Is ethics evaporating in the cyber era?

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

Abstract

The first paragraph provides a quick insight on the humanistic approach to cyber technologies starting from the early debate about the new class of objects from the ontological standpoint, the early approach to cyber ethical issues to include the pervasive use of cyber devices and technologies including the evolving use of intelligent algorithms and machine learning to manage companies and support governments. Follows a paragraph summarising the key aspects of The UNESCO IFAP Code of Ethics for the Information Society and related follow-ups. The following paragraphs analyse the side effects of tangible and intangible impacts of cyber technologies with a 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; the transformation of the Internet from space for the free exchange of ideas into a tool for supervision, management, and control.

From divergent thinking to thinking different

In the 1960s, Science fiction and later scientific magazines and TV news showed "loft-size" computers fed by punched cards, controlling a set of spinning magnetic tapes mounted on fridge size machinery all of them under the supervision of several experts in cybernetics. Did these technologies deeply impact Society? The cyber technology that really impacted society was not the one in use in the 1960s or 1970s big mainframes operated by scientists dressed in a white coat. Thirty years ago, information scientists and computer users witnessed the unprecedented revolution due to "computer for people" later on termed "personal computer". This revolution was initiated by visionary researchers like Douglas Engelbart1 and his "oN-Line System2" 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".

A significant step forward in reshaping the future is due to a research team of divergent thinkers working at the Xerox Palo Alto Research Center (PARC). Xerox Corporation, the "Document Company" member of the "Cyber" establishment, the inventor of "Xerocopies" and printing machines originated the digital revolution.

The PARC research team composed by Butler Lampson, Charles P. Thacker, Robert W. Taylor, and Alan C. Kay licensed in 1973 the Alto computer and its object-oriented interface ten years before Apple Macintosh. In the 1980s Alan Kay, developing "Databook", introduced the concept of the laptop computer. We cannot forget of course the IBM PC released in August 1981, designed by another group of divergent thinking engineers directed by Don Estridge in Boca Raton, Florida. So, California and Florida the two sunny states were at that time the homeland of the digital counter-revolution.

Born at CERN, thanks to Tim Berners-Lee and Robert Cailliau, close to the end of the 1980s to ease the information exchange among physicists, the Web technology, after some years of a transversal appeal involving philosophers and artists, flourished on the consumer and home markets in 1995, since that time another revolution was on stage. "Where do you want to go today" the Microsoft motto outlined the idea of a small world entirely connected online. Then, 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 [17 – Ronchi 2019].

[1] 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.
[2] NLS—Developed by Douglas Engelbart and Dustin Lindberg at SRI International.

Wallet, wristwatch, and …

Computers have been around for about half a century and their social effects have been described under many headings [17 Ronchi 2019]. Mobile position-aware 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 smartwatches, bracelets are becoming pervasive as well. Cyber technology is increasingly merging any sector of our daily 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 [19 – Ronchi 2019] is changing under the influence of advanced information technology. Technology is evolving toward a mature "calm" [29 - 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. The digital divide 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 rapid diffusion of "cyber" was not associated with a proper digital media literacy awareness program [9- IFAP MIL], citizens must acquire a minimum level of knowledge in the proper use of cyber-technology including the field of cyber-security [5-6 European Commission 2014-17].

From the origins of computer science, less relevance was devoted to the potential impact of research outcomes on society and economy, states must favour the creation of multidisciplinary working groups to analyse under the different standpoints, the future impacts of emerging or improved existing technologies on society, economy, and protection of human rights in a mid-and long-term perspective.

Looking for the "silver bullet"

The incredibly rapid success of the Internet, mainly due to e-commerce and social media, gave an incredible boost to the globalisation trend, a shift toward uniformity, jeopardising diversities, and cultural identities. The key element of this success was the cyber element called "platform" the main component of any kind of service or information delivery. Platforms are mainly "populated" by users that, even if they do not pay any fee, are considered customers and as "customers" they increase the market value of the platform both in the media market because of the advertisement and the ability to analyse data and resell customers' profiles.

Platforms thanks regulations-vacancy paved the way to new monopolies deeply influencing society.

Since that time citizens have increasingly used to buy and sell goods online, book their travels and vacations, as well as enjoy social media and several services unthinkable before the Internet, from extremely vertical services to crowd services [25 – Surowiecki 2004] or funding. Platforms are the real "silver bullet" that created major opportunities and a real impact on society and the economy. A relevant part of digital transformation relies on platforms and standards [20 – Ronchi 2020], these aspects are directly linked with the "owners" of such platforms and standards, this can be considered a kind of monopoly not yet regulated, a kind of grey zone, so in the digital transition there is a potential risk, despite Antitrust laws, to fall under the 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 lead to the infringement of the human right "freedom of expression" as we will see later.

An additional remark, if on one side the diffusion of platforms creates new opportunities, as it happens with small enterprises or craftsmen, 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, on the other side the access to global service platforms creates a shortcut between offer and demand cutting out a major part of the traditional added value chain, as it was a long time ago because of malls it is now because of platforms.

General aspects, ethics, human rights, and potential drawbacks

Cyber Technology is a new entity, a new class of objects, from an ontology point of view, cyber data can be duplicated without any difference (cloned) and transferred on the fly through networks.

These properties made cyber objects difficult to manage on the legal side and even created some ethical problems. Philosophers and experts in humanities debated for a long time to identify the "original" in digital data, one of the assumptions is that original data are the ones just created in the computer's memory.

Nevertheless, if in the early times of Xerocopies "originals" use to be signed in blue or green ink to make the reference document easy to identify, in the age of "digital originals" the issue of "authenticity" and "originals" has been amplified and several tools and standards were created to solve the problem in contracts, reports, instructions, technical drawings and more.
In many cases, there is a real or virtual lack of legislation, virtual because situations apparently new can be led back to traditional cases.
Probably even thanks to the web technology that opened the use of the Internet to a multidisciplinary group of users the standpoint of humanities was considered. Information Ethics was one of the issues [9 – IFAP], on the occasion of the first phase of the WSIS held in Geneva in 2003 a specific working group was created, this later on become a WSIS Action Line, C10 "Ethical Dimensions of the Information Society" [27 – UNESCO WSIS] and some other relevant documents like the "Code of Ethics for the Information Society".
The existence of knowledge "silos" unable to cooperate because of the different knowledge backgrounds and skills has been recently broken so in the last decade's philosophers and humanists started to professionally deal with computer scientists and innovators [24 – Stuckelberger 2018]. Philosophers and humanists usually consider the medium and long-term impacts of technologies on society. The emerging technological trend in autonomous vehicles, robots, machine learning and artificial intelligence may pose significant ethical problems to innovation.

In addition to all these potential drawbacks, we observe the massive decrease in the level of critical thinking and the emergence of waves of information epidemics both at the national and global level (mainstream communication, limited contraposition, censorship, fake fake-news). Post-truth in its heyday, with public perception, shaped more by means of addressing feelings and predetermined opinions rather than actual facts, with fakes, click baits, hypes and other tools introduced to form post-reality in the political and media culture [30 – Makkuni 2018]. Post-reality is changing the system of values – with the "new" normal (semantic shifts, etc) of course politically correct, new ethics putting personal free will and freedom of choice under question; traditional cultural regulators of social relations and processes being displaced by automated social algorithms (increasing role of algorithms and ML). Blurring the borders between the real and the digital world, widespread of simplified virtual mock-ups and simulacra; a mass collection of data for managing people's behaviour (evaporation of privacy, data protection), from the age of high concerns (lack of oil, drinking water, ozone hole, global warming, killer asteroids, pandemics, and more) to the 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 [21 – Ronchi 2018], soft concerns [16 – Ronchi 2021], and more [7 – European Union 2016).

Freedom of expression

The Internet has incredibly facilitated access to mass communication. It combines a worldwide broadcasting capability with a mechanism for information dissemination, which offers us the opportunity to reach a wide audience with minimal effort. Before the Internet, the only way to reach wide audiences was radio and television broadcasting, and before those were invented, mainly printed materials or heralds. In addition, it is a medium that encourages collaborations and interactions among individuals and their computers almost without regard for their actual geographic location. This incredibly easy ability to access mass communication comes together with freedom of expression because there are no filters or "editorial" committees to approve the messages.
If the early stage of Internet communication was based on the so-called "netiquette", a kind of Galateo[3] or Bon Ton of Internet users, the advent of Web X.0 and the social web requires more specific rules addressing first 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 fails 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

[3] 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.

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[4].
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 of 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. A potential solution is to support the creation of "Independent Observatories for Ethics and Fairness" which, while guaranteeing freedom of expression, can promote self-regulation, respect for ethics and the identification of potentially fake news.
Freedom of expression is ensured by the Council of Europe at Article 10 of the European Convention on Human Rights[5] 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."

Extending the view to the European Commission (EC) and the Internet Governance Forum (IGF), which principles concerning freedom of expression are shared between them. Let's start from the Internet Governance Forum established as an outcome of the second phase of the WSIS in 2005 thanks to the participation of the stakeholders. Based on 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 in the dispute on the issue of a new global agreement on Internet regulations. Anyway, the IGF Best Practice Forum in 2020[6] 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.

Now move to the European Commission side. What are the key principles and objectives that guide the European Commission's work in this area?[7] The European Commission aims to defend access to open Internet and freedom of speech.
On 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.

[4] 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.
[5] https://www.echr.coe.int/documents/convention_eng.pdf
[6] https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/11138/2452
[7] 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.

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 Kores.
4. on how to make the 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 defines Freedom of expression and information[8] 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[9] 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 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 the Internet and wireless technology [26 – Thiesmeyer 2021]. 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 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."

Oversupply of information (info-obesity)

We are flooded by emails, online news, video clips, chats, unsolicited advertisements and more, if we simply want to clean up our device every day, we must invest a significant portion of our time all of which is to the detriment of reliable information and our focus [2 – Bohn 2009]. One of the potential drawbacks due to info-obesity is the devaluation and loss of trust in professional media together with 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[10]"—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"[11].

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 the private or public environment. If we keep the similarity in the field of personal data, we must claim 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" [10 - Mayer-Schönberger 2009], traces the important role that forgetting has played throughout human history.

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN
[9] Dr. Lynn Thiesmeyer, Keio University, Digital Transitions to Digital Despotism: Cyber-insecurity and its Regional Threat to Connectivity - Outcomes of the WSIS Forum 2021 - https://www.itu.int/net4/wsis/forum/2021/Files/outcomes/draft/WSISForum2021_OutcomeDocument.pdf
[10] 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.
[11] Mayer-Schönberger Viktor, Delete: The Virtue of Forgetting in the Digital Age, ISBN-13: 978-0691138619, Princeton University Press 2009.

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.

Goodbye privacy

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 [11 - Merriam Webster]. Cyber technology contributed in relevant mode to the sudden and initially invisible shift to "goodbye privacy" and blurring of ethical principles. Cyberspace is not a black hole where poor personal data, a kind of "outer space", no man's land not subject to humans' material desires and malicious behaviours. The APPification process boosted the dissemination of personal data, the more technology we use, the more visible we become. 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. IoT will add a lot to our lives, but this will cost us a significant part of our privacy. We may say "we have nothing to hide" but what a malicious use others might do of our personal data [22 – Ronchi 2018]. Your personal information is now shared among several companies, and you will never be sure that it will disappear from the online database. This last aspect, "never disappear", takes us to another relevant point. Introducing the concept of data ownership, we refer to the copyright concept. If my data are mine, I can even delete them, isn't it?

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. Recently the European Commission boosted the concept of Open Science as a powerful tool to significantly improve research achievements, the running Horizon Europe framework opted for the Open Science approach "by design" so all the EU funded project must publish their scientific outcomes and ensure long term access to them thanks to specific data repositories.

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 [28- UK Government], the combined use of them may led 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[12]. 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 [13 – Darrow 2016]. As it appears from the previous paragraph, ownership of data [12 - My Data] is not yet a well-defined legal concept even if the recent introduction of the GDPR did a significant step forward [15 - Regulation (Eu)]. 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. If we focus on cyber-rights we must prioritise the right to safety, security, and ownership. Information system hacking can compromise both safety and security (data, smart home, smart cities, smart mobility, etc.). Cyber-attacks and Hybrid Threats depict a new scenario in the XXI century. Digital identity thefts create additional challenges.

[12] My data belongs to me. http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-dis cussion-personal-data-virtualisation-society-wsis10-review

Artificial Intelligence and ML

Artificial Intelligence (AI), cutting edge technology in the eighties depicted by the 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 machines and camcorders 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"[13] , 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 term "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 in any kind of datasets (social, political, medical, business, etc), which are used to inform "managers" and enhance decision-making. We used to 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 "imitating" the human brain, 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 assistants, chatbots, SIRI, ALEXA, GOOGLE Assistant, Mercedes Benz, and Volkswagen onboard 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, a 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 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, 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, as 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 a way to extrapolate a significant result. The typical taxonomy of ML is at the top level subdivided into 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

[13] 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.

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 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[14].
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 patterns 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, on the contrary traditional NAI algorithms use to provide the rationale behind the outcomes step by step. 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[15]. 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 task 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 is 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 emergencies can adapt and adjust resources to try to cope with unexpected events. Of 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.

We increasingly hear of car driver assistance technologies or even autopilot. In case of law infringement or accident who is in charge as responsible, the "driver", the car builder, the software company, all of them? No one, the fate? As usual in risk analysis in addition to risks due to our behaviour or decisions, we have risks that do not fall under our control. 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 an integral part of the package. Some lane control systems are cheated by multiple lane lines due to old lines still visible. Some accidents involving "intelligent" cars and even humans already happened, and the responsibilities are not yet undoubtedly assigned. Last but not least, the ethical aspect will merge with intelligent algorithms.

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

To conclude: Don't you feel framed?

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 smartphone camera and microphone [23 – Ronchi 2018]. 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. Computer vision will enable your smartphone to identify every single person in a group you photographed and video analysis plus 3D real-time modelling enable intelligent optimisation algorithms to improve human performances, wearable sensors and IoT complete the schema.

Don't you feel framed by such an "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 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 was to collect all the different tiles. Online malls and delivery platforms offer, in addition, to analysing your browsing, the opportunity to save a "wish list" to better focus on the market trends. So, again don't you feel framed?

Bibliography

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. 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/
9. Information for All Programme (IFAP), International Conference on Media and Information Literacy for Building Culture of Open Government, http://www.ifapcom.ru/en
10. Mayer-Schönberger V (2009) Delete: the virtue of forgetting in the digital age. Princeton University Press. ISBN-13: 978-0691138619
11. Merriam Webster: Ethic, http://www.merriam-webster.com/dictionary/ethic
12. My data belongs to me, http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-discussion-personal-data-virtualisation-society-wsis10-review
13. 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/
14. Protection of personal data in EU, http://ec.europa.eu/justice/data-protection/
15. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
16. Ronchi A.M., Soft but still concerns, proceedings International Conference on 'Homeland' Security Emerging Trends, Challenging Aspects - Hasan Kalyoncu University, Turkey 2021
17. Ronchi Alfredo M., (2019), e-Citizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer (D)
18. Ronchi Alfredo M. (2019). e-Services: Toward a New Model of (Inter)active Community, ISBN 978-3-030-01842-9, Springer (D)
19. Ronchi Alfredo M. (2019 D) e-Democracy: Toward a New Model of (Inter)active Society, ISBN 978-3-030-01595-4, Springer (D
20. Alfredo M., (2020). Digital transformation, proceedings ICCC New Delhi, CyberLaw

21. Ronchi Alfredo M., (2018), 21ST Century Cyber Warfare, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018
22. 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
23. Ronchi Alfredo M., (2018), . . .1984 won't be like "1984"?, ISBN 978-5-91515-068-9, Interregional Library Cooperation Centre, Moscow
24. Christoph Stuckelberger, Pavan Duggal (2018), Cyber Ethics 4.0: Serving Humanity with Values, ISBN 978-88931-265-8, Globethics net
25. Surowiecki J (2004) The Wisdom of crowds: why the many are smarter than the few. Doubleday, Anchor. ISBN:978-0-385-50386-0
26. Thiesmeyer Lynn, WSIS Forum 2021 Outcomes, https://www.itu.int/net4/wsis/forum/2021/Files/outcomes/draft/WSISForum2021_OutcomeDocument.pdf
27. 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/
28. UK government service design manual: open data. https://www.gov.uk/service-manual/technology/open-data.html
29. Weiser Mark D, The computer for the 21st century, Scientific American Ubicomp Paper after Sci Am editing, 09-91SCI AMER WEISER
30. Ranjit Makkuni, Betrayed IT Revolution, https://www.facebook.com/watch/?v= 192288409296674