From Ingsoc to Skynet it is not only science fiction

From novels and science fiction to quasi-reality

Alfredo M. Ronchi
JRC S2D2 – Politecnico di Milano
alfredo.ronchi@polimi.it

Abstract

The paper will provide an overview on the following side effects of tangible and intangible impact of cyber technologies with specific focus on the oversupply of information (info-obesity), resulting in its devaluation and loss of trust to professional media; monopolization in the field of communication, information and digital technologies (mainstream communication, freedom of speech); the transformation of the Internet from a space for the free exchange of ideas into a tool for supervision and management (the betrayal of IT revolution) , with Internet companies turning into digital giants, moving from digital platforms to digital ecosystems and annexing not only cyberspace, but also real sector industries (monopoly and dominant position); the massive decrease in the level of critical thinking and the emergence of waves of information epidemics of national and global levels (mainstream communication, limited contraposition, fake fake-news); post-truth in its heyday, with public perception shaped more by means of addressing feelings and personal opinion rather than actual facts, with fakes, clickbaits, hypes and other tools introduced to form post-reality in the political and media culture; changing the system of values – with the new normal (semantic shifts, etc), new ethics putting personal free will and freedom of choice under question; traditional cultural regulators of social relations (covid 19 example) and processes being displaced by automated social algorithms (increasing role of algorithms and ML); blurring the borders between the real and the digital world, wide spread of simplified virtual mock-ups and simulacra; mass collection of data for managing people's behaviour (evaporation of privacy, data protection), formation of an appropriate economic imperative to direct the development for business, society and states; increasing the level of conflict in society (between individuals and groups – haters, discrimination) and between states (XXI Century warfare, soft concerns).

Science fiction movies

Exterior, night time, raining

"*I've seen things you people wouldn't believe. Attack ships on fire off the shoulder of Orion. I've watched C-beams glitter in the dark near the Tannhauser Gate. All those moments will be lost in time, like tears in rain. Time to die.*"

[Roy—Rutger Hauer—blade runner is a 1982 American science fiction film directed by Ridley Scott and starring Harrison Ford, Rutger Hauer, and Sean Young.]

This is one of the most famous and quoted sentences kept from one of the masterpieces of science fiction movies from the 1980s. Will lifes in the near future really get closer to the one depicted in the film, a dystopian Los Angeles in November 2019? Genetically engineered organic robots visually indistinguishable from humans will be integrated in our society. Cyborgs will perform the most dangerous or stressing tasks. We are already in that period of time, but a similar scenario is still far or very probably not realistic in our future. There are several science and technology fiction-movies depicting our future lifestyle, from Fritz Lang's Metropolis (1927) to James Cameron's Avatar (2009), passing through We probably feel much more immersed in an everyday reality like "Antitrust", directed by Peter Howitt (2001), or, even more realistic, and due to this concerning, "The Net"[1].

[1] The Net" directed by Irwin Winkler (Columbia Pictures Industries Inc.—1995).

Why do we refer to fiction to introduce serious topics like digital transformation and e-Citizenry? Because fiction sometimes anticipates a reasonable scenario of future society and lifestyles.
We do not foresee in a near future "replicants", "precocs", tele-transportation or flying cars[2] but we are aware of the potential revolution due to digital technology and e-Services.

"The Net", for instance, draws a not completely unreal scenario of identity theft. This movie outlines, if needed, the potential fragility of our digital-identity-based services and systems: police, banks, state archives, social security, ownership, personal data, etc.; they all rely on digital technology and are in some way exposed to hackers.

The purpose of this paper is to help in drawing and understanding a realistic scenario of what we might face in the near future as e-Citizen [24 – Ronchi], even if, as stated many times, "prediction is difficult, especially if it involves the future![3]" Sometimes the term "e-Citizens" simply identifies members of the network, Internet users. This paper identifies as "e-Citizen" a citizen surrounded by public administration's digital services, integration of cyber tech in his/her everyday activities at home or work, the transition from his traditional role and behaviour. Of course, we cannot forget the huge set of services provided by private organisations as the completion of the scenario.
A major part of the population has already started the journey from Citizens to e-Citizens; they already ask and receive certificates online, book a medical service, work in tight "cooperation with digital tools, and receive the feedbacks online or pay taxes and vote in this way.

"Back to the future", if we consider articles, books and movies from the past, we find that at least three aspects of future technologies are emphasised: the presence of objects with incredible features (or at least features that were unattainable at the time that the movie was released), the simplification of daily activities, and finally (often the most interesting aspect of the future to novelists and movie directors) the negative aspects of technological development, the dangers posed by *hardware and machinery*.[4]

Sometimes our predictions for the future come true, at least to some degree, and sometimes they do not (consider, for example, the evergreen prediction that by the 1970s/1980s/1990s... everyone would be using flying cars, just like those depicted in the film *The Fifth Element*[5] by Luc Besson).

I once attended a presentation by a technology forecaster—a "future guru" —Paul Saffo[6], the director of and a high-level researcher at the *Institute for the Future*[7], a "think tank" based in Silicon Valley that attempts to predict trends in various sectors. Initially I thought of another "researcher of the future" (from the movie *Back to the Future*), but Saffo did not have flowing white hair or a wild expression, so no time travelling (at least for the moment!). Instead, he presented a talk analysing technological potentials and current trends that could be used to predict the progress of technology over the next ten or so years. The scenario proposed for the first decade of the new millennium was that of businessmen that are permanently flying around the world and permanently connected to the global telecommunications network while doing so. These businessmen are

[2] Even if now "taxi drones" are under test in some countries (e.g. China, UAE), "Flying cars" were a typical representation of the future since the fifties.
[3] Quote from Neils Bohr, who won the Nobel Prize in Physics.
[4] In the world of cinema, we often encounter dark visions of a technological future, including Metropolis by Fritz Lang, Modern Times starring Charlie Chaplin, 2001: A Space Odyssey by Stanley Kubrick, Tron from Disney, The Lawnmower Man by Brett Leonard, Johnny Mnemonic by Robert Longo (based on the work of William Gibson), The Thirteenth Floor by Josef Rusnak, The Matrix by Andy and Larry Wachowski, Enemy of the State by Tony Scott, Nirvana by Gabriele Salvatores, Minority Report by Steven Spielberg, and the off-the-wall Brazil by Terry Gilliam.
[5] The Fifth Element by Luc Besson (Gaumont – 1997))
[6] https://www.saffo.com
[7] Further information is available at: http://www.iftf.org (last accessed Aug 2021)

continually racking up frequent flyer *bonus miles* and credit card *rewards* from travelling, which then enable them to travel to places that they really do not want to visit—a vicious circle!

Another interesting interpretation of the future of technology comes from Susan J. Blackmore[8], in a discourse that, among many other topics, encompasses viruses, religions and amanuenses. She believes [16 - Dawkins, 17 - Moritz] that the Internet functions as a *replicator* that can perpetuate content, just as nature makes species that are destined to survive more prolific, we will see later the idea expressed by Viktor Mayer-Schönberger and the right to be forgotten.

Consider the already mentioned, interesting and somewhat alarming forecast for 2005 published by the Japanese Banks Association in 1999. The forecast was delivered by the general manager of DoCoMo, Masao Nakamura, in 2000 while presenting the commercial response to their i-mode system. The study forecasted that in 2005 the vast majority of the clients of banks and telecommunications would not be human. Most transactions would be carried out between *machines*, while in some cases one of the actors would be an animal. The study predicted highway telepayment systems, prepaid cards (evolutions of the credit system) that are able to communicate directly with the current accounts of the suppliers, and wearable devices for kids, elderly people and animals that are able to converse with cars, warning the driver or triggering the engine control unit or ABS system if danger is imminent, as well as the attendance of virtual *videopresences* at ceremonies and job meetings, as made possible by three-dimensional holographic images. Predictions in the field of technology are sometimes or usually based on hints, some of the predictions come true other don't.

Virtual reality has also inspired many other artists, such as painters, sculptors, and movie directors (*The Lawnmower Man* directed by Brett Leonard - Allied Vision 1992; *The Thirteenth Floor* directed by Josef Rusnak - Sony Pictures Releasing; *The Matrix* directed by Lilly Wachowski and Lana Wachowski - Warner Bros. Picture 1999 - and its sequels).

Blurring the line between virtual reality, art, and entertainment, we should also mention some computer games such as *Final Fantasy*, as derived from the drawings of Akihiko Yoshida.

Designing the future

The cyber technology that really impacted society it is not the one in use in the 1960s or 1970s big mainframes operated by scientists dressed with white coat. Thirty years ago, information scientists and computer users witnessed the unprecedented revolution due to personal computing. This revolution was initiated by visionary researchers like Douglas Engelbart[9] and his "oN-Line System[10]" that is directly connected with "The Mother of All Demos", as retroactively termed its presentation at the IEEE on 9 December 1968, to do not forget his concept of a revolutionary device: the "mouse"; Butler Lampson, Charles P. Thacker, Robert W. Taylor and Alan C. Kay licensing in 1973 the Alto[11] computer and its object oriented interface ten years before Apple Macintosh[12]. In the 1980s Alan Kay, developing "Dynabook", introduced the concept of laptop computer[13]. We cannot forget of

[8] Please refer to Sect. 1.8.2. Susan J. Blackmore, University of the West of England, Bristol: http://www.www10.org/keynoters/speech/susan/Memes.html.
[9] On the occasion of the WWW 1997 Doug Engelbart introduced the concept of a "multidimensional" operating system showcasing a graphical interface associating each single process to a "dimension" of a n-dimensional interface.
[10] NLS—Developed by Douglas Engelbart and Dustin Lindberg at SRI International.
[11] Xerox Alto had a limited diffusion on the market, in the 1980s Xerox created Star a modified and cheaper follow-up of Alto.
[12] Steve Jobs understood the relevance of that revolutionary approach to computing and activated Lisa and later Macintosh projects.
[13] https://history-computer.com/products/dynabook-complete-history-of-the-dynabook-computer/

course the IBM PC released in August 1981, designed by a group of engineers directed by Don Estridge in Boca Raton, Florida.
Born at CERN close to the end of the 1980s Web technology flourished on the consumer and home markets in 1995, since that time another revolution was on stage. “Where to you want to go today” the Microsoft motto outlined the idea of a small world entirely connected online. Starting from the first decade of the twenty-first century a relevant number of Governmental Agencies, Institutions and Private Enterprises spread all over the world both in industrialised and developing countries invested time and resources on e-Services.

New garderobe

Cyber technology is increasingly merging any sector of our life, we are witnessing relevant changes due to both technological enhancements and modification of user requirements/expectations. In recent times the digital domain, once strictly populated by professional users and computer scientists, has opened to former digitally divided. Society [26 – Ronchi 2019] is changing under the influence of advanced information technology. Computers have been around for about half a century and their social effects have been described under many headings. Technology is evolving toward a mature “calm” [35 - Weiser 1991] phase, “users” are overlapping more and more with “citizens” [3 - Council of Europe 2001] and they consider technology and e-Services [25 – Ronchi 2019] as an everyday commodity, to buy a ticket, to meet a medical doctor, to access the weather forecast. Mobile devices, home appliances and IoT represent the most recent revolution in both technology and society, they are perceived as something different from computers even if they play, among others, the same role and immediately became part of our daily life, a wearable accessory as our wallet or wristwatch. Home assistant appliances like Alexa, wearable devices like smart watches, bracelets are becoming pervasive as well. Digital divide [18 – Pimienta] in its original semantic meaning is mainly bridged thanks to mobile position aware devices but now we must deal with a different divide the knowledge divide. The mass use of technology in all the fields impose to acquire a minimum level of knowledge in the proper use of cyber-technology including the field of cyber- security.

Platforms

The internet, apart from different potential benefits, gave an incredible boost to globalisation trend, platforms and regulations-vacancy paved the way to new monopolies deeply influencing society.
Citizens use to buy and sell goods online, book their travels and vacations, as well as enjoy a number of services unthinkable before the Internet from extremely vertical services to crowd services [32 – Surowiecki 2004] or funding. Platforms are the real “silver bullet” that created major opportunities and real impact on society and economy. A relevant part of digital transformation relies on platforms and standards, these aspects are directly linked with the “owners” of such platforms and standards, this can be considered a kind of monopoly not yet regulated, a kind of grey zone, so in the digital transition there is a potential risk to fall under control of few key players. This aspect was recently outlined by the censorship action of some platforms that cancelled user profiles and entire video channels opening the discussion on the balance of the rights between the owner of the platform and the user of the platform. This aspect can led to the infringement of the human right “freedom of expression” as we will see later.

The diffusion of platforms if on one side creates new opportunities on the other side “kills” several existent businesses. If on one side platforms open the “global” market to small and micro enterprises offering them a “window” on the globe. The access to global service platforms creates a shortcut between offer and demand cutting out major part of the traditional added value chain, as it was long time ago because of malls it is now because of platforms. The big difference is that

you don’t need to invest relevant capitals to feed your business, the key investment is the creation of the digital platform, the asset you own is the number of users both on the offer and demand side, this to do not consider the fiscal benefits they usually enjoy compared with the traditional retail system. This new model led to positively evaluate and size on the market companies having a relevant number of “customers” paying zero money to the company
On the occasion of the pandemic the extended use of lockdown boosted the access to on-line services ranging from government offices to on-line shops to buy goods and receive food and drinks at home including a massive use of social networks, music, and video streaming throughout the whole day.

Digital Transition

Nowadays there is a recurring buzzword: Digital Transformation (DX or DT) [27 – Ronchi 2020] – it is an opportunity or a nightmare? The pandemic strengthened this trend, digital transformation will help to mitigate the effects of the crisis, improve resilience. “Resilience”, by the way, another recurring term in the pandemic time. We all agree on the meaning of the term “transformation” but “Digital” has different meanings. Jim Swanson, CIO of Johnson & Johnson says “Digital is a loaded word that means many things to many people”.
“Say 'digital' to persons and they think of going paperless; another might think of data analytics and artificial intelligence; another might picture Agile teams; and yet another might think of open-plan offices". A comprehensive definition of the term Digital transformation should be the integration of digital technology into all areas of activity, from business to public sector, fundamentally changing how we operate and deliver value to customers or citizens. The adoption of digital technology represented a true competitive advantage, literally “Competitive advantage refers to factors that allow a company to produce goods or services better or more cheaply than its competitors. These factors allow the productive entity to generate more sales or superior margins compared to its market competitors.”
It is evident that digital transformation it is not a process “one size fits all”, each specific sector and even activity requires a particular approach and custom solution; this starting from the three main branches: citizens, companies, public administrations. Because digital transformation will look different for every company, it can be hard to pinpoint a definition that applies to all. Sometimes this means walking away from long-standing business processes that companies were built upon in favour of relatively new practices that are still being defined. In such a situation the “trial and error” finding by continues improvements the optimal solution is the practical approach.

Change in technology and user profiles cannot avoid impacting the market. The market is evolving in a very significant way. The diffusion of platforms if on one side creates new opportunities on the other side “kills” a number of existent businesses. The access to global service platforms creates a shortcut between offer and demand cutting out major part of the traditional added value chain, as it was long time ago because of malls it is now because of platforms. The big difference is that you don’t need to invest relevant capitals to feed your business, the key investment is the creation of the digital platform, the asset you own is the number of users both on the offer and demand side, this to do not consider the fiscal benefits they usually enjoy compared with the traditional retail system.
Following the schema of some of the recent revolutions the idea was: digital technology is disruptive cancelling a number of businesses, but new businesses will be created, the key point is that the specific nature of digital technology is actually creating less positions than the one eliminated. The visible effect now is an increasing number of workless people replaced by software and robots. In

some fields the transition is carried out adding some digital intelligence to optimize workers activity to evolve later on to fully robotized systems. Furthermore, everyone experienced in "ICT based innovation" knows that "It is not only a matter of technology". Human factors are an essential tile of the whole process as well as a re-thinking of the whole organisation and process. We must keep humans in the loop and carefully consider the social and economic impact due to digital transition.

Digital Transition is a critical process involving opportunities and threats, benefits, and drawbacks. In addition, there is a gap to be bridged due to cultural behaviours, age, and education.
One of the potential drawbacks is due to the deep technological intrusion affecting our daily life, we feel framed by cyber devices more than supported. Some evident outcomes of this feeling are the "right to disconnect[14]"—controversial reform of French labour law by the labour minister Myriam El Khomri back in May 2016 and the "right to obsolescence" or the "right to be forgotten" due to Viktor Mayer-Schönberger, the author of "Delete: The Virtue of Forgetting in the Digital Age"[15].

The "right to disconnect" is self-explanatory and states the abolition of non-stop "digital slavery", the "right to be forgotten" refers to the intellectual property from the "continental" standpoint that, in addition to the "economic" rights identifies, even more relevant, some moral rights like paternity, adaptation, modification, ... "withdraw". The author has the moral right to "withdraw" his work of art from private or public environment. If we keep the similarity in the field of personal data we must claim for the right to withdraw them from the "digital universe"; this right is usually termed "right to obsolescence" or the "right to be forgotten". Viktor Mayer-Schönberger, the author of "Delete: The Virtue of Forgetting in the Digital Age" [12 - Mayer-Schönberger 2009], traces the important role that forgetting has played throughout human history. The book examines the technology that's facilitating the end of forgetting: digitization, cheap storage and easy retrieval, global access, multiple search engines, big data analytics, machine learning, infinite replications of information, etc.
If it is true that our ancestors survived the evolution process because of their ability to transfer to future generations relevant information thanks to primitive forms of writing, the dangers of everlasting digital memory, whether its outdated information taken out of context or compromising photos, the Web won't let us forget, as is well evident and already creating troubles. The supporters of a "natural" approach propose an expiration date for digital information or a progressive vanishing of data as it happens in the human world. Other experts propose to apply the moral right of the author/owner to "withdraw" his data, and here comes the first crucial point: author, owner, or subject...? A vanishing memory offers the ability to make sound decisions unencumbered by the past, offers the possibility of second chances.

All these to do not mention the cultural, social, and economic impacts [19 – Prado] not always positive especially in a long-term perspective. Technologies originally conceived by idealists to provide much more freedom and wellness to humans took then a wrong path framing humans due to all the constraints placed upon us with new technologies. For instance, as liberating as they are—by providing flexibility and instant connectivity—we have become enslaved to our devices, fearful of losing out information and access in an increasingly competitive and fast-paced world. Consequently, our bodies have suffered, as have our minds (due to information overload or "info-obesity"), what of our work-life balance—and this is just to begin with! Ranjit Makkuni's paper "Betrayed IT

[14] loi n 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels https://www.theguardian.com/money/2016/dec/31/french- workers-win-legal-right-to-avoid-checking-work-email-out-of-hours, last accessed January 2019.
[15] Mayer-Schönberger Viktor, Delete: The Virtue of Forgetting in the Digital Age, ISBN-13: 978-0691138619, Princeton University Press 2009.

Revolution"[16] outlines a vision for new design of devices, clutter-free access to web documents to create deeper learning experiences. At the implication level, the Makkuni rethinks implications for new design of web mark-up languages that support the creating of 'privacy' based secure browsing.

Following the same fil-rouge, on March 29th 2017 Congress passed a law that makes it legal for your Internet Service Providers (ISPs) to track and sell your personal activity online. This means that things you search for, buy, read, and say can be collected by corporations and used against you. To fight against such privacy breaching some initiatives have been carried out; "Internet Noise" is an application that could be activated during your Internet browsing activity in order to minimize the risk of being profiled. Internet noise will visit non-stop a random set of websites adding an incredible amount of "noise" to your browsing history. Internet Noise is actually hosted by the GitHub website[17].

Cyber nightmares

After the explosion of the use of the Internet in the middle of the 1990s old and new dangers started to populate the network directly delivered on tablets and mobile phones.

Cybersecurity[18] [6 – European Union 2013] was one of the key enablers to enter the cyber era and activate e-Services, it contributed significantly to build confidence in these sectors, so citizens started to use home banking and e-commerce as well as e-health and e-government. Through time the number of different connected devices increased, laptop, tablets, smartphones, IoT assistants, and it became more complex to maintain an adequate level of security and preserve confidence.

As a side effect of globalisation and massive use of cyber services and the "APPification[7]" of society the number of crimes both perpetrated at local and global level is growing up.
As we all see cyber technology is merging every day with an increasing number of sectors, from the diffusion of smart phones always-on onward we embedded cyber technology everywhere, any sector, so today and much more tomorrow we will deal with relevant impacts on society and an increase of cybercrimes or cyber abuse/misuse [29 – Ronchi 2018]. Our washing machine might be hacked by ransomware, fridge might send orders for tons of food, Alexa might spy our private life and broadcast audio, smart home might not be any more perceived as "sweet".

Current digitisation of almost everything including security and government services has created increased vulnerability to cyber-attacks, Governments and Law Enforcement Agencies are aware of this and look for potential countermeasures not only following traditional solutions [5 - European Commission 2017]. Citizens, small, medium, and big enterprises are more and more storing their data and information on clouds, procedures and production pipelines are more and more automated and robotized, products themselves are incorporating increasing portions of cyber technologies, software as a service approach is quickly gaining the stage. The more we become digitalised, the more we are vulnerable to hackers and hybrid threats[19] [7 - European Union 2016]. Of course, the overall scenario includes many other aspects and "shades"[20] [9 - European Defence].

[16] Outcomes WSIS Forum 2018. ISBN 978-92-61-25151-2. https://www.itu.int/net4/wsis/forum/2018/Files/documents/outcomes/WSISForum2018_ForumTrackOutcomes.pdf, last accessed January 2021.
[17] https://slifty.github.io/internet_noise/index.html, last accessed January 2021.
[18] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf or http:// eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri1⁄4CELEX:52013JC0001&from1⁄4EN, last accessed January 2021.
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN
[20] Ronchi A.M., Soft but still concerns, proceedings International Conference on 'Homeland' Security Emerging Trends, Challenging Aspects - Hasan Kalyoncu University, Turkey 2021

The discontinuity ignited by cyber technology and its pervasiveness created the fundamentals for a completely new scenario where the malicious use of digital technologies is becoming a new business opportunity not only as a direct mean to steal "assets" and take control of smart objects but even under the format of “cyber-crime as a service”, at the same time terrorists found in cyber technology the best mean both to run their activity and to enrol new “adepts”. To build a sounding information society we must efficiently counteract cyber-criminality and establish a clear vision on legal behaviours in the cyber-world.
It is common knowledge that organizations worldwide face a dangerous shortage of network security personnel that have the skills required to defend against cyber-attacks. At the same time the number of breaches grows steadily, with the incident response and attack defence techniques being time-critical, as the majority of compromises (87%) occurring within minutes[21]. This situation illustrates the problem of lack of preparedness organisations face in defending effectively against cyberattacks.

More recently the issues concerning ethics[22] [31 - Stuckelberger], data ownership, privacy and more arose as well as the impact of cyber technology on society and economy [10 - IFAP].

1. Risks associated to the diffusion and pervasive role of ICTs are no more concerning our computer and data but involve privacy, safety, public opinion, governments, national security, transportations, manufacturing, home appliances, sometimes even specific aspects of freedom as stated by the Universal declaration of human rights[23]; e.g. Article 12[24], Article 19[25], Article 21.2[26]. New concerns Merriam Webster: Ethic, http://www.merriam-webster.com/dictionary/ethic [13 - Merriam]

are due to old and new technologies, artificial intelligence was popular in the 1990s and impacted citizens making “intelligent” washing machines, photo and video cameras and a number of devices, big data analytics is everyday providing new outcomes and services, last but not least quantum computing is close to reach the market offering a completely new set of applications.

Ingsoc: Is Privacy evaporated?

The concept of "data" as it relates to people’s everyday life is still evolving [1 - Burrus 2014]. We inherited the concept of copyright and we, more recently, faced the concept of privacy [13 - Merriam Webster]. Copyright and copyleft are two sides of the same coin, they both pertain to the intellectual property of something, but which is the most relevant... if any? Traditionally, copyright and copyleft have been regarded as absolute opposites: the former being concerned with the strict protection of authors’ rights, the latter ensuring the free circulation of ideas. Indeed, a commonly held belief about copyleft is that it begins where the boundaries of copyright end, spreading over a no man’s land of more or less illegal exploitation.
Copyright and privacy; it seems reasonable that both derive from the concept of data ownership. we take a picture of an agreeable landscape, add our name as the author/owner on it and publish it on our web page; if someone else downloads our picture, crops the author’s name, and posts it on his/her website, it's a copyright infringement. Nowadays open data is one of the buzzwords most popular; if a public authority will release different sets of “open data” apparently anonymised [34-

[21] Commission
[22] Ethics was one of the key aspects considered by UNESCO IFAP since 1995, the “Code of Ethics for the Information Society” was released in 2011 on the occasion of the General Conference 36th Session held in Paris // https://unesdoc.unesco.org/ark:/48223/pf0000212696
[23] Universal declaration of human rights https://www.un.org/en/about-us/universal-declaration-of-human-rights
[24] “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.ù2
[25] “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”
[26] “Everyone has the right of equal access to public service in his country.”

UK Government], the combined use of them may lead to identifying your personal behaviour; that's a form of privacy invasion or perhaps violation [4 - Darrow 2016].
Historically speaking, the idea of even owning information is relatively new[27]. The earliest copyright laws, which granted the creator of artworks, among the other rights, exclusive rights to duplication and distribution of said work, first appeared in the early 18th century. Nevertheless, it would still be hundreds of years, however, before the concept of "data" as we understand it even began to develop. As it appears from the previous paragraph, ownership of data [14 - My Data] is not yet a well-defined legal concept. We all agree about privacy and intellectual property infringement but personal data even if clearly belonging to the same “galaxy” are not properly identified and protected. If this represents the state of the art in general, it might not always be the case. Individual nations and international organizations are attempting to establish rules governing who can collect what data and what they're allowed to do with it. Germany, in fact, has a legal concept known as "informationelle Selbstbestimmung" or informational self-determination. What does informational self-determination mean? An individual has the right to decide for himself or herself what information can be used by whom and for what.

Back to the fresco depicted by the fiction movie sector we find “Enemy of the State” is a 1998 American conspiracy movie providing a realistic picture of framing technology, let’s have closest look to the script:

Brill [Gene Hackman]: *The government’s been in bed with the entire telecommunications industry since the forties. They’ve infected everything. They get into your bank statements, computer files, email, listen to your phone calls... Every wire, every airwave. The more technology used, the easier it is for them to keep tabs on you. It’s a brave new world out there. At least it’d better be.*
...
Thomas Reynolds [Jon Voight]: *Ten-year-olds go on the Net, downloading encryption we can barely break, not to mention instructions on how to make a low-yield nuclear device. Privacy’s been dead for years because we can’t risk it. The only privacy that’s left is the inside of your head. Maybe that’s enough. You think we’re the enemy of democracy, you and I? I think we’re democracy’s last hope.*

It is a thriller film directed by Tony Scott and starring Gene Hackman, Will Smith, and Jon Voight.

We live in a world in which there are already countless sensors and smart objects around us, all the time. The car we drive, the phone in our pocket, our wristwatch, the clothes we wear, are smart and connected; then the concept of “private” becomes far more ephemeral. This is not enough; what it is not collected by APPs will be collected in a seamless mode by IoT[28]; of course, IoT will add a lot to our life, but this will cost us a significant part of our privacy. The world we contributed to create, filled up with cutting edge technologies fully connected, take us to a simple, even if uncomfortable to hear, truth: we are unable to prevent all possible data tracking. Cameras, satellites, sensors, and software virtually everywhere ensure that, no matter how much technology you eschew, someone can get some data from you. Your credit card company “tracks” your purchases and, in one word, your lifestyle. Your phone carrier “tracks” your calls, social relations, and geographic location and more thanks to your inseparable ”buddy” the smart phone. Your preferred software platforms track your contacts, your position, and visits throughout the day, asking if you know that place or the score that experience. Your area’s law enforcement tracks the roads and intersections you walk

[27] My data belongs to me. http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-dis cussion-personal-data-virtualisation-society-wsis10-review
[28] SAS report on The Internet of Things. http://www.sas.com/it_it/offers/ebook/iot-visualise-the-impact/index.html

through or drive down every day. Local administration CCTVs or private safety cameras follow you within shops or residential buildings, even inside the elevator. Your home cameras do not only capture the actual location of your cat but send somewhere on a cloud your video clips of your private environment. Your smart watch or bracelet acquire health date about your blood pressure, your heartbeat, your sleep, and oxygen in the blood sending to the same or a different server your data potentially reusable for business purposes.
Unless we decide to move to the mountains, renouncing to today's technology, some tiny data that describes our behaviour and us will probably be tracked. No matter, you may say, we have nothing to hide, but what about the use, abuse or misuse others may do?
The Internet Revolution gave a boost to data creation and dissemination, MAC addresses, web logs, and intentional or unintentional[29] applications to websites and services, and social platforms ignited the sedimentation of personal and many times sensitive information apparently lost in the cyberspace. Very soon the first drawbacks come on stage: privacy infringements, stalking, hacking, cyber-crimes, stolen identities, darknet and more [2 - Bohn R. 2009].
However, Google, Facebook, Twitter, Apple, Microsoft, Amazon, and any of the other hundreds of companies that can and do collect data about you can use "your" data for all kinds of amazing things. In the "Appification" era there are almost no limits to data collection and reuse; "someone" knows exactly where you are now and where you have been, APPs may collect your medical data, fitness program, your expenses or collect and analyse your contacts, your photos or video clips, access your smart phone camera and microphone. What about the push message asking to provide details about your activities yesterday evening, something that your digital "buddy" was unable to trace? Your bank will suggest, accordingly with some intelligent algorithms the average monthly expenses due to profiles matching with yours and send an alert if you are exceeding the limit. Don't you feel framed by such "intelligent" environment? Social and communication media complete the panorama adding a "private depth" to the general fresco, ad-hoc defined tweets or posts may collect and analyse users' feedbacks in order to guide or anticipate citizens 'actions and feelings. In recent times crowd data collection, open data, and big data, more or less anonymised, have provided the big framework where to collect all the different tiles. Online malls and delivery platforms offer, in addition to analyse your browsing, the opportunity to save a "wish list" to better focus on the market trends.

Following the same fil rouge on the borderline between licit and illicit activities, simply consider a typical example, an unseen observer that follows you and take notes about all the different places you visit and the time of your visits; he does nothing with this information, simply stores it in his notebook, he is unseen, and you will never face him and discover his activity; basically, in doing so he didn't break any law. His behaviour is unconventional but still legal. If you act in public spaces or visible by public there are no laws that state that you are the sole proprietor and owner of the information regarding your public life; the collection of this information doesn't violate any right. If we look in law, the closest legal offence in such a situation is stalking even if this offence usually is directly connected with harassment; but the unseen observer does not ever interfere with you so no harassment, no stalking even because the unseen observer is your smartphone, and it can't be convicted of stalking you. This is what happens when some "autonomous" on-line applications start showing you your yesterday's paths across the city showing some geo-referenced pictures you shot asking for the reason you went there and what you did in the 15 minutes you spent stopping on the way to your destination. Of course, the system recognises your friends in the pictures and next time probably will ask you why you met them.

[29] Sometimes clicking to receive information or services we subscribe a contract that can automatically be extended to "sister" services or applications.

Normally the first thought in consideration of such "assistance" is a positive appreciation for the care and support in keeping track of our activities as a kind of "assistant" or "mayordom" at our full service, afterwards we start feeling this "cyber-being" too present too invasive and the challenge is to reconquer our privacy.

Anyway, even if we enjoy some benefits on the reverse there is a real risk of abuse, misuse, and misinformation thanks to these technologies. The movie "Citizen Kane[30]" directed and interpreted by Orson Welles in 1941 outlined the relevant "power" of journalism[31], the movie "Network[32]" directed by Sydney Lumet outlined the power of television in 1996 and perhaps "The Net[33]" and "S.Y.N.A.P.S.E.[34]" together with "The Social Network[35] (2010)" started to outline the power of the Internet.
Computer biometrics is nowadays very advanced; so, starting from the Apple tools to recognize people appearing in your pictures once you gave the system two or three samples, a group of Russian developers released in recent times a powerful application, FindFace, that performs in real time the face recognition even of multiple persons and connects them to their V-Kontakte, the Russian version of Facebook, page. This enables users to take a picture with the smart phone on the street on in a disco and immediately discover the identity of the subjects. Is this a potential infringement of privacy? Is this a powerful tool for stalkers? Technological evolution does not have limits; it is already available for the professional market, e.g., law enforcement, a full version of FindFace offering far better performances without the limitation to V-Kontakte subscribers.
Biometric identity checks are already available and used on consumer devices, so we can authorise a money transfer to our bank thanks to our face, iris, or fingerprint, we can open safety doors simply showing our face to the video camera, public CCTV can offer high quality images to identify criminals.

News and Media are key elements in the global society. CNN, BBC, Al Jazeera[36], Al Arabiya[37] are writing the history of the planet 24/7 and on the grassroots side YouReporter[38], Twitter, and Instagram are complementing this effort. The risk of misuse of such technologies and misinformation is probably higher than in the past. So, it might happen that we will watch an updated version of the movie "Wag the Dog[39]" in the near future.

In June 1993 "The New Yorker" published a cartoon by Peter Steiner. The cartoon features two dogs: one sitting on a chair in front of a computer, speaking the caption to a second dog sitting on the floor "*On the Internet, nobody knows you're a dog*". Right or wrong, that's one of the features of the Internet. That's the story of the Syrian "lady" blogging in 2011, the starting point for the "dark power" of the Internet, the realm of hackers and cheaters. The key point is what is written or anyway appears on the Internet is news by itself. There is no more time to check everything; the Internet provides real-time news. We will come back on this aspect dealing with news and reliable sources and "Appification" related problems and informed consent will be also considered later.

[30] Citizen Kane directed by Orson Welles, 1941 RKO Pictures.
[31] The Italian title of the movie was "The forth power" in analogy with the third "The workers" depicted in the extraordinary painting by Pellizza da Volpedo.
[32] Network, directed by Sydney Lumet, 1976 Metro-Goldwyn-Mayer United Artists.
[33] The Net", directed by Irwin Winkler (Columbia Pictures Industries Inc.—1995).
[34] S.Y.N.A.P.S.E. (Antitrust), directed by Peter Howitt (Metro Goldwjn Mayer—2001).
[35] The Social Network directed by David Fincher (Columbia Pictures 2010).
[36] www.aljazeera.com/, last accessed January 2020.
[37] www.alarabiya.net, last accessed January 2021.
[38] A recent event in the field of newspapers is the birth of The Huffington Post, inventing a completely new approach to newspapers.
[39] Wag the Dog (1997), Dustin Hoffman, Robert De Niro and Anne Heche, directed by Barry Levinson.

The evolution of online news due to the social web and the birth of "prosumers" did the rest. Twitter, YouTube, Facebook, Instagram, Telegram, and blogs represent a real revolution in the domain of news.
As already stated, the Internet is much more a counter-power than a power; the common idea about the Internet is the network as a powerful tool of freedom and democracy. This is probably true, but the opposite is even true, the misuse of the network and misinformation disseminated and empowered by the Internet and its powerful mechanism.
Cyber IDs allow multiple IDs and potentially Dr Jekyll and Mr Hyde. We are flooded[40] by user-generated content (UGC) largely without any qualification and certification of the source. Many times, the drawback attributed to the amanuenses is affecting even web publishers: information and content is re-used and re-published adding or replicating errors and bugs. The short content production chain, sometimes even limited to a one-stop shop, does not include an editor in chief or a supervisor; so far, the overall quality of prosumer content and information is quite low.
As an IBM top manager told recently on the occasion of the Global Forum: "Do not trust in any information coming from unknown source."

As clearly anticipated by several movies, stolen digital identities, digital desaparecidos, and other digital crimes, these are the nightmares of the cyber age. In the near future, it will be necessary to find a satisfactory equilibrium between privacy and the "open" systems enabled by ICT. On the one hand, technologies should enable each of us to be more self-sufficient and may indeed push us to become more "removed" or isolated from the rest of the world. On the other hand, they produce and store an incredible amount of "evidence" (files, transactions, video-clips, pictures, etc.) documenting our existence moment by moment. The more technology we use, the more visible we become. High technology is now used to such an extent that it is often possible to track people using their devices. Internal and external video-surveillance systems connected to computer vision-based systems are able to identify a person, a vehicle and their behaviour in both 2D and 3D. ATM transactions and credit card usage indicate our movements, tastes and lifestyle. The contents of our PCs and our Internet activities are monitored by spyware, fished, and hacked (in the most optimistic vision, such activities would simply lead to the creation of personal profiles for e-Commerce applications, but that is a different topic altogether). There are also privacy concerns related to the general use of RFID and IoT. These technologies effectively give machines "X-ray vision". Cyber pickpockets can use it to play "who's got the Rolex", or even simply "who's got the contactless credit card".
The massive use of contactless devices and even more the large diffusion of social media, IoT and CCTV enhanced these concerns. A hot topic is for sure the release of "open data" sets and the analysis of "big data". Even if at the end the effect is similar, we can subdivide in two main branches privacy breaches: "voluntary" and "third parties". The first group refers consciously or unconsciously to risky behaviours such as providing personal information to register for a service or authorizing the access to personal data to install an APP, and more. The latter refers mainly to hacking or the publication of non-sufficiently anonymised data sets by institutions and authorities. It may happen that in cross-referencing different open data sets some "identity" of the data holders is unintentionally disclosed. The second potential breach in privacy is much more care of public administration; in addition, the diffusion of the one-time password (OTP) access application on mobile phones overcharges our phone of critical duties. If we lose our phone or if it will be stolen, we will suffer a real nightmare, like the ones depicted in many Hollywood movies. Rules and obligations may differ from country to country and from continent to continent, but the importance

[40] Roger E. Bohn, James E. Short (2009) How Much Information? 2009, Global Information Industry, Center University of California, San Diego.

of keeping personal information[41] private is always recognised and protected. It is mandatory to ask for explicit[42] approval every time personal information is stored in any format, *". . . consent as defined and further specified in EU Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website*"[43]

Freedom of expression

If the early stage of Internet communication was based on the so-called "netiquette", a kind of Galateo[44] or Bon Ton of Internet users, the advent of Web X.0 and the social web requires more specific rules addressing first of all the field of ethics and privacy. Of course, freedom of expression is one of the most appreciated opportunities offered by the network and it is already evident that any kind of top-down censorship or control does not succeed even if the concept of Cyber Sovereignty, exists and is promoted. The evident vocation toward freedom of expression is many times a direct cause of governmental censorship forbidding social applications in some countries. So it happens that Twitter, Facebook, Instagram, YouTube or even some thematic websites are not allowed. Here apart from political, ethical, and philosophical issues may come to the fore the economic and financial aspect of entering that market adhering to the requested censorship or not[45].

Freedom of expression is usually associated with the terms hating, online libel, hoax, fake news this because the improper use of freedom of expression can generate such negative behaviours. Of course, such extensive and negative interpretation of freedom might generate some reactions that can be even worse than the problem itself. A typical and sometimes concrete example 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.

The Council of Europe at Article 10 of the European Convention on Human Right[46] states:
"1 - *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*

2 - The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

[41] Directive 2002/58/EE of the European Parliament and of the Council of 12 July 2002 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML, last accessed February 2021.
[42] Informed consent to store and use for specific clearly stated uses the requested information.
[43] Directive 2002/58/EE of the European Parliament and of the Council of 12 July 2002 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML, last accessed February 2021.
[44] Monsignor Giovanni Della Casa was a Florentine poet, writer on etiquette and society; Galateo overo de' costumi was inspired by Galeazzo Florimonte, Bishop of Sessa.
[45] E.g. markets potentially offering "billions" of additional customers. Sometimes the censorship is not declared but the bandwidth devoted to the specific service or website is so narrow that it is practically impossible to connect.
[46] https://www.echr.coe.int/documents/convention_eng.pdf

Which principles concerning freedom of expression are shared by the European Commission and Internet Governance Forum? On the basis of the analysis of its activity, the IGF might be considered too close and too committed to the interest of a strict number of ruling members. This was already evident on the occasion of the dispute on the issue of a new global agreement on Internet regulations. Anyway, the IGF Best Practice Forum in 2020[47] and the national, regional, subregional and youth IGF initiatives (NRIs) annual programme scores the interest in Digital Rights & Freedoms 28 on 30, higher priority respect cybersecurity and Internet governance ecosystem.

What are the key principles and objectives that guide the European Commission's work in this area?[48] The aim of the European Commission is to defend access to open Internet and freedom of speech.
On the occasion of the annual global conference of the Internet Governance Forum (IGF) held in Baku on 5–9 November 2012 the European Commission defended the open Internet and promoted the Internet as a frontline in efforts to ensure freedom of speech globally.
The delegation from across the Commission made a strong intervention into debates about the future of Internet governance at the IGF. The EC delegates strongly defended the view that there is no need for a new treaty to regulate the Internet. Instead, the multi-stakeholder model should be promoted further and be made more inclusive and responsive. More generally the Commission emphasised the need for the Internet to remain a vibrant environment for innovation and economic growth, and to improve as a space where transparency, democracy and protection of human rights are guaranteed.
As a key funder of the Internet Governance Forum, the Commission co-organised four sessions of the IGF 2012 conference:
1. on the protection of the rule of law in the online environment, to discuss different issues related to the responsibility and role of Internet service providers in preserving freedom of speech;
2. on the evaluation of the Internet Freedom Initiatives, for the promotion of the No-Disconnect strategy and exchange of information about other similar initiatives in different countries;
3. on media pluralism and freedom of expression in the Internet age, which is currently addressed by the High-Level Group on Media Freedom and Pluralism established by Vice President Kroes;
4. on how to make Internet a better place for children, to discuss the responsibility of different actors in the area of child protection on the Internet.

The European Commission provides a definition of Freedom of expression and information[49] as.
"*1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.*
2. The freedom and pluralism of the media shall be respected."
This right is enshrined in article 11 Freedom of expression and information of the Charter of Fundamental Rights.

On the occasion of the WSIS Forum 2021, Prof Lynn Thiesmeyer[50] outlined some drawbacks of digital transformation "*A number of countries, notably those with a high level of internal conflict, are monitored by international commissions and tech organisations due to their high degree of Internet*

[47] https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/11138/2452
[48] Mr Andrea Glorioso, European Commission Policy Officer at the DG Information Society and Media, on Tuesday, 29th May 2012, to discuss the European Commission's position on various Internet governance issues.
[49] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN
[50] Dr. Lynn Thiesmeyer, Keio University, Digital Transitions to Digital Despotism: Cyber-insecurity and its Regional Threat to Connectivity - Outcomes of the WSIS Forum 2021

filtering and censorship. Since February 1, 2021, however, the case of Myanmar has gone beyond censorship. It now includes blocking access to the Internet and the Cloud, and shutting down a large portion of citizen access to Internet and wireless technology. Further, internet banking technology has been used to seize the assets of international organisations. These actions threaten the digital and informational freedom and security of the country, and also of its regional partners in business and in development assistance. ...The digital transformation is a tool and a process that not only can empower and liberate nations and their capacities but can also be used to remove and destroy those capacities, including the digital transformation itself. In addition to working directly against Sustainable Development Goals 9, 11, and 16, these actions deny both domestic and international freedom of communication, knowledge, and economic activity among ordinary citizens as well as between the nation and its economic partners. The lack of international standards and countermeasures is hampering approaches to the growing regional cyber-insecurity, but we also need to examine particularly the incentives and disincentives faced by Myanmar if it is to regain free and comprehensive ICTs and access."

Education

With the spread of the coronavirus, the education system is facing a new crisis, extended school closures may cause not only loss of learning in the short term, but also further loss in human capital and diminished economic opportunities over the long term.

Before the outbreak of the coronavirus pandemic, the world was already dealing with a learning crisis, traditional education methodologies were already outdated. An educational and communication divide was already on stage between millennials (generation Y) and the educational system. It is a common understanding that recent generations represent a discontinuity if compared with the past ones. Such discontinuity or, if preferred, singularity is recognised both by adults complaining because their children do not pay attention or are getting bored by learning and, by adults, that discovered new skills and capabilities in young generations.

People that grown up playing video games, browsing the Internet, chatting, and looking for help online in communities, they use technology seamlessly. A new model for communication processes is required.

Young are used to receiving information really fast. Their brain seems to be able to process information in parallel and multi-task. So, they prefer direct/random access to information and content. Graphic and Video content are longer preferred than text. They use to look for support and buy things online and use to belong to one or more communities.

This is a side effect of their special skills acquired in hours and hours of digital tasks. Social psychology offers compelling proof that thinking patterns change depending on an individual's experiences. A sufficiently long training may activate this phenomenon. In fact, some researchers believe multi-sensory input helps kids learn, retain, and use information better. So, the Apple motto "think different!" is much more than a motto.

As already outlined a renovated approach to education it is not only a matter of network infrastructure and computers, but also a matter of humans so both students and teachers need to adapt to collective online learning, improve emotional and behavioural self- regulation.

Having the evidence that traditional didactic doesn't match with young's expectations we need to take advantage from the additional need to make educational activities more resilient to start reshaping the system to fit with both requirements: resilience and generation Y compliance.

Education system must cope with such requirements and take advantage from similar new skills even if there are some "side effects" that must be amended or at least mitigated. Direct access to information and related hyperlinks may create some drawbacks, among the others, a kind of

"surface knowledge", many times more suitably identifiable just as "information", without the required contextualization and logical connections with other items, plus the risk to lose the logical path related to the key topic. So kids use to say "*Why I need to memorize historical events when I can simply "google them"*?"
The overall effect is to create "archipelagos" or even "islands" of "surface knowledge" without connection with the rationale background or deep knowledge on the specific topic. In addition to this both the social networks and online resources could provide fake or unreliable information many times in absence of critical thinking on the student's side. So, in parallel with the setup of education innovation, that is nowadays led by ICT, we must improve student's critical thinking and technology awareness. The latter includes specific knowledge about potential risks associated to an improper use of technologies.
Mentors need to upgrade their knowledge in ICTs possibly bridging the generational gap as much as possible that means to use social media activating a tight and multilateral interaction with students. Leading the change having proactive approach to the natural evolution of the content domain. Time will solve this problem; in fact, the early generation X is coming on stage.

The Pandemic

In the last decades we faced different pandemics from AIDS to Ebola in 2020 the term pandemic took the real meaning to be global and really creating a global concern, the "transversal" risk of death. Scientific studies and evidence show that COVID-19, if not promptly cured, is more severe an illness than is seasonal influenza, and is probably more contagious than are seasonal influenza viruses, having a basic reproduction number (*R*0) nearly twice as high.
COVID-19 was declared a pandemic by WHO[51] on March 11, 2020, the first non-influenza pandemic, affecting more than 200 countries and areas, with more than 59 million cases by May 31, 2020. Countries have developed strategies to deal with the COVID-19 pandemic that fit their epidemiological situations, capacities, and values.
The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. Such "countermeasures", isolate infected people, locking down cities and countries, are not new, they recall medieval times plus some usual precautions in case of flue like to wash hands, keep a reasonable distance from other people, do not touch your mouth, nose or eyes with dirty hands and in case of close contact wear a surgery mask as Chinese and far eastern people use to wear since long time, nothing better and more up to date? Technology incredibly progressed though the time and more specifically cyber technology reinvented itself several times. We have crowd services, social media, IoT, sensors, AI, machine learning and any kind of privacy border line technology no chance to help fighting the pandemic? One of the first cyber tools to be identified was the contact tracing APP rolled out to automate labour intensive tasks critical to containing the spread of the virus. Of course, the ability to trace in real-time our contacts impact our privacy and in some way our freedom, let's get much more in detail on potential privacy infringements and the golden balance to be find between privacy and public health.

Contact tracing applications

We know that since long time ago our "activities" were traced[52], nevertheless, citizens are really concerned about privacy issues related to medical folders and contact tracing even if, they are not

[51] World Health Organisation - https://www.who.int
[52] Ronchi, A.(2019) , eCitizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer

really concerned in case of sport and wellness APPs that use to transfer our medical data to some almost unknown centralised servers.
The pandemic moved the focus of already existent tracing application from security and marketing to interpersonal contacts, of course this sector was already active in the security field but become appealing to a wider set of software developers because of the incredibly wider potential application both on citizens and government side.
There are several issues and challenges connected with contact tracing applications. In the EU, the general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19.
To start we can split into two main sectors both issues and challenges: citizens side and health authorities' side.

If on the citizens side the positive aspect is to be alerted if any existent contact is dangerous the key concern is about to limit the infringement of their privacy and have a clear trust relationship with the software company and the government including the unit responsible for storage of data. We all know that health[53] is probably to only sector where privacy is applicable even to the owner of data him or herself. These privacy concerns mean even the choice to download / install and activate the application. For sure the discovery that time ago, the updated version of Android and IOS had a specific section devoted to connecting with tracing APPs didn't enforce this trust relation knowing that anyway our phones are already traced by Telcos.
Since the start of the pandemic, governments and stakeholders involved in the fight against the virus, such as the scientific research community, have been relying on data analytics and digital technologies to address this novel threat. Governments and private actors turned toward the use of data driven solutions as part of the response to the COVID-19 pandemic, raising numerous privacy concerns. In the EU, the GDPR data protection [22 2016/679] legal framework was designed to be flexible and, as such, can achieve both an efficient response in limiting the pandemic and protecting fundamental human rights and freedoms.
There are several paragraphs within the UN Declaration of Human Rights[54], as we have already mention, related to the management of the pandemic let's recall two of them: *Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. Article 13: 1. Everyone has the right to freedom of movement and residence within the borders of each State; 2. Everyone has the right to leave any country, including his own, and to return to his country.*
Data protection[21 Protection] is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures. Because the virus knows no borders, it seems preferable to develop a common European, if not global, approach in response to the similar crisis, or at least put in place an interoperable framework.

On the side of health authorities apart from the need to ensure the full Institutional ownership of data ensuring no data leak or improper use, misuse of information, one of the key aspects is the widest installation and activation of the tracing tool. The return value of such campaign is useful and relevant only if a significant part of the citizens activates it. A draft list of the key aspects to be considered is:

- Widespread number of citizens installing and activating the application;

[53] Ronchi, Alfredo M., (2019). e-Services: Toward a New Model of (Inter)active Community, ISBN 978- 3-030-01842-9, Springer (D)
[54] https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

- A comprehensive national epidemiologic strategy articulating instrumental support to the public health system, manual contact tracing;
- The model chosen (technology used, architecture retained, definition of 'proximity' between the devices, both in terms of distance and duration, etc.);
- Widespread access to mobile devices and connection (considerable segments of the population are unable to acquire or use them, in particular high-risk groups such as healthcare personnel, disabled and elderly people).

The use of such applications has been planned in conjunction with a set of measures that all use non-pharmaceutical interventions. Different countries all around the world issued specific norms and regulations concerning the guidelines to develop contact tracing APPs. The European Institutions published clear regulations and recommendations concerning the design and development of the APPs. Key aspects to be carefully considered were privacy issues starting from the personal information requested to download and activate the APP, the anonymisation, sometimes pseudo-anonymisation, of data to be exchanged to validate potential risky contacts, the request of consent to store contact info and related upload on local, semi-centralized or centralised servers. How long personal data will be stored on servers, who is in charge as data controller, and who is entitled to access or share such data. An additional relevant aspect concerns the voluntary or compulsory use of the APP not only related to the activations but much more related to the need to have a positive/green feedback from the APP in order to perform an activity or enter a specific place. An interesting document concerning the use of cyber technologies to support governments is the French Senate document entitled "Crises sanitaires et outils numériques : répondre avec efficacité pour retrouver nos libertés"[55].

One of the building blocks of Skynet

Artificial Intelligence (AI), cutting edge technology in the eighties depicted by press as a dangerous shift of humans towards technological slavery, was looking for a reasonable field of application as it happened in the case of the Japanese stock exchange, unfortunately some "bugs" in the system generated the crash of the market. The concrete application was addressed to make, among the others, washing machine and camcoders smarter. The traditional domain of Artificial Intelligence, generated along its path some specific domain of application making our software, home appliances, accessories, and cars more "intelligent". This evolution was accompanied by the usual philosophical debate on "Can machine think?". The reference study in this sector is indubitably due to Alan Mathison Turing, mathematician, philosopher, cryptographer and more, and his article "Computing machinery and intelligence"[56] , the first paragraph entitled "The Imitation Game" starts with - "I propose to consider the question, "Can machines think?" This should begin with definitions of the meaning of the terms "machine" and "think." – and then explains his vision on "thinking machines" providing a more sophisticated definition and revolutionary insight on future technologies. Now AI is back on stage with a completely different impact on society.
In the era of open and big data, AI allows extremely large data sets to be analysed computationally to reveal patterns, which are used to inform managers and enhance decision-making. We use to

[55] https://www.senat.fr/rap/r20-673/r20-673.html
[56] A. M. Turing (1950) Computing Machinery and Intelligence. Mind 49: 433-460., https://www.csee.umbc.edu/courses/471/papers/turing.pdf last access July 2018.

identify two different branches of AI: “General” also known as “strong AI” and “Narrow” also known as “weak AI”.
On one side we find a broad-spectrum artificial intelligence designed to face a wide range of problems, on the side of weak AI, we find vertical solutions based on a well-defined domain of knowledge as it happens for instance for expert systems or car automatic driving systems. They are designed to deal with a specific domain of knowledge, characterised by well-defined rules and situations; they can be further trained and even implement machine learning; additional everyday examples are intelligent personal assistant, chatbots, SIRI, ALEXA, GOOGLE Assistant, Mercedes Benz and Volkswagen on board assistants. More in detail:

Narrow AI (ANI) - Narrow AI is a collection of technologies that rely on algorithms and programmatic responses to simulate intelligence, generally with a focus on a specific task. Time ago this was the branch of AI addressed to create expert systems, software application designed to solve specific problems providing the rationale of the outcomes. When you use a voice recognition system like Amazon’s Alexa to turn on the lights, that’s narrow AI in action. Alexa may sound smart, but it doesn’t have any advanced understanding of language and can’t determine the meaning behind the words you speak. The program simply listens for key sounds in your speech and, when it detects them, follows its programming to execute certain actions. To users, this can seem surprisingly intelligent — and voice recognition is far from a simple computing task — but in reality, there is no actual “thinking” going on behind the scenes. Non-player characters (NPCs) in games are another good example of ANI. While they take human-like action, in reality they’re simply following a pre-programmed series of actions designed to mimic how a human would play the game.

General Artificial Intelligence (GAI) - GAI, in contrast, is intended to think on its own. The goal of GAI research is to engineer AI that learns in a manner that matches or surpasses human intelligence. GAI is designed to learn and adapt, to make a decision tomorrow that is better than the one it made today. None of this is easy, which is why most examples of AI you’ll encounter today are the narrow form. GAI is a new, complex and varied category with numerous sub-branches, most of which are still research topics in a lab. Modern AI systems focus on solving specific tasks, such as optimization, recommendation or prediction systems and don’t learn broad concepts generally, like a human would.

Machine Learning

Machine learning (ML) is an interesting subset of AI that is providing inspiring solutions to complex problems, a typical field of application is the one non-approachable with algorithms and explicit programming. The basic principle is to analyse data and identify patterns that can suggest the way to extrapolate a significant result. The typical taxonomy of ML is at top level subdivided in supervised learning and unsupervised learning.
Supervised learning: a system “tutor” feeds the application with a set of inputs and expected outputs to train the system that has the identify a general rule that maps inputs and outputs; of course, this is a possible option when this “rule” is not clearly identifiable by the software programmer so a specific algorithm it is not doable.
Semi-supervised learning: the system receives only an incomplete training, there is not a complete set of outputs related to the list of inputs.
Reinforcement learning: the key feature of this approach consists in a dynamic environment that provides a score (positive or negative) rewarding the strategy to be followed to reach the requested

output; thanks to this assessment cycle we can say that the system learns and provide better solutions as much as it runs[57].
Unsupervised learning: the learning algorithm is completely independent, it does not receive any information about the outputs or any score, it must identify by itself the structure of the input and discover potential hidden patters or identify a potential goal thanks to feature learning.

Supervised machine learning algorithms and models use labelled datasets, beginning with an understanding of how the data is classified, whereas unsupervised models use unlabelled datasets and figure out features and patterns from the data without explicit instructions or pre-existing categorizations. Reinforcement learning, on the other hand, takes a more iterative approach. Instead of being trained with a single data set, the system learns through trial and error and receiving feedback from data analysis. With faster and bigger computation capabilities, ML capabilities have advanced to deep learning, a specific kind of ML that applies algorithms called "artificial neural networks," composed of decision nodes to more accurately train ML systems for supervised, unsupervised and reinforcement learning tasks. Deep learning approaches are becoming more widespread but come with high computation costs and are often harder for humans to interpret because the decision nodes are "hidden" and not exposed to the developer. Nonetheless, deep learning offers a wealth of possibilities, and already has promising applications for image recognition, self-driving cars, fraud news detection and more.

To better clarify the role of ML we can consider, among the others, two typical tasks it can perform:
Classification: Inputs are divided into two or more classes (labelled); the system must produce a model that assigns additional random inputs to one or more of these classes[58]. As we will see in the following taxonomy this process is usually performed in a supervised manner, the classes are defined a priori. A typical example of classification tasks performed by ML is spam filtering; the two classes are, of course, "spam" and "not spam". The learning process will increasingly add filters to better perform the classification.
Clustering: The tasks is to divide a set of inputs into groups (unlabelled) ; it looks like the classification tasks but this time the groups are not known beforehand. This typically an unsupervised task.

Let's leave this side of the technology to face another relevant one, how to deal with responsibilities in case of accidents that directly involve AI or ML?
If we refer to air-control probably one of the closest sectors the choice is usually between technical problems and human factors. Many times, the final verdict is a mix of several causes that all together led to a disaster. Accordingly with the reports, 70% of aviation accidents can be attributed to human error. Why? Because humans are active players inside the systems, and they are the only components that during emergency situations have the capacity to adapt and adjust resources to try to cope with unexpected events. Off course these responsibilities are not only in charge to pilots, but they are also shared among organisational failures, conditions of the operators (physical and mental state), physical and technological failures and finally human errors.

Back to road vehicles in case of law infringement or accident who is in charge as responsible, the passenger, the car builder, the software company, all of them? No one, the fate? We must consider that even the "road environment" is part of the system, horizontal and vertical signals, timely updates of maps and road works are integral part of the package. Some lane control systems are

[57] Bishop, C. M. (2006), Pattern Recognition and Machine Learning, ISBN 0-387-31073-8, Springer
[58] In case of more classes it is termed "multi-label classification".

cheated by multiple lane lines due to old lines still visible. Some accidents involving cars and even humans already happened, and the responsibilities are not yet undoubtedly assigned.

The existence of knowledge "silos" unable to cooperate because of the different knowledge background and skills has been recently broken so in the last decades philosophers and humanists started to professionally deal with computer scientists and innovators. They use to consider mid and long-term impacts of technologies on society. Emerging technological trend in autonomous vehicles, robots, machine learning and artificial intelligence may pose significant questions to innovations.

Ethical and Moral Aspects in Unmanned Vehicles and Artificial Intelligence

We already entered the era of Unmanned Vehicles; drones, boats and more recently cars are going to be "driven" by software; sensors, cameras, radars, and more are the senses of our vehicles. If the risk that a flying or floating drone can be hacked is concerning us, as well as, the temporary lack of specific legislation, what about the concerns related to ethical and moral aspects, not neglecting the legal ones, concerning autonomous road vehicles such as cars and buses?[59] Similar concerns regard artificial intelligence that already is and will increasingly pervade applications and devices. A number of services are managed today by artificial intelligence as well as decisions and even critical decisions are assigned to A.I., expert systems and fuzzy logic were some of the keywords in the 1980s, as we already pointed out, at that time A.I. advances captured the interest of journalists being considered the seed of the "Skynet" or the ignition of the progressive slavery of men ruled by machines. At the end of the 1970s early in the 1980s we start hearing about computers writing their code while running "intelligent" applications, basically auto-instructing themselves. A relevant number of computer scientists, mainly coming from cybernetics, were experimenting new languages and new approaches to make machines "intelligent", much more similar to humans. It was the time of Symbolics computers, LISP and PROLOG programming languages. Craig Reynolds, from the Symbolics Graphic Division, devised an algorithm that simulated the flocking behaviour of birds in flight. "Boids" made their first appearance at SIGGRAPH in the 1987 animated short "Stanley and Stella in: Breaking the Ice"[60]. This similarity with humans balanced another typical characteristic of humans that it is not yet in the DNA patrimony of machines, the ability to self-repair.

Computers start to become intelligent, remind HAL 9000[61] envisaged in the 1968 fiction movie "2001 A Space Odyssey[62]"; the spaceship officer Dr. Dave Bowman used to interact with HAL by voice calling "Hello, HAL. Do you read me, HAL?"—HAL: "Affirmative, Dave. I read you.", Dr. Dave Bowman: "Open the pod bay doors, HAL", HAL: "I'm sorry, Dave. I'm afraid I can't do that" . . . We all know what happened later.

Nowadays we call "Hi Google: Set temperature to 24C", "Hello Mercedes play disco music" or even closer to science fiction Alexa taking full control of our daily life. If we refer back to science fiction this "world of machines" might generate big concerns about the future, I don't refer to "Terminators" but simply remind the movie "WarGames[63]" or "Eagle Eye[64]", in both cases artificial

[59] Such as the one recently activated in Paris

[60] Stanley and Stella: https://youtu.be/3bTqWsVqyzE, last accessed January 2020.

[61] It is a well-known story the idea to call the spaceship computer HAL the three letters following IBM, as well as Windows New Technology (WNT) was the follow up of VMS the digital Virtual Address eXtension (VAX) operating system.

[62] 2001: A space Odyssey" (1968), science fiction movie directed by Stanley Kubrick, written by written by Kubrick and Arthur C. Clarke—the name HAL was probably chosen simply using one letter before each of the letters of the acronym IBM—International Business Machines Corporation.

[63] Wargames cold war scientific fiction movie directed by John Badham (1983). Eagle Eye, action thriller film directed by D.J. Caruso (2008)—both movies depict a lethal competition between humans and self-improving artificial intelligence machinery.

[64] Eagle Eye is a 2008 American action-thriller film directed by D. J. Caruso.

intelligence leads machines to apparently logical outcomes that are in direct contrast with human basic principles[65].
Safety and security standards for such devices are not set actually; how will two cars, both from the same builder or not, behave in case of imminent collision? A mother with a baby on one vehicle, a couple of retired citizens on the other one. Of course, the cyber-driver is supposed to be perfect, but the environment may introduce some bias, hence on the moral and ethical side how will the cyber-driver take decisions? There might be a "creative" solution due to human mind? How much technology and A.I. overlap moral and ethical aspects?
As an additional concern, today even cars may be subject to cyber-attacks as it already happened to Jeep vehicles in the United States; if on one side the regular car service or recall for update can be performed through the permanent car connection to the Internet, no more requiring us to physically take the car back for service (this might lead to unwanted outcomes[25]), on the other side, in case of cyber-attacks, our car might behave in a unpredictable way.
Therefore, possibly before a mass diffusion of such vehicles, we must be aware about some aspects: the risk of cyber-attacks that may turn everyday commodities like cars into "weapons" and the "programmed" behaviour of cars in case of "risky" scenarios. Security standards and harmonised "behaviours" together with an appropriate legal framework will probably help[26]. As a general remark concerning the incremental use of technologies to ease the life of humans, we must always consider the outcomes in case of system fault as well as the technical specification that trace the boundaries of the operativity of the solution. Many times, scientific and technological advances provide additional opportunities to citizens making accessible or easier to experience something. Simply consider the full set of technologies supporting drivers on wintertime or enjoying 500 horse power, if the system will not work how to manage? The same happens with auto pilots on boats, you set the route but then you cannot go under the ship's deck to watch television, other route can cross your one, floating objects can hit your ship's hull. The list of examples is endless, so a certain level of knowledge is required, technology may help us but not bridge major gaps.
Apart from the already reminded problem at the Japanese Stock Exchange, again due to automatic management, we cannot forget the shortcut generated on Boeing 737 Max, flawed data from a faulty sensor prompted MCAS (flight control software) to force the nose of the aircraft down repeatedly, when the pilots were trying to gain height, ultimately pushing it into a catastrophic dive.

To underline the interests in AI on October 2017 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".

From Ingsoc to Skynet

To conclude let's recap the key points outlined within this paper, cyber technology is nowadays pervasive and at different level present all-over the globe, digital data creation in the different formats (text, graphic, audio, video, etc.) are growing exponentially, because of the tight relation between cyber technology and our everyday life. A significant investment in digital literacy starting from primary schools is a paramount, young generations are exposed to many threats because of their intensive use of technologies without and adequate knowledge of potential drawbacks and

[65] We can recall the Isaac Asimov's "Three Laws of Robotics":
A robot may not injure a human being or, through inaction, allow a human being to come to harm. A robot must obey orders given it by human beings except where such orders would conflict with the First Law. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

risks. The capillary presence of “extreme” user friendly cyber-devices enabled “digital divided” citizens, not aware about potential risks, to access the cyber-world.
Cyber security together with cyber laws, when necessary, are a pre-condition to safely exploit e-Services. E-Government, e-Business or e-Health are in danger and may act as bad ambassadors if cyber security is not ensured technically and legally.
At global level the malicious use of cyber “troops” may design a credible warfare scenario reserving traditional warfare scenarios to minor local conflicts still based on conventional weapons [23 Ronchi].

In conclusion we are already in the arena of a cyber “warfare” [28 – Ronchi 2018] where troops, tanks, ICBM, choppers are the “cleverest” bit and bytes assaulting or defending our resources and lifestyle. To extremely simplify the basic scenario, it is not conventional war, it is not guerrilla warfare, it is not terrorism where one single man can create relevant damages somewhere, it is a new treat in which one single man located anywhere can create relevant damages globally. This to do not consider other potential perverse uses of digital communication and “Ingsol” or “Skynet” technologies.

The different paragraphs composing the present paper outlined some of the specific trends of cyber technology identifying potential benefits and threats. The practical impossibility to protect privacy as outlined in the specific paragraph take us to feel under the Ingsoc’s Big Brother [30 – Ronchi 2018] control non forgetting the role of misinformation and censorship in digital media. Digital transformation and the increasing role of AI and ML instructing and managing our activities and even private lives adds the flavour of Skynet, created by Cyberdyne[66] Systems.

References

1. Burrus Daniel, Who Owns Your Data?, https://www.wired.com/insights/2014/02/owns-data/
2. Roger E. Bohn, James E. Short (2009) How Much Information? 2009, Global Information Industry, Center University of California, San Diego.
3. Council of Europe (2001) New information technologies and the young. Council of Europe Publishing, Paris
4. Darrow Barb, The Question of Who Owns the Data Is About to Get a Lot Trickier, Fortune, http://fortune.com/2016/04/06/who-owns-the-data/
5. European Commission (2017) Resilience, Deterrence and Defence: building strong cyber-security for the EU, JOIN (2017) 450 final
6. European Union (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
7. European Union (2016) Joint Framework on countering hybrid threats a European Union response, 2016
8. EU Cyber Defence Policy Framework (2018 update), Council of the European Union 2018
9. European Defence Action Plan: Towards a More Competitive and Efficient Defence and Security Sector, European Parliament Legislative Train 04.2019
10. Information for All Programme (IFAP), Information Ethics, http://www.unesco.org/new/en/communication-and-information/intergovernmental-programmes/information-for-all-programme-ifap/priorities/information-ethics/

[66] The movie “Terminator” by James Cameron probably suggested to Japanese entrepreneurs to establish a Cyberdyne - https://www.cyberdyne.jp/english/

11. Information for All Programme (IFAP), International Conference on Media and Information Literacy for Building Culture of Open Government, http://www.ifapcom.ru/en
12. Mayer-Schönberger V (2009) Delete: the virtue of forgetting in the digital age. Princeton University Press. ISBN-13: 978-0691138619
13. Merriam Webster: Ethic, http://www.merriam-webster.com/dictionary/ethic
14. My data belongs to me, http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-discussion-personal-data-virtualisation-society-wsis10-review
15. Darrow B, The question of who owns the data is about to get a lot trickier, Fortune. http://fortune.com/2016/04/06/who-owns-the-data/
16. Dawkins Richard (1995), The Selfish Gene, ISBN 9780586083161, Orio Publishing Co, United Kingdom, London
17. Moritz E (1990) Memetic science: I. General introduction. J Ideas 1:1–23 and Moritz E (1995) Metasystems, memes and cybernetic immortality. In: Heylighen F, Joslyn C, Turchin V (eds) The quantum of evolution: toward a theory of metasystem transitions. Gordon and Breach, New York (J Gen Evolut Spec Issue World Futures 45:155–171)
18. 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
19. Prado D (2014) Towards a multilingual cyberspace, internet and socio-cultural transformations in information society. Interregional Library Cooperation Centre, Moscow. ISBN:978-5-91515- 061-3
20. Bohn RE, Short JE (2009) How much information? 2009, Global Information Industry Center. University of California, San Diego
21. Protection of personal data in EU, http://ec.europa.eu/justice/data-protection/
22. Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
23. Ronchi A.M., Soft but still concerns, proceedings International Conference on 'Homeland' Security Emerging Trends, Challenging Aspects - Hasan Kalyoncu University, Turkey 2021
24. Ronchi Alfredo M., (2019), e-Citizens: Toward a New Model of (Inter)active Citizenry , ISBN 978-3-030-00746-1, Springer (D)
25. Ronchi Alfredo M. (2019). e-Services: Toward a New Model of (Inter)active Community, ISBN 978-3-030-01842-9, Springer (D)
26. Ronchi Alfredo M. (2019 D) e-Democracy: Toward a New Model of (Inter)active Society, ISBN 978-3-030-01595-4, Springer (D
27. Ronchi Alfredo M., (2020). Digital transformation, proceedings ICCC New Delhi, CyberLaw
28. Ronchi Alfredo M., (2018), 21ST Century Cyber Warfare, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018
29. Ronchi Alfredo M., (2018), Cybertechnology: Use, abuse and misuse, ISBN 978-5-91515-070-X, UNESCO IFAP Interregional Library Cooperation Centre – Moscow, Moscow, Russian Federation
30. Ronchi Alfredo M., (2018), . . .1984 won't be like "1984"?, ISBN 978-5-91515-068-9, Interregional Library Cooperation Centre, Moscow
31. Christoph Stuckelberger, Pavan Duggal (2018), Cyber Ethics 4.0: Serving Humanity with Values, ISBN 978-88931-265-8, Globethics net
32. Surowiecki J (2004) The Wisdom of crowds: why the many are smarter than the few. Doubleday, Anchor. ISBN:978-0-385-50386-0
33. 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/
34. UK government service design manual: open data. https://www.gov.uk/service-manual/technology/open-data.html
35. Weiser Mark D, The computer for the 21st century, Scientific American Ubicomp Paper after Sci Am editing, 09-91SCI AMER WEISER