II International Conference
Tangible and Intangible Impact of Information and Communication in the Digital Age
9-12 June 2019 Khanty-Mansiysk, Russian Federation

Cybertechnology: Use, abuse and misuse

Alfredo M. Ronchi
EC MEDICI Framework
alfredo.ronchi@polimi.it

Abstract: As a side effect of globalisation and massive cyber services the number of crimes both perpetrated at local and global level is growing up. Governments and Law Enforcement Agencies are aware of this and look for potential countermeasures not only following traditional solutions. Technological countermeasures are not enough there is a need to foster the Culture of Cyber Security. This paper will start setting the scene and describing the evolutionary path followed by cyber technology. The issue of privacy tightly connected with information and data ownership will open a more general discussion about risks and threats connected with the increasing use of cyber technologies. Cybersecurity and the need to foster a "Culture of cybersecurity" will take us to the latest part of the document devoted to the social and economic impact of "cyber". Economic and social impact of cyber technology are considered as well.

Keywords: Data Ownership, Privacy, Ethics, Cybersecurity, Culture of cybersecurity

Setting the scene

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 up to former digitally divided. Technology is evolving toward a mature "calm" [5 - Weiser 1991] phase, "users" are overlapping more and more with "citizens" [6 - Council of Europe 2001] and they consider technology and e-Services [7 – Ronchi 2019] as an everyday commodity, to buy a ticket, to meet a medical doctor, to access the weather forecast. Mobile devices 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. In recent times artificial intelligence is back as a cutting-edge technology together with new trends like machine learning, quantum computing, open data and big data analytics.

Digital revolution in a nutshell

Thirty years ago, information scientists and computer users witnessed the unprecedented revolution due to personal computing[1]. This revolution was initiated by visionary researchers like Douglas Engelbart[2] and his "oN-Line System[3]" 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

[1] The "Homebrew Computer Club" was a "club" of computer hobbyists founded in the Silicon Valley in 1975, they use to meet and present their achievements. This group and the atmosphere of the time is well depicted in the movie "Pirates of Silicon Valley" (1999 Turner Network Television) based on Paul Freiberger and Michael Swaine's book "Fire in the Valley: The Making of the Personal Computer".
[2] 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.
[3] Developed by Douglas Engelbart and Dustin Lindberg at SRI International.

Lampson, Charles P. Thacker, Robert W. Taylor and Alan C. Kay licensing in 1973 the Alto[4] computer and its object oriented interface ten years before Apple Macintosh[5]. In the 1980s Alan Kay, developing "Dynabook", introduced the concept of laptop computer.

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. As a side effect of globalisation and massive use of cyber services and the "APPification[6]" of society the number of crimes both perpetrated at local and global level is growing up.

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 [2 - European Union 2016]. 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 [1 - European Commission 2016]. Of course, the overall scenario includes many other aspects and "shades", this paper poses the focus on the "grassroots" of hybrid threats, citizens in their everyday use of cyber technology.

From vision to reality

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.
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. 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".
Cybersecurity [3 – European Union 2013] was one of the key enablers in order 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 the time it become more complex to maintain an adequate level of security and preserve confidence. More recently the issues concerning ethics, data ownership, privacy and more arose as well as the impact of cyber technology on society and economy.
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, and more. New concerns 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.

Use, abuse and misuse

Privacy is concerned with control over information, who can access it, and how it is used. Privacy has many dimensions, from concerns about intrusive information collection, through the risks of exposure, increased insecurity or interference in their decisions that individuals or communities are subjected to when their 'private' information is widely known. Privacy is generally linked to individuals, families or community groups, and is a concept that is often used to demarcate a line between a 'private' and 'public' sphere.

[4] Xerox Alto had a limited diffusion on the market, in the 1980s Xerox created Star a modified and cheaper follow-up of Alto.
[5] Steve Jobs understood the relevance of that revolutionary approach to computing and activated Lisa and later Macintosh projects.
[6] The incredible capillary diffusion of APPs creating a real phenomenon: APPification

Some people probably consider cyber space as a kind of "outer space" no man's land not subject to humans' material desires and malicious behaviours. Voluntary or involuntary personal data dissemination is not a new phenomenon; before the Internet it was less evident and limited to some specific domains: credit card companies, travel agencies, real estate companies, car dealers, etc., basically people officially owning your personal information being in a position to suggest new opportunities or anyway reuse your personal data for different purposes. Later on, it was the time of "fidelity cards" and the explosion of CRM. The mass diffusion of the Internet ignited the real blast of personal information collection and data harvesting. There was no care about privacy both on the Institutions and citizens side.

Information is built on top of single or aggregate of data; for quite a long-time people used to think that cyberspace is a "black hole" without memory where you pour data without any side effect. Young generations shared on line sensitive information in order to access a videogame or chat with friends or, more recently, posted images and clips about their private life. In the "APPification[7]" 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, or fitness program, your expenses, or collect and analyse your contacts, your photos or video clips. In recent times crowd data collection, open and big data, more or less anonymised, has provided the big framework.

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 [10 – Babel 2015]; of course, IoT will add a lot to our life but this will cost us a significant part of our privacy. In a single generation, we witnessed the evolution of information technology from mainframes, exclusive patrimony of space agencies and super-calculus centres, to owning in our pockets a device ten thousand times more powerful, capable of observing and recording video, audio, location, and motion. These devices can communicate with nearly any other digital device from household appliances to cars. Collectively we have the ability to store, access, and process more data than humanity has created in its entire history. The actual "visual" trend is producing an incredible amount of photo/video documentation of our everyday life; does this mean "goodbye privacy?" [11 - Google]. Starting from all these aspects we will deal with main features concerning ownership, moral rights, privacy, ethics [17 – BBC], legal framework, security, even OSINT [19 – Central Intelligence Agency 2001] [20 - Central Intelligence Agency 2010] and more [21 - Hock].
You fill up a form to install a new APP and suddenly you receive a bunch of offers and advertisements often claiming that you subscribed to that service. Yes, you subscribed to the form to install the APP but thanks to a kind of letter chain the company in charge of collecting the forms to install the APP is the same company that manages dozens of business companies and you unintentionally subscribed to the "full" service. Your personal information is now shared among a number of companies and you will never be sure that they will disappear from on-line data bases. 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?
A special role in this risky environment was due to chatrooms and social media, a nowhere land where thanks to anonymous genderless profiles and always on geo referenced devices cyber criminals found a proactive environment. Till now despite experts' efforts there are few countermeasures to minimize harm.

Owning Information

The concept of "data" as it relates to people's everyday life is still evolving [12 – 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

[7] Kind of neologism stressing the incredible proliferation of APPs.

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 [29 – UK Government], the combined use of them may lead to identifying your personal behaviour; that's a form of privacy invasion or perhaps violation [14 – Darrow 2016].

Historically speaking, the idea of even owning [25 – My Data] information is relatively new[8]. 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.

The world we contributed to create, filled up with cutting edge technologies and 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 off of you. Your credit card company "tracks" your purchases and, in one word, your life-style. Your phone carrier "tracks" your calls, social relations and geographic location. Your area's law enforcement tracks the roads and intersections you walk through or drive down every day. Local administration CCTVs or private safety cameras follow you within shops or residential buildings, even inside the elevator.
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?

If we specifically refer to the intellectual property from the "continental" standpoint apart from the "economic" rights we find, 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" [24 - 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 applying 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.

As it appears from the previous paragraph, ownership of 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-

[8] My data belongs to me, http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-discussion-personal-data-virtualisation-society-wsis10-review

determination mean? An individual has the right to decide for himself or herself what information can be used by whom and for what. The General Data Protection Regulation (GDPR) in Europe is an attempt to protect privacy, national and international regulations/norms increase the opportunity to limit anonymity and pursue criminals but without risks awareness and proper education we cannot succeed. If we want to consider the positive side of cyber, today we have a rich set of technologies from the basic mobile phone, geo location to CCTV and specific apps protecting us. Internet of Things (IoT) is increasingly populating our environment, smart objects are around us, our mobile phone, tablet, smart fridge, smart washing machine, Alexa and more create a networked environment talking each other.

EU Data Protection Regulation and personal data re-use

Updating and extending previous regulations[9] in 2016[10] the European Commission issued a data protection Directive [29,30 - EU], the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the Regulation entered into force on 24 May 2016, it applied from 25 May 2018. The Directive entered into force on 5 May 2016 and EU Member States had to transpose it into their national law by 6 May 2018. One of the improvements is the geographic coverage of the Directive, formerly one of the main critical aspects in both the national and international regulatory frameworks. The new regulation will apply if the data controller or processor (organization) or the data subject (person) is based in the EU. Furthermore (and unlike the previous Directive) the Regulation will also apply to organizations based outside the European Union if they process personal data of EU residents.

An additional interesting aspect is represented by the definition of "personal data". According to the European Commission, "personal data" is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, "posts" on social networking websites, medical information, or a computer's IP address. This is a relevant step forward in privacy issues. As clearly stated in the title of the Directive a specific focus concerns data re-use. Nowadays on-line applications, APPs and open data represent the typical environment for data re-use.

What laws and legal implications may occur to "entities" re-using data? This question pertains the problem we can summarise as "Transparency & Openness vs Privacy, Security & Ownership". If we consider a governmental organisation we can refer to ethics [22 – UNESCO IFAP] and integrity within the organization. Usually speaking about governmental bodies, we assign them high ethical standards, respect their dignity and organizational integrity.

Data re-users' main concern is rights and dignity of others. The majority of open data re-users are NGOs who often declare missions that are directly linked to rights of certain social groups. Having responsible data policies sends a clear signal to all stakeholders that an organization does in fact care about its affected groups, especially those vulnerable. More in general, considering both governmental bodies and data re-users, an additional aspect concerns reputation in front of donors, partners, and customers. Institutions and organisations having data re-use policies in place does send a clear signal to donors, partners, customers and other stakeholders that the organization threats its activities with care and high ethical standards [30 – UNESCO-WSIS].

Responsibilities in data re-use

Waiting for a sound definition of data ownership, it is worth it to consider the responsibilities in data re-use. Re-using data (e.g. Open Data or Big Data), organisations have the duty to ensure people's rights to consent, privacy, security and ownership during the processes of: collection, analysis, storage, presentation and re-use. Consent is a relevant "keyword"; it means to explicitly provide the consent to use and manage private information provided in order to access a specific service. The request for "consent" must incorporate a clear and complete description of the use and aim of such data collection. Such a request may incorporate the description of future re-use of such dataset. If the potential use and re-use of data is articulated in different aims and steps the

[9] 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 access December 2017.

[10] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, entered into force on 24 May 2016.

consent must be requested in the so-called “granular” way that means that the platform will request a sequence of different consents that should be provided or not care of the citizen; in the field of APPs this is usually known as Warsaw Declaration on "APPification of society" [32 - Warsaw Declaration] (September, 2013).
How is the right to consent usually ensured? One of the typical approaches is “informed consent”; this is the mechanism through which people agree to provide information for research or data collection projects. The informed consent policy is very well known in the medical sector; you read and sign the informed consent form before a surgical operation or a specific therapy but even more frequently when you apply to download eHealth APPs that will collect some physical parameters to perform their duties.
Informed consent finds its basis in three components:

1. Disclosure of research objectives and any risks or negative consequences of the capacity of participating individuals to understand the implications of the participating voluntariness of their participation;
2. Informed consent includes plain language, easy-to-understand explanations of the types of data to be collected;
3. The purposes of collecting data, the intended and potential unintended uses of that data, who has access to and control over the data, risks of data leakage to third parties, and any benefits of participation in data collection.

Once data are collected and utilised for the specific proposes stated by the request for consent it might happen that the same data will be useful for different purposes; how can we manage? Even if people used to think that once available data is re-usable without limitations, re-use of data collected for a different scope basically requires a new request for consent specifying the new purposes. This is a real problem that affects major parts of open data collected by public bodies, and not only them. Imagine extending that same principle of specific consent to anything that anyone is able to “capture” regarding your life. Suddenly, you'd have to sign a legal release every time you swipe your credit card, take a taxi or walk through a store equipped with security cameras. The question of who owns your data is not an easy one to solve. It becomes particularly problematic because you potentially create “public” data (whether or not it gets recorded) every time you leave your house entering “public” space. The number of steps you take, whether you look ahead or at the ground, what types of clothes you wear, and any number of decisions you make in view of other people are all potential data; this happens when airports security activate a passenger’s shadowing or free Wi-Fi connections asking for your identity, e.g. typing your mobile phone number to gain access to the Internet, track your position.
This looking from the perspective of privacy; but at the same time public institutions must respect the values of transparency and openness. The contraposition of such duties, transparency & openness versus privacy, security & ownership, finds its solution in the ethical and responsible re-use approach. This contraposition of duties may be schematized in a very effective way considering the right to privacy patrimony of those without “power”, while the need for transparency and openness is for those who have “power”.
So, in extreme synthesis we have some principles: transparency & openness together with do no harm! The main concepts to be considered are: the right to consent and the respect of privacy, security & ownership. The concepts of privacy, security, commercial or state secrecy can be secured following the “do not harm” principle. Data re-users must do all within their powers to not cause any harm to any of the stakeholders that can rise as a direct or indirect result of open data re-use. To conclude, if we consider the process from the data stages point we find: collection and storage, analysis and presentation.

Privacy and risk related to breaches

Responsible and ethical data re-use is around the concept of privacy, legal requirements, risks and mitigations associated. Article 12 of the Universal Declaration on Human Rights [31 - Universal Declaration] states, “*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation*”.
Due to the spread of online applications and the need to process and file personal information such as names, addresses, telephone numbers and email addresses, national authorities all over the world have started to look for potential infringements of privacy by hackers [28 – Thompson 2008]. Indeed, there have even been some international-level infringements; for example, the customer database belonging to a very well-known underwear brand was cracked and personal information about various celebrities was made public.

Rules and obligations may differ from country to country and from continent to continent, but the importance of keeping personal information private is always recognised and protected. It is mandatory to ask for explicit approval every time personal information is stored in any format. It is also mandatory to ask for explicit approval when the data is updated, communicated or transferred to a different organisation. In addition, an agent responsible for the personal information must be nominated and referenced by the organisation. In contrast, owners are responsible for managing the personal information stored in their PDAs and mobile phones.
Dealing with privacy it seems worth it to mention a recent trend, the "right to disconnect". This right become popular because it was introduced as a part of a much larger and controversial reform of French labour law[11] by the labour minister Myriam El Khomri back in May 2016; "*plein exercice par le salarié de son droit à la déconnexion*"; this was reportedly the only one that did not generate widespread protests in France.
Today the digital tools are blurring the boundary between personal and professional lives, this effect is often termed "time porosity" or "spill over". Myriam El Khomri commissioned a report submitted in September 2015, which warned about the health impact of "info-obesity" which afflicts many workplaces.
On 1 January, an employment law entered into force that obliges organisations with more than 50 workers to start negotiations to define the rights of employees to ignore their smartphones. Under the new law, companies will be obliged to negotiate with employees to agree on their rights to switch off and ways they can reduce the intrusion of work into their private lives. If a deal cannot be reached, the company must publish a charter that would make explicit the demands on, and rights of, employees out-of-hours. However, it foresees no sanction for companies that fail to define it.
Anyhow, this principle was already adopted by some large groups such as Volkswagen[12] and Daimler in Germany; or nuclear power company Areva and insurer Axa in France have already taken steps to limit out-of-hours messaging to reduce burnout among workers. Some measures include cutting email connections in the evening and weekends or even destroying emails automatically that are sent to employees while they are on holiday. A study published by French research group Eleas[13] in October 2016 showed that more than a third of French workers used their devices to do work out-of-hours every day. About 60% of workers were in favour of regulation to clarify their rights.

Back to privacy issues in general let us take into account more closely privacy risks and their mitigation; key risks related to privacy are: disrespect of privacy can cause humiliation, embarrassment or anxiety for the individual, for example from a release of health data, it might be concluded that an individual accessed treatment for a sensitive sexual health condition; can have an impact on the employment or relationships of individuals; can affect decisions made about an individual or his ability to access services. This specific point might lead for instance to: their inability to obtain insurance; financial loss or detriment; a risk to safety, such as identifying a victim of violence or a witness to a crime.
As usual when we have to deal with risks we analyse them in order to find mitigation actions. Let us start considering a basic privacy risk assessment, determining any specific unique identifying variables, such as name, cross-tabulating other variables to determine unique combinations that may enable a person to be identified, such as a combination of age, income, and postcode. In addition, acquiring knowledge of other publicly available datasets and information that could be used for list matching. Of course, this procedure will not ensure 100% privacy because new data sources might be open to public access, completing the puzzle. As an example, think about the typical concerns related to some on line personal feedback or, better, on-line vote, and how to ensure a single vote from right-holder citizen and at the same time disjoin his/her identity from the expressed vote.
Privacy and technology are still looking for a golden balance; the summary below was written by the Congressional Research Service, which is a nonpartisan division of the Library of Congress, and was published

[11] loi n° 2016-1088 du 8 août 2016 Chapitre II Adaptation du droit du travail à l'ère du numérique Article 55 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.

[12] No connection between 18:15 and 7:00.

[13] http://www.eleas.fr/expertises/gestion-des-tensions-au-travail/ , last access February 2018.

on Mar 28, 2017[14]. This joint resolution nullifies the rule submitted by the Federal Communications Commission entitled "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services." The rule, published on December 2, 2016:

- applies the customer privacy requirements of the Communications Act of 1934 to broadband Internet access service and other telecommunications services,
- requires telecommunications carriers to inform customers about rights to opt in or opt out of the use or the sharing of their confidential information,
- adopts data security and breach notification requirements,
- prohibits broadband service offerings that are contingent on surrendering privacy rights, and
- requires disclosures and affirmative consent when a broadband provider offers customers financial incentives in exchange for the provider's right to use a customer's confidential information."[15] [GovTrack.us]

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" [18 – Brunton] is an application[16] 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 web sites adding an incredible amount of "noise" to your browsing history. Internet Noise is actually hosted by the GitHub web site[17].
This is a synthesis of the first step, awareness, citizens and especially young generations must be aware about potential drawbacks due to cyber technologies. Next step is to educate fostering the culture of cybersecurity.

Security in the cyber world, a paramount

Cyber-security was one of the first aspects to be improved since the inception of the "Information society" idea. Of course, any kind of on-line activity must be managed in a secure way or at least, as we will see, at a certain level of "insecurity". Quoting Salman Rushdie, "There is no such thing as perfect security, only varying levels of insecurity."

Some recent events may be summarized as follows: After the attack to Sony Pictures, to get closer in time, on the occasion of the 2016 Presidential elections there arose the suspicion of a potential mass intervention of foreign hackers influencing the results of the ballot.

The progression of cyber-attacks is amazing; let's consider year 2017:

January 2017, the EU raises an alarm on fake news and hacking. EU commissioners have raised fresh concerns about fake news and hacking in Europe but warned that there are "no easy solutions".

February 2017, Yahoo sends out another round of notifications to users, warning some that their accounts may have been breached as recently as last year. The accounts were affected by a flaw in Yahoo's mail service that allowed an attacker—most likely a "state actor," according to Yahoo—to use a forged "cookie" created by software stolen from within Yahoo's internal systems to gain access to user accounts without a password. A number of other attacks include the so-called Zcoin; a simple one-digit typo within the source code of a cryptocurrency called Zcoin has allowed a hacker to make a profit of over $400,000 worth of cryptocurrency.

March 2017, UK: 26 million NHS patients' records in a security scare over SystmOne "enhanced data sharing"; "Privacy campaigners last night said the breach was "truly devastating" with millions of patients having no idea if their records had been compromised. GP leaders said the breach had "potentially huge implications" and could see family doctors flooded with complaints." (source "The Telegraph").

---

[14] This measure has not been amended since it was introduced. The summary of that version is repeated here.

[15] https://www.govtrack.us/congress/bills/115/sjres34/summary#libraryofcongress , last access February 2018.

[16] The Electronic Frontier Foundation (EFF, https://www.eff.org) is one of the most active actors in counterbalancing any potential infringement of privacy and freedom due to digital technology as stated in their motto, "defending your rights in the digital world".

[17] https://slifty.github.io/internet_noise/index.html , last access February 2018.

April 2017, Cyber Attacks Statistics, motivations behind the attacks: Cyber Crime 71,1%, Cyber Espionage 21,2%, Hacktivism 3.5%, Cyber Warfare 1.2% (source Hackmageddon). Scottrade Bank data breach exposes 20,000 customer records, 60 GB MSSQL database contained customer records and other sensitive data (source CSO from IDG).

http://www.hackmageddon.com/, last accessed 22 November 2017.

https://www.csoonline.com/article/3187480/security/scottrade-bank-data-breach-exposes-20000-customer-records.html, last access February 2018.

May 2017, ransomware WannaCry caused global chaos; Wired magazine titled it "The Biggest Cybersecurity Disasters of 2017 so far". The Guardian issued an article starting with the following sentences: "Massive ransomware cyber-attack hits nearly 100 countries around the world - More than 45,000 attacks recorded in countries including the UK, Russia, India and China may have originated with theft of 'cyber weapons' from the NSA".

June 2017, a ransomware called Petya, which holds data hostage by scrambling it until a payment is made, caused widespread disruption across Europe and the United States.

July 2017, Italy, UniCredit bank was attacked by hackers; they have taken 400,000 IDs, but apparently no code or password that allows them to operate without authorization on current accounts. July 2017, Reuters - Cyber attackers are regularly trying to attack data networks connected to critical national infrastructure systems around Europe, according to current and former European government sources with knowledge of the issue.

August 2017, Russian hackers are targeting hotels across Europe; the hackers used booby-trapped Word documents and a leaked NSA hacking tool to get a foothold into the networks to then attack guests.

September 2017, The Guardian alerts: Hackers attacking US and European energy firms could sabotage power grids, water, gas; and a joint report presents physical and network-based malware affecting ATMs. September 2017, online sexual extortion: man sentenced in Romania in connection with death of British teenager.

September 2017, European Union Agency for Network and Information Security, ENISA, inaugurated as permanent EU cyber security agency. Europol's European Cybercrime Centre (EC3) and Trend Micro, a global leader in cybersecurity solutions, and released a comprehensive report on the current state of ATM Malware.

October 2017, the internet of things: when your washing machine and blood pressure monitor become a target for cyberattacks. October 2017, 195 individuals detained as a result of global crackdown on airline ticket fraud.

November 2017, British cryptocurrency Electroneum hit by cyber- attack after raising £30m, the cyber-attack that has shut investors out of their accounts for several days. The company's website came under a distributed denial of service (DDoS) cyber-attack. Similar attacks to South Korean cryptocurrency.

This short summary of attacks covering almost one year looks like a war report; the increasing pace of new attacks is amplified by the almost daily creation of new segments of cyber services and technologies [4 – European Parliament 2019].

Today we face some new concerns, the use of cyber technologies to disseminate and promote radicalisation and organize criminal activities, the emerging trend of "cyber-crime as a service", potential hybrid threats, the on-line disinhibition effect that enable and favour illicit behaviours, the lack of Ethical principles. It might be interesting to better investigate about the psychological, sociological, anthropological and moral aspects that contribute to a similar behaviour.

We all discussed for quite a long time about the potential problems due to the so called "digital divide", the goal was and still is to bridge the gap between digitally savvy and the "analog generation" on one side and the creation of a proper digital infrastructure. The gap between e-Citizens and digitally divided citizens has not disappeared yet but is becoming smaller every day. In the near future young generations [8 - Ronchi 2010] will not figure out how their parents used to fulfil some tasks in the past.

These efforts were mainly devoted to basic capacity building in the use of digital technology and more specifically e-services to ensure the shift from traditional interaction, mainly human mediated to digital interaction. Citizens

use to prefer to go to the front desk or use the telephone. In the 1990s the problem related to the digital infrastructure and more in general to the access to the Internet started to be partially solved thanks to some telecom players that breaking the rules offered phone free access to the Internet, this approach later evolved to ISDN flat rate connections.

Having positively solved Internet access the next true revolution was ignited by mobile position-aware devices. Smart phones before and immediately after tablets, two kinds of "non-computer" devices enabled mass access to e-services. "Non-computer", yes; one of the last barriers was the approach to "computers", the inherited idea of complexity and high skills requested in order to use and not damage them; smart phones and tablets [8 - Ronchi 2010] were not perceived as "computers", they are something different, friendlier, more personal. In few words, you don't need to think "do I need to take it with me?"; it is like your wallet, you take it!
These devices together with mobile connectivity turned citizen into e-citizens but a relevant problem wasn't solved like cybersecurity and privacy issues. These aspects are particularly sensitive with reference to young generations and kids, nowadays already on line. It is a common understanding that recent generations [9 – Jones 2011] represent a discontinuity compared with 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 have discovered new skills and capabilities in young generations [6 - Council of Europe 2001].
Many times, in this sector we used to think about the day after tomorrow, skipping today and tomorrow; network infrastructure is there, there is a bunch of useful software tools and APPs addressed to citizens, tablets and smartphones have overturned the scenario but it is evident that there is a gap to be bridged; how many citizens are aware about potential cyber risks? The attack surface is nowadays getting wider but risks awareness is very limited. In a society everyday more dependent from cyber technology there is a clear need to improve awareness about potential the risks in the cyber universe. The main objective is to bridge the second gap, after the digital divide we need to bridge the cultural divide concerning cybersecurity. If cybersecurity was a prerequisite to promote home banking and e-Commerce nowadays we need to ensure a "culture" of cybersecurity to avoid a bad ambassador effect extended to the whole sector of e-Services. This task is even more relevant than the efforts devoted to bridge the digital divide, the cultural divide is more critical. This need is particularly relevant in case of young generations, the risk to be victims of different types of criminal actions is relevant: cyber bulling, blackmails, extortions. There is an urgent need to foster a culture of cybersecurity starting from kids and reaching elderly people.
On February 2019 Onar bin Sultan Al Olama Minister of State for Artificial Intelligence (UAE) said: "It is very easy today for a nation to be attacked through hacking into its defence system unlike before when it required physical invasion. From national security and cyberwarfare to our smart fridge and unmanned transport system we have to face security problems.

Education: The Culture of Cybersecurity

To contribute to bridge cybersecurity divide we can foresee a methodology based on awareness, education and live training. This methodology has been promoted on different occasions including the cybersecurity track of the World Economic Forum held in Davos (January 2019)[18], a couple of workshops on the occasion of the WSIS Forum[19] (April 2019), and IST Africa[20] (May 2019). The first action to be performed is to improve awareness about the potential risks due to improper use of digital technology both due to direct and indirect risks.
Once the awareness process is activated and the interest to improve knowledge about cybersecurity raises it is time to provide the fundamentals on cybersecurity. Education is the next action to be performed in order to fertilize the seed of the culture of security since primary schools and in the transition phase ensure proper education to citizens. As a direct consequence of some recent mass cyber-attacks like Petya, WannaCry, Andromeda and a number of Cryptominers some countries decided to foster the culture of cyber security from the grassroot, primary schools included.

[18] https://issuu.com/cyberfuture/docs/2019_cyber_future_dialogue_resoluti
[19] https://www.itu.int/net4/wsis/forum/2019/Home/Outcomes#documents
[20] http://www.ist-africa.org/Conference2019/

More in general Governments should invest in media information literacy [23 – UNESCO IFAP RU], critical thinking, security, cyber-privacy and info-ethics. If a proper merge of official curricula must join the required knowledge in the field of security the approach to proper educate citizens must be based on effective methodologies suitable to the target audience (kids, teenagers, adults, etc.). With specific reference to universities, cyber-security courses already included in existing curricula have been improved and new post degree and continuous education courses are now available. Digital technology may help offering from edutainment Apps as experienced by the Italian Police to video reels to be enjoyed anywhere anytime. In addition, an increasing number of universities designed and activated on line courses providing the key concepts to setup a first "defence line" against cyber- crimes, such courses are now compulsory for both students, professors and administrative personnel.
Cyber-security is a paramount issue to enable the fruitful implementation and adoption of e-Services from e-Government to e-Health. The World Summit on the Information society devoted since 2005 a specific action line "Building confidence and security in the use of ICTs" [15 – UN General Assembly].

Benefits due to a "Culture of Cyber Security"

The underlying concept to foster the development of a Culture of Cybersecurity could change substantially the "window of vulnerability" both in case of private users and organisations. The impact of a strong "Culture of cybersecurity" on business and economy is quite evident both as a direct and indirect effect. Citizens and organisations will increase the level of trust in cyber technologies with positive effects both on safety and security in a widest sense. These effects will involve smart cities, transportations, commerce, government, etc.

Technology may help: Live Training

Awareness and educational initiatives must be planned to provide a significant contribution to bridge the "cultural" gap but a live training is needed. Actually, the access to training infrastructure is mainly limited to big enterprises and governmental institutions principally due to the cost and complexity of such solutions we hope in the future it will be possible to find tailored solutions suitable for small enterprise and even citizens. Live training actions can be based on Cyber Ranges, a typical solution to train[21] and test cybersecurity measures and exercise professionals. 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 [16 – Council of the European Union 2018]. 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[22].

This situation illustrates the problem of lack of preparedness organisations face in defending effectively against cyberattacks. Cyber Ranges (CR) are steadily gaining popularity as a means to prepare cyber security professionals and fill the industry's skills shortage.

The cyber ranges are interactive, provide a simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They will provide a safe, legal environment to gain hands-on cyber skills (based on a Cybersecurity Competence Based Curriculum) and a secure environment for product development and security posture testing.
Similar platforms will provide a simulated environment to conduct tests and rerun exercises to enhance cyber defence technologies and skills of cyber defence professionals. In addition, simulation features may include a global situational awareness dashboard, informing the user about the risks and associated attack surfaces of the simulated organisation(s). These platforms will provide a toolkit placeholder to develop and introduce tools to be used for testing the resilience of networked, socio-technical and cyber physical systems in general by exposing them to realistic nation-state cyber threats in a secure, sandboxed facility without dropping the need and experience of threat intelligence and communication. Innovation lies also on effectively monitor and prevent cyber-attacks by means of specific ontologies, on-line textual content analysis (e.g. social media), supported by innovative deep semantic algorithms and machine learning tools. Since most of potentially useful online contents

[21] https://www.ixiacom.com/company/blog/benefits-cyber-range-training
[22] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

relevant for online cyber-threats are not available in the Surface Web, the CR platform implements existing methodologies and solutions for online source identification, crawling and indexing, by making them efficient and effective for contents in the Deep Web and Dark Nets, with the expectation of inclusion of additional tools through a Cyber Range Network. These platforms will enable the conduct force-on-force cyber games/exercises, and cyber capture the flag (CtF); they will provide an environment to integrate technologies and test company-wide cyber capabilities, cybersecurity technologies, and customer and partner capabilities, along with the testing and demonstration of cyber technologies to test existing and future mission-critical systems against cyber-attacks. On the training side, they will offer cyber professionals the opportunity to develop the skills through facing a wide range of cyber-attacks and their overall impact. These platforms will allow organizations to learn and practice with the latest techniques in cyber protection, practitioners to create and practically test different defence and incident response strategies in short time. Upon completion of a training session the practitioners will receive suggestions on relevant best practices in the specific situation, identified by the platform or retrieved in the knowledge base.

Risk assessment: mapping

We all know that security and privacy are subject to risk, as already stated; thus, it is important to identify and mitigate risks associated with privacy and security concerns. In order to reach this goal, as a first approach, we can perform the following steps: identify the persons at risk in the event of personal information exposure (not restricted to the data owner or collector); identify knowledge assets that can be extracted from the data collected (discrete data points, meta-analysis of data points; mash up of the collected data and external data sources); evaluate the importance of each knowledge asset to the potential goals/harms (little or no relevance, significant relevance, crucial). This approach, many times, will lead us to identify the crucial nodes that, if adequately protected, will ensure no harm. The level of privacy risk will be dependent on the likelihood that identification could occur from the release of the data and the consequences of such a release. Anyway, mitigation is many times linked to de-identification.

In the previous paragraph, we mentioned not only privacy but even security. Security, somewhat linked to privacy, adapts security protocols and tactics to encompass:

1) Digital information security;
2) Physical and operational security;
3) Psychosocial well-being required for good security implementation.

Nowadays the key concept is “holistic security”, a “global” approach to security integrating all the different aspects and problems. A specific interest is devoted to digital security.

Digital security is more than focus on software or tools, integrating emotional well-being, personal and organizational security. Good implementation of digital security tools and tactics requires attending to the practitioners’ psychosocial capacities to recognize and respond dynamically to different threats to them and to participants related to project data collection and communications (intimidation, social engineering).

Social impact

As already outlined social media are one of the milestones recently introduced in the digital domain. Social media is the key of success of the digital domain, the reply to the Win ’95 promo “Where do you want to go today?”; the real mass use of digital resources, the one creating “addiction”, is the social side. Since the creation of the first blogs opening the opportunity to share opinions and beliefs with a significant number of users, the number of “social” applications has grown very quickly: Blogs (‘90), Wikis (‘95), Semantic Web (‘97), Wikipedia (‘01), Picasa (’02), My Space (‘03), Facebook (‘04), YouTube (‘05), Twitter (‘06), VKontakte (’05), renren (2005), Weibo (2009), Instagram (’10), SnapChat (2011), WeChat (2011),. . . . Social newspapers (e.g. YouReporter, Bambuser), and more, much more.

The idea to share something with someone else, a group of people, sometimes generates a sense of belonging to a “community”. Communities are an integral part of the history of technology; in the specific field of communication we find “amateur radio”, also called ham radio or OM (old man) and later on the citizens’ band

(CB) community. Of course, technical communities are not limited to the field of communications; we have computer graphics, video games, and more, such as the Manga Fandom[23], but communication is the key player in the creation of communities and due to this communities directly dealing with communication means are facilitated. Since the beginning of computer user's communication, a sense of community arose and a common feeling on behavioural rules was implemented.

The sense of belonging to a community it is not the only driver for social media, perhaps even the opportunity to share your opinions with a huge audience together with the "right" to the Andy Warhol's 15 minutes of celebrity are some more aspects that boosted the social media phenomenon. The result for many people was to enjoy their life looking through the viewfinder of the mobile phone, and to post private video that recall "The Truman Show" and EDtv in a kind of a compulsive sharing of "privacy". This absolute lack of privacy and many times the will to overperform lead to major or minor drawbacks. An evident side effect of a similar "modus vivendi" is an addiction to on-line digital devices, some authors call this generation "long thumbs". Recently a wave of rebellion to such cyber slavery suggests not only to employers and workers to enforce the "right to disconnect" but even citizens and young generations must apply the same principle of turning off cyber devices to relax and have quality time.

If the early stage of Internet communication was based on the so-called "netiquette", a kind of Galateo[24] 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 is enforced. 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, YouTube or even some thematic web sites 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[25].
The Internet Revolution gave a boost to data creation and dissemination, MAC addresses, web logs, and intentional or unintentional applications to web sites and services, and social platforms ignited the sedimentation of personal and many times sensitive information apparently lost in the cyberspace [33 - Pimienta 2014][34 - Prado 2014]. Very soon the first drawbacks come on stage: privacy infringements, stalking, hacking, cyber-crimes, stolen identities, dark net and more [35- Bohn 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. 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.
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

[23] Manga fandom is a worldwide community of fans of Japanese cartoons manga.
24 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.

[25] E.g. markets potentially offering "billions" of additional customers. Sometimes the censorship is not declared but the bandwidth devoted to the specific service or web site is so narrow that it is practically impossible to connect.

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.
Anyway, on the reverse there is a real risk of abuse, misuse and misinformation thanks to these technologies. The movie "Citizen Kane[26]" directed and interpreted by Orson Welles in 1941 outlined the relevant "power" of journalism[27], the movie "Network[28]" directed by Sydney Lumet outlined the power of television in 1996 and perhaps "The Net[29]" and "S.Y.N.A.P.S.E.[30]" together with "The Social Network[31]" 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 few years ago 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.
News and Media are key elements in the global society. CNN, BBC, Al Jazeera[32], Al Arabiya[33] are writing the history of the planet 24x7 and on the grassroots side YouReporter[34] and Tweeter 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[35]" 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[36]. The evolution of on-line news due to the social web and the birth of "prosumers" did the rest. Twitter, YouTube, Facebook and blogs represent a real revolution in the domain of news. 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[37] by user-generated content (UGC) largely without any qualification and certification of the source generating Fake News. 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

---

[26] Citizen Kane directed by Orson Welles, 1941 RKO Pictures.

[27] 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.

[28] Network, directed by Sydney Lumet, 1976 Metro-Goldwyn-Mayer United Artists.

[29] "The Net", directed by Irwin Winkler (Columbia Pictures Industries Inc. - 1995).

[30] S.Y.N.A.P.S.E. (Antitrust), directed by Peter Howitt (Metro Goldwjn Mayer - 2001).

[31] The Social Network directed by David Fincher (Columbia Pictures 2010).

[32] www.aljazeera.com/ , last access February 2018.

[33] www.alarabiya.net , last access February 2018.

[34] A recent event in the field of newspapers is the birth of The Huffington Post, inventing a completely new approach to newspapers.

[35] Wag the Dog (1997), Dustin Hoffman, Robert De Niro and Anne Heche, directed by Barry Levinson.

[36] Alfredo M. Ronchi. e-Services: Toward a New Model of (Inter)active Community, Springer International 2019

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

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.*"

Economic Impact

Web technology represented an incredible business opportunity for citizens and small enterprises, thanks to web sites people gained visibility on the global market, so wine producers, artisans and the whole galaxy of small businesses developed their activity without the need to be included in the traditional wide distribution networks. Now we are in the age of "platforms", platforms make the difference. Platforms are the real "silver bullet" that created mayor opportunities and real impact on society and economy. Global markets are easily reachable via business (biz) platforms, revolutionary business models are based on platforms, innovative services, crowd [36 – Surowiecki 2004] based initiatives and even innovative financial and trading activities share the same component. Thanks to digital platforms and a lack of legislation a number of market giants have grown up managing incredibly huge assets owning none of them, simply think about RB&B or Uber but the list is almost endless.

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 for malls it is now for 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. Even crypto currencies are in some way a follow up of this trend.

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. By unit of product/service it costs less a hamburger of electric energy? Do we agree with this scenario, are we happy to live in symbiosis with "computers"?

Another relevant innovative trend is the use of "crowds" to provide data and services not foreseeable before the Internet; simply think about APPs like Tripadvisor[38] or the one providing the local gas price daily or real-time traffic bottlenecks. It seems to be a completely new paradigm of software development beyond user groups and open software, the only way to face huge projects and compete with key software enterprises. The average "size" of "social" products and services is now affordable only by crowdsourcing. A number of services that do not find a proper economic dimension or even do not have the required appeal in order to be provided by companies may only rely on the crowd[39], crowds and platforms. This approach enabled innovative solutions like project funding or collaborative film production[40]. In the global society crowds are playing the role of "public services" [36 - Surowiecki 2004].

The affordable availability of both access and connectivity together with the diffusion of smart mobile devices enabled a real universe of new applications and services, some based on voluntary information provision, some based on big or open data. Such services were almost unthinkable before.

Conclusions

As we outlined in the present document, use, misuse and abuse of data and more specifically personal data may cause minor or major threats, ranging from privacy infringements to political, economic and national security threats. The concept of data ownership and personal data protection is relatively new and not universally shared. Breaches in information flows may ignite hybrid threats. To improve resilience and mitigate risks due to hybrid threats we need to promote awareness about cyber risks before the cyber technology will spread and control major part of reality, both adults and young generations must be aware about potential risks. Some of the potential risks increase or reach a dangerous level as much as people use technologies disseminating personal

[38] Tripadvisor was one of the first on-line services enabling users to rete hotels and restaurants, http://www.tripadvisor.com , last access February 2018.

[39] James Surowiecki, (2004) The Wisdom Of Crowds: Why the Many Are Smarter than the Few, ISBN 978-0-385-50386-0, Doubleday; Anchor.

[40] Http://www.wreckamovie.com Tempere Finland last access April 2018

information and content this implies that urges to inform users about similar risks sometimes not immediately evident but potentially dangerous even in case of hybrid threats. If security and safety will not be ensured a sentiment of unreliability may arose and delay the deployment of cyber technologies and e-services. This will be the first defence line at grassroots level of course more specific and sophisticated actions will complete the overall defence schema.

References

[1.] Joint Framework on countering hybrid threats a European Union response, European Commission JOIN (2016) 18 final, 2016

[2.] Shared Vision, Common Action: A stronger Europe, European Union, June 2016

[3.] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final

[4.] European Defence Action Plan: Towards a More Competitive and Efficient Defence and Security Sector, European Parliament Legislative Train 04.2019

[5.] Weiser Mark D., The Computer for the 21st Century, Scientific American Ubicomp Paper after Sci Am editing, 09-91SCI AMER WEISER

[6.] Council of Europe (2001) New information technologies and the young. Council of Europe Publishing, Paris

[7.] Ronchi Alfredo M. (2019), e-Services: Toward a New Model of (Inter)active Community, Springer

[8.] Ronchi Alfredo M., The fourth screen, proceedings Global Forum 2010

[9.] Jones, Chris and Shao, Binhui (2011). The net generation and digital natives: implications for higher education. Higher Education Academy, York

[10.] Babel Chris, Tackling Privacy Concerns Is Key to Expanding the Internet of Things, Wired Innovation Insights, Feb 2015

[11.] Google - Privacy & Terms, https://www.google.com/intl/en/policies/privacy/

[12.] Burrus Daniel, Who Owns Your Data?, https://www.wired.com/insights/2014/02/owns-data/

[13.] Merriam Webster: Ethic, http://www.merriam-webster.com/dictionary/ethic

[14.] 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/

[15.] Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society, http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf

[16.] EU Cyber Defence Policy Framework (2018 update), Council of the European Union 2018

[17.] BBC Ethics Guide, http://www.bbc.co.uk/ethics/introduction/intro_1.shtml

[18.] Brunton Finn, Nissenbaum Helen (2015), "Obfuscation: A User's Guide for Privacy and Protest", ISBN: 9780262331302, DOI: https://doi.org/10.7551/mitpress/9780262029735.001.0001, MITPress

[19.] Central Intelligence Agency, Intelligence: Open Source Intelligence, https://www.cia.gov United Nations Manual on the prevention and control of computer-related crime, UN 2001

[20.] Central Intelligence Agency, Intelligence: Open Source Intelligence, https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

[21.] Hock Randolph, Internet Tools and Resources for Open Source Intelligence - OSINT, http://www.onstrat.com/osint/

[22.] 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/

[23.] Information for All Programme (IFAP), International Conference on Media and Information Literacy for Building Culture of Open Government, http://www.ifapcom.ru/en

[24.] Mayer-Sch√∂nberger Viktor, Delete: The Virtue of Forgetting in the Digital Age, ISBN-13: 978-0691138619, Princeton University Press 2009

[25.] My data belongs to me, http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-discussion-personal-data-virtualisation-society-wsis10-review

[26.] Protection of personal data in EU, http://ec.europa.eu/justice/data-protection/
[27.] Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC
[28.] Thompson Herbert H., "How I Stole Someone's Identity", Scientific American, August 2008
[29.] UK Government Service Design Manual: Open Data, https://www.gov.uk/service-manual/technology/open-data.html
[30.] 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/
[31.] Universal Declaration of Human Rights, http://www.un.org/en/universal-declaration-human-rights/
[32.] Warsaw Declaration, http://www.coe.int/t/dcr/summit/20050517_decl_varsovie_EN.asp, Council of Europe Warsaw Summit May 2005
[33.] Pimienta Daniel, Redefining Digital Divide Around Information Literacy and Linguistic Diversity in a Future Context of Access Provision, Internet and Socio Cultural Transformations in Information Society, ISBN 978-5-91515-061-3, Interregional Library Cooperation Centre, Moscow 2014
[34.] Prado Daniel, Towards a Multilingual Cyberspace, Internet and Socio-Cultural Transformations in Information Society, ISBN 978-5-91515-061-3, Interregional Library Cooperation Centre, Moscow 2014
[35.] Bohn Roger E., Short James E. (2009), How Much Information? 2009, Global Information Industry Center University of California, San Diego
[36.] Surowiecki James, (2004) The Wisdom of Crowds: Why the Many Are Smarter than the Few, ISBN 978-0-385-50386-0, Doubleday; Anchor