; in order to have a decision somehow comparable to a human's, an automaton should be able to participate in the human way of life, interact with the world, have relationships, feel and have inclinations and desires like those of human beings. All this is currently impossible, which brings us to the second consideration: if it were to become possible in some remote future (studies on super-intelligent autonomous agents provide food for thought), it would be even more problematic and dramatic to delegate life and death decisions in a theater of war to a machine rather than a human.

This would, first of all, run counter to the fundamental principle of "respect for human autonomy" established by the EU Ethics Guidelines for Trustworthy AI as the basis for the ethical assessment of the development and impact of AI, citing a "human-centric approach, in which the human being enjoys a unique and inalienable moral status of primacy in the civil, political, economic and social fields".

Furthermore, there is a sense in which the concept of attack-defense-conflict can be more broadly applied, and that goes well beyond the military dimension: cyberspace. Certainly, in many cases cyber-attacks can take on even geopolitical relevance since attacks on a nation's cyberspace are attacks on the nation itself and its strategic assets. In many other cases, such attacks can be declassed as criminal acts lacking in any geopolitical objective. Whatever the aims of cyber-attacks, there are some facts and problems common to all and to cybersecurity in general. Cyber-attacks do not produce kinetic, physical effects but can have devastating and irreversible impacts: suffice it to think of the repercussions of publishing masses of sensitive data. These attacks are relatively easy to carry out, need no national armed force or mercenary militia; indeed, the computer skills of a single individual, even of a minor child, are sufficient. Every system is susceptible; cybersecurity

supplies the immunity. Monitoring system vulnerabilities, sharing information on attacks, creating "cybersecurity by design" and educating business executives and public administration officials on cybersecurity are all obligatory and must be done within the framework of a common European regulatory program convergent with the regulatory activity practiced by the US so as to avoid market fragmentation.

It is not enough to depend solely on human ability to ensure system security. The speed and variety of some attacks call for prompt identification and equally rapid strategies for dealing with the problem. In that sense, artificial intelligence is an instrument that, at least in part, is able to respond to firms' need to build secure, resilient systems. Attackers, however, are also adept at teasing out system architecture weaknesses, resulting in nothing less than an AI version of "capture the flag".

AI thus offers sound assistance for optimizing systems' immune response; nevertheless, as was pointed out earlier, it is not infallible. It is a system that operates autonomously, which makes it fragile and vulnerable, and it is up to humans to be vigilant. The good and effective human management of AI walks a fine line between control and application. In addition to the mere application of a technology, human control is necessary for maintaining a system's efficacy (the technical motive) in order to preserve the skills, role and dignity of humans (the ethical motive).

New business models and the choices companies make

Digital transformation is a term often used in reference to a generic process that foregrounds digital technology, yet its real scope is certainly much broader and more complex than that. When referring generically to change within a firm, it is important to specify what is going to change – processes, products, services or the entire business model – and at what rate of speed, i.e. if the change will be gradual or sudden. In the majority of cases, digital transformation exclusively affects processes that become more efficient and less costly, i.e. they do the same things they did before the change, but better.

Considering the digital revolution as an agent in the increased efficiency of business operations leads, however, to the conclusion that it is still incomplete. Thus, it should perhaps not be viewed as an industrial revolution – on a par with electrification and automation – but as merely a technological one.

The data tell a different story though. The technology available today has fostered a full blown revolution in business models that are surely allowing

companies to do things better but also to do new things; i.e. to change how they deliver value to their customers and the society in general. According to the most recent macroeconomic forecasts for the digital era – or as some prefer to call it the "data era" – the GDP of industrialized countries will grow twice as fast as it did during the decade following the Second World War, qualifying it in the final analysis as a true industrial revolution.

In effect, these technologies share a feature that establishes a point of rupture with the past. In the first place, they make it possible to involve end users in the creation of value by means of complex clustering activities and the personalization of goods and services, even on a large scale (mass customization). Secondly, they affect not only operational models but also business models (business model revolution); this thanks to digital servitization, subscription-based-revenue models and, in general, the use of smart devices as points of entry for customers to access customized services. An example is mobility 2.0, which overturns the concept of automobile ownership by using the car itself as an entry point for the offer of smart mobility services.

The many technologies currently contributing to this macro-transformation are the offspring of the current era of exponential growth in the field of technology. We have a mini-revolution around every 3 to 5 years, and technologies that were once not expected to develop rapidly have now become tools at the service of the digital strategy of every enterprise and institution. It is estimated that approximately one-third of businesses in Italy use Big Data and Artificial Intelligence to gain competitive edge, and that many among the remaining two-thirds are at an often-advanced stage of experimentation. Cloud computing is the enabler of this transformation and AI is and will continue to be the differentiating factor.

The importance of this is frequently underscored in the catchphrase "data is the new oil", a statement that, although it renders the idea, lacks precision. Data are not only a consumable asset but can be utilized countless times; while oil has to be drilled and oil fields remain contested, data are frequently shared spontaneously by persons in exchange for services. Furthermore, the data transmitted over the 5G network and optimized by AI systems will eventually allow countries to reduce emissions by 15% – in clear contrast with what typically happens in industrial revolutions – and aid in ensuring environmental sustainability and achievement of the Paris Agreement goals.

The data associated with the use of new technologies are encouraging from the industrial standpoint also. The 2021 McKinsey report on the State of AI describes the evolution of business's adoption of this technology over the

current year. As in 2020, and possibly propelled by the Covid-19 pandemic, the adoption of AI-related instruments and processes increased over the previous year and the data show two key results. The first is the significant rise in the number of companies that consider AI instrumental to at least 5% of their Earnings Before Interest and Profit (EBIT). The second is the expansion of the use of this technology, which had initially been limited mainly to smart reporting and marketing, bottom-line assessment and the production of completely new AI-enabled goods and services.

The situation in Italy is different. In November 2021, the European Commission published its Digital Economy and Society Index (DESI), which measures the digitalization of Union member states. Italy ranked particularly low in terms of exposure to STEM skills, which is the principle culprit in the delays behind the adoption of these technologies by the small and medium-sized enterprises that are the backbone of the nation's economic fabric.

Closing the cultural divide with other member countries is both fundamental and urgent. According to the best known theories on change management, the main cause for resistance is fear of the unknown; yet, failure to embrace and govern change runs the risk of some companies being excluded from the global economy or, in the best of cases, denied the many the opportunities for evolution that are mediated precisely by digital technology.

Big Data and machine learning applications have in the past been used to streamline processes, improve industrial performance and automate a series of low value-add procedures with a view to raising efficiency as well as in some cases to cutting jobs; yet, those same applications are today drivers behind innovative business models designed instead to enhance prospects for creating jobs rather than eliminating them.

From the standpoint of digital infrastructure, on the other hand, Italy has made clear progress and investments, which qualify it as a possible European leader. Only advanced support technologies and infrastructures can assure the broadest assessment of data and intangible assets. Technological support infrastructures play a key role in the development of data-driven applications, the speedy communication of data and awareness that the advantages of digital-mediation are not reserved for the major players alone, but are within everyone's reach; those most instrumental to accelerating these aspects are connectivity and cloud computing.

The diffusion of fiber optics and 5G connectivity allow companies to build IoT and IIoT networks whose performance meets the needs of the industrial processes they underpin. Cloud computing technology, which offers

everyone access to powerful low-cost infrastructures, democratizes access to data-mediated opportunities formerly available to only a few highly structured corporations, and accelerates research and the specialization of data-driven algorithmic approaches. Moreover, cloud infrastructures facilitate the ongoing transition from on-premises services to those "as-a-service", triggering a radical change in business models: The digital economy has gone from Software as a Service (SaaS) to Platforms as a Service (PaaS) to Infrastructure as a Service (IaaS), all the way to what is now referred to as "everything as a service".

Ulterior opportunities for the development of data-driven business models have been made possible thanks to advancements in blockchain technology, which has contributed to the creation of new ways, such as the metaverse, for users to interact.

Indeed, blockchains essentially make it possible to notarize data written on a shared platform, thereby making them non-modifiable. This technology permits the issuance of Non-Fungible Tokens (NFT) that provide certification of proprietorship and authenticity to any asset, particularly digital ones, making it possible to simulate the rarity of assets even in the non-physical world.

Artificial Intelligence has a different impact on this new scenario, which is drawing us toward a future "world of worlds". First of all, new ways of interacting by means of state-of-the-art sensors and actuators fueled by advanced AI algorithms facilitate multimodal experiences that employ more than one sense contemporaneously while interacting at a distance.

A second impact is associated with computer vision, which makes it possible to reproduce digital copies of physical elements simply and efficiently and to incorporate them into digital worlds that can be generated even without the supervision of a human being.

The third impact lies in the management of virtual economies where virtual assets are traded in virtual worlds with real money. Over the past year, the importance of these new opportunities for the national economy has led the Ministry of Economic Development to propose a national strategy for the implementation of AI. The proposal suggests improving the dialogue between institutions, universities and the business world on how to use this technology to the strategic advantage of the entire nation.

Artificial intelligence, ethics and sustainability: future pathways

One way to offer an ethical assessment of AI applications could be to calculate the risks and benefits of each, in the same way medical treatments are validated. Nevertheless, although this approach is a reasonable one, it cannot provide answers to the underlying question: What is to be considered a risk and what a benefit?

There are at least three benefits regarding the sustainability that AI can offer the present and the future: timesaving, defense of the environment and reduction of the education gap.

First, the global pandemic – which is still ongoing – has changed many people's way of working as well as the value of work itself in a paradigm shift that regards the values around which people organize their lives. Saving time to dedicate to one's cultural and interpersonal growth has become an increasingly important benefit. While AI is justifiably viewed as a technology that cannot replace features of human uniqueness such as real relationships and emotions, it certainly can help humans lighten the burden of daily life by eliminating the need to travel to work, simplifying industrial processes and avoiding time-wasting errors. Large-scale application of AI gives humans the gift of time that we were not accustomed to having but which the pandemic foregrounded and qualified as an important if not obligatory value.

Secondly, one of the most significant threats of the present century, climate change and its negative consequences, have heightened concern for the defense of the environment and nature. AI will allow for rapid scientific progress in the study of climate change thanks to its capacity to process massive quantities of data. We are already seeing the results of AI's contribution to predicting variations in global temperatures, natural phenomena such as precipitation, particularly damaging events such as floods and forest fires, along with multiple other meteorological and geophysical factors. Moreover, AI supports environmental sustainability and protects natural ecosystems by helping to increase the energy efficiency of industry and promote dematerialization (meetings or lessons on-line, remote working, e-books); it also encourages the circular economy by incorporating recyclability and reusability into product design.

European awareness of the environmental benefits of AI is widespread in public institutions, research centers and private enterprise; thus, it has been noted that the underuse of AI would be ethically unacceptable. On the other hand, it is also true that vast amounts of energy are required to develop and run many AI systems; on the other hand, these systems make it possible to

replace lower-tech operations that would require much greater amounts of energy. As mentioned earlier, if the risk/benefit analysis is a good approach in the ethical assessment of a technology, and if defending the environment is a value and a benefit, then every use of AI could be evaluated according to a risk/benefit ratio keyed to environmental costs, with a view to avoiding those (in reality, rare) applications that would result in a greater environmental price tag.

Saving time to cultivate one's personal life and protect the environment are two goals, two benefits, that AI is capable of providing. In that sense, AI and sustainability are allies – the blue and the green are twin revolutions.

A third front, and one where the risk/benefit ratio is more difficult to describe, is reduction of the education gap. AI is clearly a factor in the expansion of knowledge and the spread and exchange of information as well as of scientific progress, as witnessed by the fight against the Covid-19 pandemic and studies on climate change. What is more problematic however, is evaluating whether the AI revolution has amplified or reduced the educational divide between regions of the world, areas of an individual nation, neighborhoods of the same metropolitan city or even between genders. What's more, AI is a technology, and technology necessarily carries with it a transfer, or redistribution, of power. With regard to ethical considerations, therefore, it is up to humans, specifically those who govern, to design an AI aimed at accelerating the reduction of educational inequality as well as at designing educational systems that incorporate highly qualified digital training.

On the continent of Europe, the Next Generation EU gives AI a pivotal role in the formation of citizens. For example, it earmarks 2.1 billion euro for Italy to update the technology of its educational and training systems: 650 teachers are to be trained over a 5-year span in digital education, in digital technology instruction and in instruction that uses digital technology. Moreover, the use of AI and the increased digitalization of schools should relieve teachers of many non-educational tasks, such as bureaucratic obligations. While many professions will disappear as a consequence of the digital revolution, the most recent international studies, although not in agreement on the number, predict a significant loss of jobs in OECD countries to automation and substantial transformations in a large number of professions, many new jobs will be created for a larger number of skilled workers; take the aforementioned example of cybersecurity or the jobs that will be created in concomitance with the increase in free time. Besides, the first industrial revolution also wiped out many jobs, only to see new ones sprout up unexpectedly in fields such as textiles and manufacturing.

With regard to the current revolution, AI automation is capable of replacing the more repetitive and less desirable tasks without eliminating, at least for the short to medium term, those more creative ones that require human intelligence. It is of particular importance to concentrate on the new skills that will be required by the work world over the coming years, and the capacity of the school system to direct students toward them in order to avoid, or at least reduce, a mismatch between the supply of and demand for skills.

Indeed, the correct match of supply with demand could be calculated at both national and international levels precisely with the support of AI. The task is an enormous one and, as the previously cited DESI study points out, Italy has a particularly large deficit when it comes to digital skills, a limitation common in any case to many academic systems. Approaches to providing digital skills are often simplistic, and tend to lump digital skills in with those of science and technology. The AI revolution also calls for decision-making, political, ethical and communications skills. As has been convincingly observed, the AI revolution requires that the push to optimize STEM skills must coincide with a rediscovery of the humanities as true conveyors of the knowledge needed to comprehend the role of AI, the relationship between humans and technology and the impact of the digital revolution on social cohesion.

Nevertheless, the digital divide runs along not only along geographic, economic or social lines, but is also inevitably the result of physiological causes. As the brain ages it loses plasticity, which weakens learning ability and receptiveness to new and more complex forms of knowledge. Thus, the pervasiveness of the digital revolution triggers, or threatens to trigger, an acceleration in ageing that could potentially result in difficulty keeping pace with and acquiring new daily and professional skills. This organically induced digital divide risks leading to exclusion, feelings of uselessness and even outright depression. If the still professionally active elderly are unable to gain proficiency in the new knowledge and technologies that come with the AI revolution, their risk of being demoted or reassigned becomes a source of severe distress.

The ethical/political challenge that follows is compelling: facilitating the elderly's full access to new technologies by investing in customized training methods capable of putting their potential and their extraordinary baggage of experience to best use.

Finally, there are various possible ways to prepare present and future generations for digital technologies, and it would be both simplistic and

myopic to stop at merely imparting information and techniques. Training in the acquisition and use of digital instruments offers an opportunity for the radical transformation of educational curricula – for optimizing those capacities for logical analysis, reasoning and critical thinking of which Artificial Intelligence does avail itself but which are uniquely reserved for human beings. We cannot delegate the interpretation of reality to technology, much less the direction of the transformation of reality. It is by means of critical thinking that the human being is able to claim responsibility for guiding and dominating technology – in other words, the dignity that sets humans apart from other autonomous agents.

Apart from education, other assets such as the right to personal freedoms should also be encouraged by the massive diffusion of AI. One research front could consist of analyzing how AI-enabled interlinkage and knowledge exchange can contribute over the medium/long term to closing the gap in people's enjoyment of human rights around the world. AI can reduce the divisions between people because it exponentially increases accessibility to the circulation of ideas and information. Because it offers platforms for shared planning and for reciprocal support and the undertaking of political initiatives by populations still forced to live in conditions of reduced freedom.