Cyberlaw University®
Education in Cyberlaw - A cut above the rest

A CYBERLAW UNIVERSITY INITIATIVE

CYBERLAW UNIVERSITY INTERNATIONAL E-JOURNAL

WWW.CYBERLAWUNIVERSITY.COM

S.NO.	NAME OF ARTICLE	PAGE NO.	DETAILS OF AUTHOR(S)
1.	**EMERGING CYBERLAW TRENDS IN 2021 IN INDIA**	**Page 03-Page 06**	Dr. Pavan Duggal President, Cyberlaws.Net S-307, Block S, Part 1, Greater Kailash, New Delhi, Delhi 110048 +91 11-46584441 pavanduggal@yahoo.com
2.	**CONTACT TRACING, MEDICAL DATA CONNECTED ISSUES & CHALLENGES**	**Page 07-Page 23**	Mr. Alfredo M. Ronchi General Secretary of the European Commission-MEDICI Framework Piazza Leonarda da Vinci, 32, 20133, Milan, Italy 00390223991 alfredo.ronchi@polimi.it
3.	**SOCIAL MEDIA, USE, MISUSE, ABUSE, REGULATION AND THE WAY FORWARD**	**Page 24-Page 45**	Mr. Alfredo M. Ronchi General Secretary of the European Commission-MEDICI Framework Piazza Leonarda da Vinci, 32, 20133, Milan, Italy 00390223991 alfredo.ronchi@polimi.it
4.	**CYBER RESILIENCE, CYBER DISASTER MANAGEMENT - THE WAY FORWARD**	**Page 46-Page 54**	Mr. Alfredo M. Ronchi General Secretary of the European Commission-MEDICI Framework Piazza Leonarda da Vinci, 32, 20133, Milan, Italy 00390223991 alfredo.ronchi@polimi.it
5.	**DIGITAL TRANSFORMATION – NEED OF TODAY'S TIME**	**Page 55-Page 69**	Mr. Alfredo M. Ronchi General Secretary of the European Commission-MEDICI Framework Piazza Leonarda da Vinci, 32, 20133, Milan, Italy 00390223991 alfredo.ronchi@polimi.it

EMERGING CYBERLAW TRENDS IN 2021 IN INDIA

- **Abstract**

The year 2021 promises to usher in a new era of cyber legal developments and growth as far as India is concerned. This year is promising to see a plethora of activities which will contribute to evolving cyber legal frameworks and related ecosystem in India.

- **National Cyber Security Strategy**

One of the first keenly awaited trends in Indian Cyberlaw jurisprudence in the year 2021 will be the National Cyber Security Strategy. This Strategy will aim to build on the National Cyber Security Policy 2013 and would aim to be a comprehensive guiding gospel for individuals, all decision and policy makers as well as other stakeholders. The said Strategy is likely to throw more light on appropriate response mechanisms concerning protection of cyber security in all government and other sectors in India.

The Government of India has been working on the National Cyber Security Strategy for quite some time and the entire world is looking up with bated breath to see how the said Strategy is going to evolve. The National Cyber Security Strategy should inform the appropriate relevant authorities of all considerations they need to take into consideration, while dealing with cyber security ramifications concerning their operations. This assumes more significance as India is consistently on the radar as a potential target by cybercriminals and cyber security breaches. Given the fact that India does not have a law on cyber security, the National Cyber Security Strategy should be seen as an interregnum step, before India graduates to a full-fledged cyber security law.

While all attention will be on the new National Cyber Security Strategy, we need to be mindful of the legal ramifications of the said Strategy. The said Strategy document will be the manifestation of Government's thought processes and will not have the statutory penal force behind the same, unlike a law passed by the Parliament. Hence, the Strategy would be only a directory and would no longer be mandatory.

- **Need for Dedicated Law on Cyber Security**

Very quickly, India will have to work start working extensively on coming up with a dedicated national cyber security law. The need for having cyber security law by India is immense, because that will be an important tool to protect India, its cyber security and its cyber sovereign interests. At a time when a lot of other countries have already started coming up with dedicated laws on cyber security, India is slightly behind the curve. There is a need for appropriate action in this regard in order to ensure that India does not lag behind others in this direction.

- **Growing Cybercrimes in India and Their Regulation**

Meanwhile, cybercrime is likely to consolidate its further growth and position ever since the advent of The Golden Age of Cybercrimes in the year 2020. Cybercrimes including phishing, identity theft, and frauds have massively increased in the last one year. However, their coverage under the existing laws are neither adequate nor comprehensive.

We are further likely to see much more growth and consolidation in cybercrime penetration in India. This would underline the need for coming up with more effective and deterrent legal frameworks to regulate cybercrime. Hopefully, the year 2021 would see the Government focusing on more effective ways of trying to combat the newly emerging cybercrimes including phishing, identity theft, and financial frauds. The year 2021 could see the initiation of a process of making more stringent legal provisions for fighting cybercrimes in India.

- **Personal Data Protection in India**

Another major Cyberlaw trend in India for the year 2021 will be the passing and implementation of the Personal Data Protection Bill, 2019. Historically, India has not had a dedicated data protection law. The Government of India had tabled the Personal Data Protection Bill, 2019 before the Parliament of India in December 2019. The year 2020 saw the said Bill under the active consideration of the Joint Parliamentary Committee of the Indian Parliament.

At the time of writing, it is expected that the said Joint Parliamentary Committee would come up with its report in 2021 and on the basis of the same, the Government is likely to make appropriate changes in the Personal Data Protection Bill, 2019 and have it passed in the Parliament. This Bill is likely to change the rules of the game, in terms of providing stringent obligations for all data handling entities. Implementing the Personal Data Protection law will definitely strengthen the Indian Information Technology ecosystem, apart from strengthening appropriate protection for personal data. Hence, all stakeholders need to be prepared for a new set of compliances concerning data protection in the year 2021.

- **Protection of Non Personal Data in India**

This year is also likely to see the Government coming up with new approaches to deal with the protection of non-personal data. This is important as the Personal Data Protection Bill, 2019 only has a limited mandate of protecting personal data and non-personal data is clearly outside the ambit of the said law. It will be imperative that the Government would need to work extensively on the protection of non-personal data as well.

- **Need for Updating Indian Cyberlaw**

The year 2021 is also expected to see movement towards appropriate amendments in the Indian Information Technology Act, 2000. It is pertinent to note that the Information Technology Act, 2000 is India’s mother legislation to deal with all activities in the electronic ecosystem. The said law was passed more than two decades back and only got amended in the year 2008 and has been crying for appropriate amendments to make it more topical and relevant with the passage of time.

It is also hoped that the year 2021 could potentially see more appropriate changes in the Indian Cyberlaw, to incorporate enabling legal provisions to deal with the challenges thrown up by newly emerging technologies.

Further, the year 2021 is expected to see the Government coming up with new rules and regulations under the Information Technology Act, 2000. This is so because there are various areas and issues, where the Government needs to come up with appropriate rules and regulations under the Information Technology Act, 2000.

- **Protecting Indian Cyber Sovereignty**

The year 2021 should also see activities in the direction of enhancing and consolidating of cyber sovereignty of India. India as a nation needs to give more pronounced focus and importance to cyber sovereignty. India needs to learn from the experiences and experiments of other nations on cyber sovereignty and come up with appropriate mechanisms and processes to protect and preserve Indian cyber sovereignty.

- **Need For More Clarity On Blockchains**

The year 2021 could also hopefully see more action in India in terms of clarity on the legal issues concerning bitcoins and blockchains. India is by and large pretty ambivalent of its legal approaches concerning bitcoins and blockchains. However, with the increased adoption of Blockchains in various sectors of human activities and endeavors, the need has become more prevalent for India to come up with dedicated legal frameworks to regulate bitcoins and blockchains.

- **Enabling Regulation of Artificial Intelligence**

The year 2021 could also see more action in terms of coming up with enabling legal frameworks to regulate Artificial Intelligence. Artificial Intelligence is growing at a very rapid pace. A lot of developments are taking place in various applications of Artificial Intelligence in various sectors. However, the absence of enabling legal frameworks on Artificial Intelligence has led to a situation where enabling legal frameworks are required for further growth of Artificial Intelligence. Hopefully, the year 2021 could also see the Indian Government focusing on enabling legal frameworks for promoting Artificial Intelligence.

- **Enabling Regulation of Cloud Computing in India**

Further, we are likely to see more growth in terms of enabling legal frameworks for promoting cloud computing.

- **Expanding Scope of Data Breach Notification Law in India**

Data breach notification laws in the country would require a revisit. Hopefully, the year 2021 should see action in this regard. This is so because the data breach notification requirements are of the year 2017. Since the year 2017, a lot of new developments have taken place in terms of emerging varieties of cyber security attacks and breaches. There is a need for expanding the kinds of cyber security breaches that need to be reported, within the ambit of breach notification laws.

The previous years have seen that the data breach notification laws in India are observed more in breach rather than in compliance. The absence of enforceability of legal consequences for non-compliance with data breach notification laws has further changed the landscape and has pushed the Indian corporates in a level of complacency.

We are beginning to see more non-reporting of cybersecurity breaches, though these breaches have increasingly been reported in the public domain. Hopefully, the year 2021 would see the Indian Government coming up with more enabling legal frameworks to stringently enforce data breach notification laws in the country.

- **Need for Reviewing Intermediary Liability Provisions**

Hopefully, in the year 2021, the entire aspects of intermediary liability laid down by Section 79 of the Indian Information Technology Act, 2000 is likely to be increasingly coming into focus for potential review by the Government. More and more incidents in the last few years have demonstrated that after the passing of Shreya Singhal v/s Union of India judgment by the Hon’ble Supreme Court of India in March 2015, most of the intermediaries deliberately have misinterpreted the said judgment and taken the role of being a mere spectator, as things go wrong on their networks.

There is an urgent necessity for India to revisit the entire issue pertaining to intermediary liability. The draft Information Technology Intermediary Guidelines (Amendment) Rules, 2018 had sought to put more responsibilities on the intermediaries but it never got to be notified. Hopefully, the year 2021 could also see more action in this regard in the direction of regulating intermediaries.

- **Protecting Indian Critical Information Infrastructure**

India is likely to see far more cyber security breaches in the year 2021 targeted at its critical information infrastructure. Hence, India will have to make special efforts to protect and preserve its Critical Information Infrastructure from potential cybersecurity attacks.

- **Privacy Protection**

With the Aarogya Setu app increasingly collecting humungous volumes of data , Indians silently got sensitized about the need for protecting their privacy. I expect the year 2021 to also see more actions in the direction of having enabling privacy protections in India.

These are some of the key important Cyberlaw trends that I see on the horizon. Needless to say, I am not a soothsayer or an astrologer as I cannot predict the future. I believe that on the basis of my work, the aforesaid important Cyberlaw trends are likely to impact the growth of Cyberlaw jurisprudence in India in the year 2021.

Looking forward to a very exciting phase of growth of Cyberlaw jurisprudence in India in the year 2021.

CONTACT TRACING, MEDICAL DATA CONNECTED ISSUES & CHALLENGES

- **Abstract**

The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. To aid the safe lifting of current public health restrictions, new technologies are being developed – contact tracing APPs - and rolled out to automate labour intensive tasks critical to containing the spread of the virus. Our contact tracing survey summarises the principal regulatory and policy issues Applicable to contact tracing across a range of key jurisdictions in real time.

Keywords: *Contact Tracing, COVID-19, Medical Data, Data Ownership, Privacy, Ethics, Cybersecurity, Culture of cybersecurity*

- **Introduction**

In the last decades we faced different pandemics from AIDS to Ebola in 2020 the term pandemic took the real meaning to be global and really creating a global concern, the "transversal" risk of death.

Scientific studies and evidences show that COVID-19 is more severe an illness than is seasonal influenza, and is more contagious than are seasonal influenza viruses, having a basic reproduction number (R0) nearly twice as high.

COVID-19 was declared a pandemic by WHO on March 11, 2020, the first non-influenza pandemic, affecting more than 200 countries and areas, with more than 5·9 million cases by May 31, 2020. Countries have developed strategies to deal with the COVID-19 pandemic that fit their epidemiological situations, capacities, and values.

The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. Such "countermeasures", isolate infected people, locking down cities and countries, are not new, they recall medieval times plus some usual precautions in case of flue like to wash hands, keep a reasonable distance from other people, do not touch your mouth, nose or eyeswith dirty hands and in case of close contact wear a surgery mask as Chinese and far eastern people use to wear since long time, nothing better and more up to date ? Technology incredibly progressed though the time and more specifically cyber technology reinvented itself a number of times. We have crowd services, social media, IoT, sensors, AI, machine learning and any kind of privacy border line technology no chance to help fighting the pandemic?One of the first cyber toolsto be identified was the contact tracing APPs rolled out to automate labour intensive tasks critical to containing the spread of the virus. Of course, the ability to trace in real-time our contacts impacts our privacy and in some way our freedom, let's get much more in detail on potential privacy infringements and the golden balance to be find between privacy and public health.

- **The Different Perception Of Privacy Issues**

We know that since long time ago our “activities” were traced[1], for instance, by credit card companies and later on by telecom operators,the pervasiveness of cyber tech increased a number of times such tracing opportunity, CCTV, IoT and sensors, mobile position aware devices enabled google to trace our daily life asking why we get to a specific location even showing some pictures we shoot there.Nevertheless, citizens are really concerned about privacy issues related to medical folders and contact tracing even if,they are not really concerned in case of sport and wellness APPs that use to transfer our medical data to some almost unknown centralised servers.

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?

- **Contact Tracing Applications**

The pandemic moved the focus of already existent tracing application from security and marketing to interpersonal contacts, of course this sector was already active in the security field but become appealing to a wider set of software developers because of the incredibly wider potentialapplicationboth on citizens and government side.

There are a number of issues and challenges connected with contact tracing applications. In the EU, the general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19.

To start we can split into two main sectors both issues and challenges: citizens side and health authorities’ side.

If on the citizens side the positive aspect is to be alerted if any existent contact is dangerous the key concern is about to limit the infringement of their privacy and have a clear trust relationship with the software company and the government including the unit responsible for storage of data.We all know that health[2] is probably to only sector where privacy is applicable even to the owner of data him or herself.

These privacy concerns mean even the choice to download / install and activate the application. For sure the discovery that time ago, the updated version of Android and IOS had a specific section devoted to connect with tracing APPs didn’t enforce this trust relation knowing that anyway our phones are already traced by Telcos.

Since the start of the pandemic,governments and stakeholdersinvolved in the fight against the virus, such as the scientific research community, have been relying on data analytics and digital technologies to address this novel threat. Governments and private actors turned toward the use of data driven solutions as part of the response to the COVID-19 pandemic, raising numerous privacy concerns.In the EU, theGDPR data protection legal framework was designed to be flexible and, as such, is able to achieve both an efficient response in limiting the pandemic and protecting fundamental human rights and freedoms.

[1] Ronchi, A.(2019) , eCitizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer

[2] Ronchi, Alfredo M., (2019). e-Services: Toward a New Model of (Inter)active Community, ISBN 978- 3-030-01842-9, Springer (D)

There are a number of paragraphs within the UN Declaration of Human Rights[3] related to the management of the pandemic let's recall two of them: *Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. Article 13: 1. Everyone has the right to freedom of movement and residence within the borders of each State; 2. Everyone has the right to leave any country, including his own, and to return to his country.*

Data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures. Because the virus knows no borders, it seems preferable to develop a common European,if not global, approachin response to the similar crisis, or at least put in place an interoperable framework.

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

A draft list of the key aspects to be considered is:

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

- **Specific regulationsin Europe**

The Council of Europe issued a Joint Statement on Digital Contact Tracing on 28 April 2020 One month after the first Joint Declaration on the right to data protection in the context of the COVID-19 pandemic.

"*Recalling that the data protection standards, laid down by Convention 108 and its modernised version, Convention 108+, are fully compatible and reconcilable with other fundamental rights and relevant public interests, such as public health, it is crucial to ensure that the necessary data protection safeguards are implemented when adopting extraordinary measures to protect public health.*"

The council of Europe outlined that "*Regarding the use of mobile data and technology in the fight against COVID-19, specific measures are being deployed or otherwise proposed and include: use of mobile location data to evaluate movements of population or to enforce confinement measures, use of devices as digital proof of immunity, symptoms' detection, self-testing, or finally digital tracing of the contacts of an infected person.*"

[3] United Nations (1948). *Universal Declaration of Human Rights*. [online] . Available at: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf. [Accessed 8 Feb. 2021].

The European Union, in order to be compliant with Directive 95/46/EC (GDPR) adopted the following “*Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*” - Adopted on 21 April 2020.

The World Health Organisation didn’t perform adequately providing late advice and controversial recommendations.

Key points of these guidelines are:

- Use of location data,
- Sources of location data;
- Focus on the use of anonymised data;
- Contact tracing applications;
- General legal analysis;
- Recommendations and functional requirements.

Plus,a guide for the analysis of contact tracing applications.The first paragraph of the guide states that “*publishers of contact tracing applications should consider the following criteria:*

- *The use of such an application must be strictly voluntary. It may not condition the access to any rights guaranteed by law. Individuals must have full control over their data at all times, and should be able to choose freely to use such an application.*
- *Contact tracing applications are likely to result in a high risk to the rights and freedoms of natural persons and to require a data protection impact assessment to be conducted prior to their deployment.*
- *Information on the proximity between users of the application can be obtained without locating them. This kind of application does not need, and, hence, should not involve the use of location data.*”
- *When a user is diagnosed infected with the SARS-Cov-2*[4] *virus, only the persons with whom the user has been in close contact within the epidemiologically relevant retention period for contact tracing, should be informed.*”

Successful initiative or not?Here are some figures (November 2020):

Country	**Name of the APP**	**Download**	**Population**
Italy	Immuni	7 mio	60.40 mio
United Kingdom	Nhs Covid-19	12 mio	66,65 mio
Germany	Corona Warn	18,8 mio	83 mio
France	StopCovid / TousAntiCovid	3 mio	66.99 mio
Swiss	SwissCovid	2,8 mio	8,55 mio

[4] Alias COVID-19

- **National initiatives**

Major part of the countries around the world decided to structure the fight against the pandemic on three main action lines:

- ❖ Health - healthcare guidelines and pharma;
- ❖ Laws and Regulations - ad hoc regulations and recommendations;
- ❖ Technology - information technology tools and APPs.

The health sector atnational level, after a first unappropriated attempt to “close the borders” to the virus, issued general and specific recommendations to mitigate the risks trying to harmonize the different initiatives or at least take advantage from other’s experiences and solutions.

The first two actions were not so different from the one taken on the occasion of historical pandemic, one of the attempts to create a new “weapon” to defeat the disease come from the technological sector. Tracing applications were already developed and running in the security sector from passengers shadowing to GPS or phone cell triangulation and more. The basic concept was to be able to trace citizens thanks to their mobile phones thank to an APP that will be able to alert them in case of dangerous contacts, all this without infringing privacy issues and potential malicious use of data.

As already outlined we waived some of rights to improve our safety or access some services and communication opportunity. The contact tracing APPcan succeed only if a relevant number of citizens will install and activate it that means that a trust relationship between citizens and the “APP party” must be strong. Where “APP party” means the government, data managers and controllers, software developers and telecom operators. Let’s have a look to some potential vulnerabilities.

- **Cybersecurity: APPs main vulnerabilities**

Hacking[5] a decade ago was exclusively reserved for the professionals, white-hat hackers, penetration testers; whose duty it was to break through the firewall of corporate and personal security. Nowadays the scenario is quite different, “professional” white-hat hackers are a small portion of hackers, basic hacking techniques are available on line on the Internet and more sophisticate or cutting edge are exchanged on the dark net, in addition the increasing “hacking as a service” offer is boosting business and “family[6]” affairs.

Dealing with COVID 19 contact tracking APPs since data strictly related to personal health conditions are taken into consideration, the choice of the safety model to be adopted is a paramount. What would happen if once a "GovernmentalAPP" was installed, it was hacked and compromised the content of the smart phone itself by some criminal? Undermining the integrity of the APP could allow not only to steal or compromise data, but also to take full possession of the device of those who installed the software on their device. In Europe contact tracing applications are installed on voluntary basis as stated by EU regulations this “voluntary” mode of the APP implies that no negative consequences can be associated with a person’s refusal to use the APP. Thus, screening tests, care, the ability to travel, access to certain services (e.g. public transport) cannot be made conditional on the use of contact tracing APPs. This has direct impact to employers, who may not subordinate certain rights to the use of these APPs, as this would amount to discrimination. Besides, an employer cannot compel their employees to download the APP.

[5] Ronchi, A.(2019) , eCitizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer

[6] Illegal access to private email and mobile phone messages to find evidences of betryals and more.

First of all, it must be remembered that many defects in software applications, IT processes or communications protocols do not have a real solution and, due to a closed flaw, new ones are opened; it is the never-ending competition between attacks and counter measures. Due to this reason, cyber security observers attest every year to an exponential increase in cybercrime attacks on our devices, which are the preferred victims of hackers mainly due to their capillary presence and the reduced skills or will to invest time to protect them constantly. This even if smart phones and sometimes tablets are the custodians of our most precious sensitive data (IDs including digital ones, bank account access tools, credit cards, social security, etc.).

Recent reports by security companies Palo Alto Networks[7] and Bitdefender[8] attest to how cybercriminals focus their attacks on the countries hardest hit by Covid-19, such as Italy. The Clusit (Italian Association on Cybersecurity) 2020 Report[9] also underlines that the attacks no longer start from individual web pirates, but from organized groups that base their business, for example, on knowledge of a person's health conditions. The interest is therefore very high and it is easy to expect continuous cyber-attacks.

To secure APPs it will be necessary to verify that the most serious vulnerabilities have been carefully considered, including those listed below:

SIMJacker: serious security flaw in the devices that use SIM cards for their operation, so not only phones, but also IoT products. How does the attack happen? Simply through an ad hoc SMS, sent by an attacker to his victim who, not noticing anything (the SMS does not appear!), Finds himself with a phone spying on him;

Sniffing BLE (Bluetooth Low Energy) Long-Lived: Vulnerability that exploits Bluetooth transmissions. This vulnerability is present in the Bluetooth protocol, in particular in the implementation of BLE chosen, as suggested by the European Data Protection Supervisor(EDPS)[10], to operate some contact tracking APPs. The attack allows you to spy on the victim by bypassing the protection used by the devices. In this way it is possible to track a person, collecting details in reference to his location and other potentially sensitive information;

Knob: defect in the Bluetooth standard, whereby in an outdated system an attacker can decrypt the information exchanged by the two devices and access our data, or listen to our conversations.

ToRPEDO & PIERCER[11]: A group of researchers from Purdue University and the University of Iowa revealed that 4G and 5G network protocols suffer from a number of vulnerabilities that would allow hackers to access users' phone calls and track their location.

Additional concerns to be carefully considered relates to the use of a centralized server instead of a distributed or partially distributed one. The use of a centralised server increases the risk of possible

[7] https://www.paloaltonetworks.com [Accessed 8 Feb. 2021].

[8] Bitdefender.com. (2017). *Bitdefender - Global Leader in Cybersecurity Software*. [online] Available at: https://www.bitdefender.com/ [Accessed 8 Feb. 2021].

[9] Clusit (2020). *Rapporto Clusit*. [online] Clusit. Available at: https://clusit.it/rAPPorto-clusit/ [Accessed 8 Feb. 2021].

[10] European Data Protection Supervisor - European Data Protection Supervisor. (2021). *European Data Protection Supervisor*. [online] Available at: https://edps.europa.eu/ [Accessed 8 Feb. 2021].

[11] Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information

cyber-attacks and the temptation to exploit this data for purposes other than those provided for by law. Of course due to the GDPR[12] and national regulations the server must be physically located in the EU and run under the European Data Protection Supervisor recommendations.

Potential discrimination – people who do not use the APPdelivered on voluntary basis might not be able to work or access certain public places freely, meaning their consent was not freely given and therefore is void.

Potential "Big Brother" Surveillance – in the event that the APP is adopted by part of the population, it is feared that the Government may more easily impose it on the rest of the population against their will. Moreover, if the APP is not based on pure anonymization[13] – that meansthat it is at best pseudonymous[14], users will not be protected against any kind of individual surveillance[15].

Security acclimatization – once the APP is deployed and activated, it will be easier for the Government to add coercive functions to it (individual control of lockdown). Moreover, the APP could provide an incentive to subject one's body to constant surveillance, which will reinforce the social acceptability of other technologies, such as facial recognition or automated video surveillance, which are currently widely rejected. This is in some way what is usually termed "Bad ambassador effect". To what extent are we willing to give up our privacy and freedom to increase safety, security and top down control? Let's have a look to some contact tracing APPs.

- **Italyas at November 2, 2020**

On 29 April 2020 the Italian Government issued a law decree setting out the rules governing the adoption of a tracing APP (Law Decree no. 28 of 30 April 2020[16], the Decree). On June 15, after a beta test in four regions, the APP has been made available to citizens on voluntary basis.

User tracing APPs must comply with both GDPR and strict Italian rules on remote monitoring of employees (Private Sector). Main privacy concerns and potential misuse lie in data minimization, data security, re-identification risk and actual prevention of re-use of such data for other purposes. A government wide-spread concern was about ownership and localization, in addition the data controller must be the Ministry of Health, and that data must be stored in servers on the Italian territory.

The Data Privacy Authority[17] considers that the Decree on the APP complies with national regulations and with European Data Protection Board (EDPB)[18] guidelines. The Italian Data

[12] GDPR.eu. (2019). *General Data Protection Regulation (GDPR) Compliance Guidelines*. [online] Available at: https://gdpr.eu/ [Accessed 8 Feb. 2021].

[13] Department of Health and Social Care (2020). *NHS COVID-19 app: anonymisation, definitions and user data journeys*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/anonymisation-definitions-and-user-data-journeys [Accessed 8 Feb. 2021].

[14] Prime Factors. (2020). *Psuedonymzation & Anonymization of Data - Prime Factors*. [online] Available at: https://www.primefactors.com/solutions/pseudonymization-anonymization/ [Accessed 8 Feb. 2021].

[15] Pseudonymous data is information that no longer allows the identification of an individual without additional information and is kept separate from it. In exchange for the lower level of privacy intrusion, the applicable requirements are less stringent.

[16] Gazzettaufficiale.it. (2020). *Gazzetta Ufficiale*. [online] Available at: https://www.gazzettaufficiale.it/eli/id/2020/04/30/20G00046/sg [Accessed 8 Feb. 2021].

Processing Authority[19] has issued an opinion on the Decree, a note on the DPIA, and authorization to the Ministry of Health in its quality of data controller for the data processed through the APP. The name of APP is Immuni[20]. The activation of the APP, as already stated, is voluntary and there is no need to use it to enter public spaces. Limitations are not mitigated by the use of the APP.

To download the APP few information are required (province of domicile and to be aged over 14) no registration/account required. As major part of the tracing APPs contacts is traced thanks to a Bluetooth interface, the GPS signal or any other position detection tool cannot be used accordingly with EU and national regulations. The APP generates a one-time identifier the "key" to be exchanged on the occasion of a contact with an active ImmuniAPP, data collected are stored in a semi-centralised data base. The Decree requires a 'suitable level of security" to be adopted. Anonymization or (if not possible) pseudonymization is required.

The centralised server stores the keys uploaded by infected usersplus some other data while the keys of contacts are stored locally in the smart phone memory. The application uses the "privacy by design" approach and pursuant to the Decree, a data processing impact assessment has been carried out. Keys of contacts are stored on each device for 14 days. The same retention period applies to keys uploaded by infected users on the centralized server. In any event, no data can be retained until the end of the state of emergency and in any case not later than 31 December 2020 (new regulations will be issued).

How does this APP works mush more in detail? Once installed, the APP causes the smartphone to continuously emit a low energy Bluetooth signal (BLE), with a proximity identifier. When they come into contact with each other, smartphones record each other's proximity identifier in their memory, keeping track of that contact, how long it lasted and the distance between the devices.
The identification code is temporary and anonymous, it varies often to minimize continuous tracking risks and allows the APP to establish a contagion risk assessment for each contact, based on the information uploaded voluntarily by users.

In fact, a user who tested positive for Covid-19 can personally upload the cryptographic keys to a server to trace his proximity identifier. For each user, the APP periodically downloads from the server the new cryptographic keys uploaded by users who tested positive for the virus, derives their proximity identifiers and checks if any of those identifiers correspond to those recorded in the smartphone memory in the previous days. If the APP registers that you have been close to someone positive for the virus, it will check if the duration and distance of the contact could have caused the infection. If so, the APP can send notification messages to instruct you to isolate yourself and contact the health authority.

In the beta and first version of the application a "clinical diary" function, where users can record the progress of their symptoms, was included, in the latest versions has been removed.

[17] Garanteprivacy.it. (2016). *The Italian Data Protection Authority: Who We Are*. [online] Available at: https://www.garanteprivacy.it/home_en/who_we_are [Accessed 8 Feb. 2021].

[18] European Data Protection Board - European Data Protection Board. (2021). *European Data Protection Board*. [online] Available at: https://edpb.europa.eu/edpb_en [Accessed 8 Feb. 2021].

[19] Garanteprivacy.it. (2018). *Home*. [online] Available at: https://www.garanteprivacy.it/home_en [Accessed 8 Feb. 2021].

[20] Italia.it. (2020). *Immuni - Sito Ufficiale*. [online] Available at: https://www.immuni.italia.it/ [Accessed 8 Feb. 2021].

Accordingly, with the official figures on November 2020 the APP Immuni was downloaded by seven million citizens there are no data regarding the activation of the downloaded APPs.

- **France as at December 2, 2020**

On May 29, 2020 France government published a decree (*Decree No. 2020-650 of May 29, 2020 relating to data processing known as "StopCovid"*) setting the definitive legal framework for the implementation of the contact tracing APP. On June 2, 2020 INRIA[21] (National Institute for Research in Digital Science and Technology) released to the public the APP StopCovid.

On October 22, 2020 the Government presented a new version of the APP named "TousAntiCovid". Officially, as stated by the Health Ministry, TousAntiCovid is an update of the latest version of StopCovid. TousAntiCovid provides easy access to other tools including*"DepistageCovid"*, which provides a map of nearby testing centres and waiting times, and*"MesConseilsCovid"*, which provides personalised advice on how to protect oneself and others.

Both StopCovid and the following version TousAntiCovid[22] are available on voluntary basis, no information will be needed to download and register the APP.

The APP will generate ephemeral crypto-identifiers (e.g. every 15 minutes) associated to the terminal (and not the person) to trace contacts via Bluetooth, no GPS location aware systems are in use.Of course, if we look at the "anonymisation" of the user applying the Aristotelian syllogism the crypto-identifiers are associated to the terminal (and not to the person) and the terminal is associated to the person via IMEI, SIM, MAC we derive that the crypto-identifiers are associated to the person.

Thus, the APP is not considered to anonymously trace positive to COVID citizens but it is at best pseudonymous. If a user is clinically diagnosed or is tested positive for COVID-19, he or she can choose to report it to the APP and to transmit his or her proximity history to the centralised server. Each smartphone that has downloaded the APP regularly checks with this central server to see if its crypto-identifiers are among those at risk. If they are, the APP will generate an alert sent to the user, to indicate that he/she might have been exposed to the virus, and the measures to be taken.

The decision to use a centralised server has been the subject of much criticism. It has been abandoned in Germany, which opted for a decentralized system. France Government considers that the centralised architecture offers more guarantees and security. Proximity history data recorded by the APP on the mobile phone are kept for 15 days from the time they are recorded. When this data is shared on the central server, it is also kept for 15 days from the time it is recorded. The shared authentication key and the crypto-identifiers are retained until the user uninstalls TousAntiCovid and in any event no later than six months after the end of the state of health emergency in France (currently set to be February 16, 2021). The APP can be uninstalled at any time.

Accordingly, with the official figures on November 2020 since its launch, the APP has been downloaded by almost 9.5 million people.More than 13,000 people have been notified as having been in contact with an infected person.

[21] Inria.fr. (2021). *Accueil | Inria*. [online] Available at: https://www.inria.fr/en [Accessed 8 Feb. 2021].

[22] Gouv.fr. (2021). *TousAntiCovid*. [online] Available at: https://bonjour.tousanticovid.gouv.fr/index-en.html [Accessed 8 Feb. 2021].

Some remarks concerning privacy issues, a French researcher in cryptography[23], few weeks after the release of the first version of StopCovid explained that the APP collects more data than originally understood. His findings show that all cross-contacts are sent to the central server, contrary to the government guidance which states that only the APP users who had been in contact for 15 minutes, closer than **one meter** away from a person who tested positive for COVID-19 would be stored, meaning that the APP processes more data than necessary to trace the spread of the virus, this represent an infringement to the data minimization principle. The second version of StopCovid, launched at the end of June, remedied this problem, but the French Data Protection Authority (the "CNIL[24]") noted that this second version still contained certain shortcomings concerning user information, the subcontracting contract granted to INRIA and certain data processing aimed at securing the APP. Therefore, the CNIL gave the Health Ministry formal notice to remedy this on July 20, 2020. Following the formal notice, as the CNIL considered the processing implemented were now compliant with the EU and French legislative data protection requirements, it declared the closure of the formal notice on September 3, 2020.

- **Germany As at June 23, 2020**

On June 16, 2020 the German Federal Government launched an official APP "Corona-Warn-APP[25]" which was developed by SAP[26] and Telekom[27] on behalf of the German Federal Government. The "Corona-Warn-APP" is based on the Privacy-Preserving Contact Tracing[28] ("PEPP-IT").

The German contact tracing APP and its backend infrastructure is entirely open source licensed under the Apache 2.0 license. The Corona-Warn-APP is being developed on basis of the Exposure Notification Framework ("ENF")[29] provided by Apple and Google, which will use Bluetooth Low Energy technology ("BLE")[30]. The ExposureNotification framework defines two user roles:
Affected user

[23] Gaëtan Leurent, researcher at Inria in the team COSMIQ, working on symmetric cryptography.

[24] Cnil.fr. (2016). *CNIL |*. [online] Available at: https://www.cnil.fr/ [Accessed 8 Feb. 2021].

[25] Coronawarn.app. (2020). *Open-Source Project Corona-Warn-App*. [online] Available at: https://www.coronawarn.app/en/ [Accessed 8 Feb. 2021].

[26] SAP. (2017). *SAP Software Solutions | Business Applications and Technology*. [online] Available at: https://www.sap.com/index.html [Accessed 8 Feb. 2021].

[27] Deutsche Telekom AG (2020). *Home*. [online] Telekom.com. Available at: https://www.telekom.com/en [Accessed 8 Feb. 2021].

[28] Klaine, P.V., Zhang, L., Zhou, B., Sun, Y., Xu, H. and Imran, M. (2020). Privacy-Preserving Contact Tracing and Public Risk Assessment Using Blockchain for COVID-19 Pandemic. *IEEE Internet of Things Magazine*, [online] 3(3), pp.58–63. Available at: https://ieeexplore.ieee.org/document/9241473?denied= [Accessed 8 Feb. 2021].

[29] Apple.com. (2020). *Apple Developer Documentation*. [online] Available at: https://developer.apple.com/documentation/exposurenotification [Accessed 8 Feb. 2021]. Exposure Notifications: Helping fight COVID-19 - Google. (2021). *Exposure Notifications: Helping fight COVID-19 - Google*. [online] Available at: https://www.google.com/covid19/exposurenotifications/ [Accessed 8 Feb. 2021].

[30] Bluetooth® Technology Website. (2017). *Intro to Bluetooth Low Energy | Bluetooth® Technology Website*. [online] Available at: https://www.bluetooth.com/bluetooth-resources/intro-to-bluetooth-low-energy/ [Accessed 8 Feb. 2021].

"*When a user has a confirmed or probable diagnosis of COVID-19 (as defined by the Health Authority), the framework identifies them as affected and shares their diagnosis keys to alert other users to potential exposure.*"
Potentially exposed user
"*To assign a user the potentially exposed role, use the framework to determine whether a set of temporary exposure keys indicate proximity to an affected user. If so, the app can retrieve additional information such as date and duration from the framework.*"

The Corona-Warn-APP will collect pseudonymous data from nearby mobile phones using BLE. As soon as two users approach each other within a distance of about two meters and remain at this distance for fifteen minutes or longer, their APPs will exchange data via BLE. If a user tests positive for COVID-19, the user can feed the test result into his/her Corona-Warn-APP. The Corona-Warn-APP will then anonymously inform all stored contacts. The data will be stored locally on each device preventing access and control over data by authorities or a third party.

"Corona-Warn-APP" and privacy issues; there are no major privacy concerns as the Corona-Warn-APP has been designed with a special focus on privacy from the beginning. The German Data Protection Authorities[31] generally support the Corona-Warn-APP and only expressed minor concerns, but less on the Corona-Warn-APP itself but rather on the way it may be used by IT key players.
As Apple and Google, as providers of the operating systems, have access to all data that runs over their interfaces, there are some concerns regarding the behaviour of Apple and Google.

The Corona-Warn-APP is deployed on voluntary basis but this aspect of could be undermined through social or economic pressure which could be specifically enforced by employers. As already expressed in the previous paragraph regarding anonymity issues, the Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit[32]) announced that the use of the telephone-Tan-registration is not an optimal solution because the complete anonymity of the user will no longer be guaranteed.

Currently there is one other APP available in Germany launched by Robert Koch Institute[33] (German federal government agency and research institute responsible for disease control and prevention, "RKI") – "Datenspende-APP[34]". This APP does not yet trace contacts, but only general movement and fitness information. The APP collects the user data using their fitness tracker and sends it to the RKI. The RKI analysis anomalies in the data, which is sorted by postcode: As pulse rate, sleep rhythm and activity level change due to an acute respiratory disease, the RKI claims that it can also indicate a Covid-19 disease having this data.

[31] Bund.de. (2020). *Internetauftritt des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - Homepage*. [online] Available at: https://www.bfdi.bund.de/EN/Home/home_node.html [Accessed 8 Feb. 2021].

[32] Bund.de. (2021). *Internetauftritt des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - Startseite*. [online] Available at: https://www.bfdi.bund.de/DE/Home/home_node.html [Accessed 8 Feb. 2021].

[33] Www.rki.de. (2020). *RKI - Homepage*. [online] Available at: https://www.rki.de/EN/Home/homepage_node.html [Accessed 8 Feb. 2021].

[34] Www.rki.de. (2021). *RKI - Coronavirus SARS-CoV-2 - Corona-Datenspende-App*. [online] Available at: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende-allgemein.html [Accessed 8 Feb. 2021]. Koch-Institut, R. (2020). *Corona Datenspende*. [online] Science Blog. Available at: https://corona-datenspende.de/science/ [Accessed 8 Feb. 2021].

At the beginning of April 2020, RKI launched the official Corona Data Donation App. Since then, 529.281 German inhabitants have decided to donate their data. Some of you may be asking yourselves questions about the purpose of this project and the expected scientific results. On this site, RKI would like to give the donor, a glimpse into the scientific process by sharing findings as RKI uncover them. To achieve this transparency, RKI regularly posts updates detailing the methodological approaches and interim results of analyses creating a Fever Map for Germany using vital signals collected by wearable health and fitness tracking devices and donated by sponsors.
The aim of this map is to detect regions in which the number of residents exhibiting fever symptoms is higher than average. By updating the map on a daily and municipality-level basis, RKI aims to identify so-called "hot spots" of COVID-19 as they emerge.

There are several concerns indicated by Chaos Computer Club[35], a cyber security NGO, in particular:

- ❖ RKI can directly retrieve the fitness data from the provider of the fitness tracker as the smart bracelet and wrist watch or Google Fit and only then the data will be pseudonymized (except Apple Health). As the RKI also stores access data to the fitness tracker, it can be used to access complete history and names of the users.
- ❖ Easy reversal of the pseudonymisation and the insecure handling of the confidential pseudonym as the APP does not use a standard browser but an embedded web view which is insecure due to man-in-the-middle attacks.
- ❖ The RKI server exposes additional functionality such as a management and admin interface as well as a SOAP API via the Internet. This increases its vulnerability."

- **What about China[36] ?**

Over 20 million people in three Chinese cities were under lockdown as of Friday 24 January 2020 morning, as authorities battled an outbreak of a novel coronavirus first discovered at the beginning of January in Wuhan, China, in the central province of Hubei. The strong Chinese measures came after the World Health Organization[37] decided not to declare the outbreak a "public health emergency of international concern" (PHEIC)."[38]

On January2020 China declared the Health Emergency in the city of Wuhan and Hubei Province; this paragraph offers a quick overviewon the different strategies adopted by Chinese Government after the health emergency this before setting the focus on contact tracing applications as key tool to detect cases and manage them.China embraced two main strategies, "Containment" and "Suppression". As outlined by Chinese researchers[39] "*Strategy decisions were based on factors including feasibility of interrupting virus transmission, estimates of disease severity, projected social and economic effects of strategy and disease, public acceptance and willingness, and last but*

[35] Www.ccc.de. (2020). *CCC | Home*. [online] Available at: https://www.ccc.de/en/ [Accessed 8 Feb. 2021].

[36] Updated 24 January, 2020

[37] Who.int. (2018). *Home*. [online] Available at: https://www.who.int/ [Accessed 8 Feb. 2021].

[38] https://www.facebook.com/HealthPolicyWatch (2020). *WHO Refrains From Declaring Public Health Emergency Now Over Coronavirus Virus Outbreak; But 3 Chinese Cities On Lockdown - Health Policy Watch*. [online] Health Policy Watch. Available at: https://healthpolicy-watch.news/wuhan-china-goes-on-lockdown-who-postpones-decision-on-public-health-emergency-over-virus-outbreak/ [Accessed 8 Feb. 2021].

[39] Zhongjie Li, Qiulan Chen, Luzhao Feng et al. Active case finding with case management: the key to tackling the COVID-19 pandemic. The Lancet https://doi.org/10.1016/S0140-6736(20)31278-2 (published on line June 4, 2020)

not theleast, government willpower and capacity.” In addition to these two main strategies there was a third one “mitigation”, which has not been implemented in China, include similar or overlapping measures. Comparison of the three basic strategies shows that all use non-pharmaceutical interventions as outlined in the following lines.

“Containment” strategy applies to an early-stage epidemic in a geographically limited area, taking measures that prevent person-to-person transmission of SARS-CoV-2[40] and importation and exportation of infection. The core measures of a containment strategy are proactive finding and managing cases, tracing and quarantining close contacts, and strict restriction or control of population movement when feasible and appropriate.

Maximum timeliness was requested from hospitals, laboratories and prevention departments to test, treat and isolate each suspected case and trace and isolate contacts in the shortest possible time (the time elapsed from the onset of symptoms to diagnosis went from 12 days in January to just 3 days in early February): statistical models have shown that it was above all this that reduced the number of infected and dead, compared to travel and contact restrictions. Without these measures, the number of infections would have been about 67 times greater, as some experts stated.

Core measures are summarised in:
Aim: Stop virus transmission and spread.
Scenario: Early stage of epidemic in well-defined areas.
Case detection and management: Active case detection; managed isolation and care; quarantine of close contacts.
Lockdown and intercity travel prohibition: Lockdown of endemic areas; restrict travel from those areas to other low epidemic areas.
Other physical distancing: Strict stay-at-home orders; school closure; cancellation of mass gatherings.
Personal protection: Hand hygiene; respiratory etiquette; face mask use.
Duration: Short term, followed by maintenance of elimination of transmission.
Endpoint: Vaccine response to immunise the population to achieve community protection.
Pros: Early, proactive, and strict implementation can be effective, largely preventing infection and death.
Cons: Major short-term effect on daily life and social and economic costs; continued moderate socioeconomic effects during elimination period.

The second strategy applied was that of “Suppression”, after the containment strategy has been successful and only sporadic cases and small outbreaks remain. “Suppression” strategy is useful when an epidemic is in multiple areas with varying degrees of outbreak and community spread, when it is not possible or feasible to stop spreading by confining transmission to an isolatable geographical area.

In this case, the goal is to keep the infection reproduction index (R0) low (below 1) and prevent the importation of cases. In this phase, the lockdown measures are gradually loosened (reopening of schools, restaurants and shops, etc.) even if maximum control is exercised on individual cases and small outbreaks with the restoration, if necessary, of containment measures. People who move between areas at different risk report it online or via a telephone application, which also supports in China public health operators in tracking contacts. Naturally, physical distancing and personal hygiene measures, the obligation to wear masks indoors and the ban on gatherings remain in force.

[40] Alias COVID -19 in news

Core measures are similar to those for containment and are summarised in:
Aim: Decrease or stop community transmission.
Scenario: Ongoing community transmission in which containment is not feasible.
Case detection and management: Case detection; managed isolation and care; testing of close contacts.
Lockdown and intercity travel prohibition: Few, based on risk-
Other physical distancing: Stay-at-home orders; school closure; cancellation of mass gatherings; adjustable to conditions.
Personal protection: Hand hygiene; respiratory etiquette; mask use.
Duration: Long term, adjusting suppression measures based on epidemic situation (relax or strengthen periodically).
Endpoint: Vaccine response to protect the vulnerable, stop community transmission, and achieve community protection.
Pros: Early, proactive, and strict implementation can be effective, largely preventing infection and death.
Cons: Major short-term effect on daily life and social and economic costs; premature relaxing of interventions can lead to rebound of the epidemic.

“Suppression” logically follows successful “Containment” to prevent spread from imported cases and re-establishment of community transmission. Suppression measures can keep transmission and prevalence low, decreasing the effective reproduction number (Re). Once Re is below 1 in a community, spread in that community should eventually stop. However, maintenance of strict suppression measures, particularly lockdowns and physical distancing, brings a large socioeconomic burden.

The third strategy not implemented in China, is “Mitigation”, the key aspects of Mitigation are:
Aim: Lower and delay the epidemic surge to reduce health-care demand.
Scenario: Extensive community transmission, impossible to suppress.
Case detection and management: Detection of severe cases; managed isolation and care; limited contact tracing.
Lockdown and intercity travel prohibition: None.
Other physical distancing: Cancellation of mass gatherings; school closure when and where necessary; ask vulnerable population to stay at home.
Personal protection: Hand hygiene; respiratory etiquette; face mask use.
Duration: Long term.
Endpoint: Vaccine response to protect the vulnerable, stop endemic transmission, and immunise the population to achieve community protection.
Pros: Less short-term socioeconomic effect; necessary medical care able to be provided.
Cons: Medical system capacity can still be exceeded; substantial risk of high morbidity, mortality, and economic damage.

To enforce case detection and management the Ministry of Information Industry Technology after the COVID-19 crisis outbreak decided to take advantage from an ad-hoc information technology platform. The Chinese Government encouraged the introduction of APPs for the dynamic certification of health status in a notice released by the State Council[41] Joint Defence or Control Mechanism in February 2020.

[41] Www.gov.cn. (2021). *The State Council of the People’s Republic of China*. [online] Available at: http://english.www.gov.cn/ [Accessed 8 Feb. 2021].

Based on this platform, telecom carriers (China Mobile, China Unicom and China Telecom[42]) may provide a tracking record of the cell phone users' location in the past 15 days or up to 30 days.

On the citizens side, various APPs with similar functions were introduced in different regions of China to achieve a dynamic certification of health status of the local residents. Different status (red, yellow or green) will impose a different level of restrictions or regulations. The name of such applications is "Health Code" or similar name which can be a separate APP or integrated into Alipay and WeChat. The download and activation of the APP is voluntary, whilst not technically compulsory, a clean result (i.e. green status) of the APP, the "health code", is required to be presented for access to certain public buildings or areas.

The purpose of the "health code" system is to control and monitor movements around China based on the risk profile of a user. Individuals are allocated a QR "health code" which is either green (low risk and free to move around), amber (which means at risk and must quarantine for seven days in some regions) or red (which means high risk and must quarantine for 14 days in some regions).

QR codes must be scanned before entering public places such as subway stations and shopping malls, and in some cities, before leaving apartment complexes and access will be denied and the authorities alerted if the individual should be in quarantine in accordance with their QR health code. The clean result of the APP is compulsory when the user goes to hospital or tourist sites and certain other locations; employers and owners of office buildings may require clean results of location tracking records before the resumption of work. Furthermore, some public workplaces may require visitors to provide dynamic certification of health status before granting access.

Some newspaper said that in practice, not all the operators of public workplaces, e.g. office buildings or restaurants, are strictly implementing the restriction of access based on the results of the APP.

With reference to privacy issues, following the Chinese laws and regulations when the personal data is collected and used for public security purposes, no consent from individuals providing it is required. This is the principle established by the Personal Data Security Specifications. The notice issued by the Cybersecurity Administration of China supporting mechanisms to control COVID-19 (Notice) provides that entities authorized by National Health Committee are entitled to collect this data without consent.In practice, both the Government or authorized private sector organizations may have access to personal data, but the mechanism for the processing, use and storage of the personal data lacks transparency, with the potential for abuse of personal data in the future.

Some additional remarks from Chinese citizens, they consider that information collected is excessive. To use the APP citizens must provide: Name, ID card number and facial scan. The exact data varies with the APPs. Users are required to complete a detailed questionnaire setting out medical and travel history, national identity number, possible symptoms they may have etc.

The technology rationale of these APPs is not publicly available, but it is based on the records of the individuals' location (GPS, triangulation?). No official information about the use of centralised servers, the identity and basic information of the infected user must be reported to the Disease

[42] Founded in September 2000, China Telecom is a large state-owned communication backbone enterprise. China Telecom owns the technology-leading mobile communication network. It provides global customers with comprehensive information services and customer service channel system covering all regions and services. As one of the most critical technology revolution, the development and application of Artificial Intelligence technology have risen to the level of national strategy.

Control and Prevention Centre(China CDC)[43]within a designated timeline. Based on the investigation and management guidelines of “contiguous”, the contiguous must fill out the relevant forms and report to the local Disease Control and Prevention Centre. Both the contiguous’ and the infected user’s identity is required to be filled out by the “contiguous”.

In general, in compliance with Chinese laws and regulations no consent is requested to upload and share information, e.g. the APP used in Beijing does not require consent to share or upload the data;outside of Beijing there are regional differences in the APP.

More in detail the APP used in Beijing only generally indicates that data collection is compliant with the law and only for the purpose related to COVID-19, without incorporating “privacy by design” or indicating if a privacy risk assessment has been completed, and does not make any reference to the data retention term. There are regional differences in the APPs.

Concerning data security, the data controller is responsible for the data security and must take strict management and technical measures to prevent data leakage, only the organizations authorized by the National Health Commission[44] according to the law can collect the data for the COVID-19 related purpose without consent from data subjects. Other unauthorized organizations must secure consent from data subjects before data collection.

- **Closing remarks**

We explored some of the key issues and concerns related to the use of contract tracing applications. The use of such applications has been planned in conjunction with a set of measures that all use non-pharmaceutical interventions. Different countries all around the world issued specific norms and regulations concerning the guidelines to develop contact tracing APPs. The European Institutions published clear regulations and recommendations concerning the design and development of the APPs. Key aspects to be carefully considered were privacy issues starting from the personal information requested to download and activate the APP, the anonymisation, sometimes pseudo-anonymisation, of data to be exchanged to validate potential risky contacts, the request of consent to store contact info and related upload on local, semi-centralized or centralised servers. How long personal data will be stored on servers, who is in charge as data controller, and who is entitled to access or share such data.

An additional relevant aspect concerns the voluntary or compulsory use of the APP not only related to the activations but much more related to the need to have a positive/green feedback from the APP in order to perform an activity or enter a specific place.

- **Bibliography**

Clusit, Rapporto Clusit 2020 sulla sicurezza ICT in Italia, Clusit - Astrea
Council of Europe, Joint Statement on Digital Contact Tracing, Strasbourg April 2020
European Data Protection Board (edpb), Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

[43] Chinacdc.cn. (2016). *Chinese Center for Disease Control and Prevention*. [online] Available at: http://www.chinacdc.cn/en/ [Accessed 8 Feb. 2021].

[44] Nhc.gov.cn. (2018). *National Health Commission of the PRC.* [online] Available at: http://en.nhc.gov.cn/ [Accessed 8 Feb. 2021].

A, Hendy SC, Plank MJ, Steyn N. Suppression and mitigation strategies for control of COVID-19 in New Zealand. medRxiv 2020; published online March 30. DOI:10.1101/2020.03.26.20044677 (preprint).

Syed Rafiul Hussain, et. Al., Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information, Internet Society, ISBN 1-891562-55-X

Lai S, Ruktanonchai NW, Zhou L, et al. Effect of non-pharmaceutical interventions to contain COVID-19 in China. Nature 2020; published online May 4. https://doi.org/10.1038/s41586-020-2293-x.

Zhongjie Li, Qiulan Chen, Luzhao Feng et al. Active case finding with case management: the key to tackling the COVID-19 pandemic. The Lancet https://doi.org/10.1016/S0140-6736(20)31278-2 (published on line June 4, 2020)

PresidenzaConsigliodeiMinistri, DPCM 03/12/2029

Ronchi, Alfredo M., (2019).*e-Citizens: Toward a New Model of (Inter)active Citizenry* , ISBN 978-3- 030-00746-1, Springer (D)

Ronchi, Alfredo M., (2019). *e-Services: Toward a New Model of (Inter)active Community*, ISBN 978- 3-030-01842-9, Springer (D)

Ronchi, Alfredo M., (2010). The Patient's Perspective - empowerment or bewilderment eHealth: Background, Today's Implementation and Future Trends. Alan R. Shark, SylvianeToporkoff in eHealth - A global perspective. (pp. 181- 198), ISBN 978-1451540291, CreateSpace Independent Publishing Platform

Lei Zhang, Bingpeng Zhou, et al. (2020) Privacy-Preserving Contact Tracing and Public Risk Assessment Using Blockchain for COVID-19 Pandemic, DOI: 10.1109/IOTM.0001.2000078, IEEE

SOCIAL MEDIA, USE, MISUSE, ABUSE, REGULATION AND THE WAY FORWARD

- **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 impacts 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" [4 - Weiser 1991] phase, "users" are overlapping more and more with "citizens" [5 - Council of Europe 2001] and they consider technology and e-Services [6 – 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.This to do not consider smart wristwatches, Alexa, Nest and smart tv.

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[45]. This revolution was initiated by visionary researchers like Douglas Engelbart[46] and his "on-line System[47]" that is directly connected with "The Mother of All Demos", as retroactively termed its presentation at the IEEE on 9 December 1968, to do not forget his concept of a revolutionary device: the "mouse"; Butler Lampson, Charles P. Thacker, Robert W.

[45] 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".

[46] 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.

[47] Developed by Douglas Engelbart and Dustin Lindberg at SRI International.

Taylor and Alan C. Kay licensing in 1973 the Alto[48] computer and its object oriented interface ten years before Apple Macintosh[49]. In the 1980s Alan Kay, developing "Dynabook", introduced the concept of laptop computer[50].

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[51]" 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 [29 – UNESCO & WSIS], data ownership, privacy and more arose as well as the impact of cyber technology on society and economy.Risks

[48] Xerox Alto had a limited diffusion on the market, in the 1980s Xerox created Star a modified and cheaper follow-up of Alto.

[49] Steve Jobs understood the relevance of that revolutionary approach to computing and activated Lisa and later Macintosh projects.

[50]Llull, R. (2021). *Dynabook – Complete History of the Dynabook Computer*. [online] History-computer.com. Available at: https://history-computer.com/dynabook-complete-history-of-the-dynabook-computer/ [Accessed 8 Feb. 2021].

Sterling, B. (2012). *Alan Kay, "A Personal Computer for Children of All Ages," 1972*. [online] Wired. Available at: https://www.wired.com/2012/10/alan-kay-a-personal-computer-for-children-of-all-ages-1972/ [Accessed 8 Feb. 2021].

[51]The incredible capillary diffusion of APPs creating a real phenomenon: APPification

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" ovens, 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 marketoffering a completely new set of applications.

• Social Media: Opportunities and Threats

The idea to share something with someone else, a group of people, sometimes generates a sense of belonging to a "community". Memetics[52] [9 – Moritz 1990] used to consider this "something" as the "meme". A meme is a cognitive or behavioural pattern that can be transmitted from one individual to another one. Consider young people that wear clothes in an unconventional way or use signs and gestures that show that they belong to a particular community[53]. The basic mechanism is very simple; since the individual who transmitted the meme will continue to carry it; the transmission can be interpreted as a replication. A meme carrier, known as a replicator, is created when a copy of the meme is made in the memory of another individual. Replication or self-reproduction is the basis for the memetic life cycle. This leads to the spread of memes to more and more individuals, such that the meme acts as a replicator, in a similar way to the gene[54] [9 – Moritz 1990].

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[55], but communication is the key player in the creation of communities and due to this communities directly dealing with communication means are facilitated. In the early stages of computer intercommunication, apart from exchanging signals and data, a basic text messages service was implemented. Ancient timesharing computer systems had local "mail" services so its users could communicate. But the real power of "electronic" mail came true when mail could be distributed to distant computers and all the networked users could communicate[56]. Late in the 1980s the increasing use of bulletin board systems (BBS), file transfer protocol (FTP), Telnet and other communication tools such as Veronica and Gopher prepared the playground for the massive use of

[52] Moritz E (1990) Memetic science: I. General introduction. J Ideas 1:1-23

[53] Moritz E (1995) Metasystems, memes and cybernetic immortality. In: Heylighen F, Joslyn C,Turchin V (eds) The quantum of evolution: toward a theory of metasystem transitions. Gordonand Breach, New York (J Gen Evolut Spec Issue World Futures 45:155–171)

[54] Moritz E (1990) Memetic science: I. General introduction. J Ideas 1:1–23 // Dawkins R (1976) The selfish gene. Oxford University Press, New York

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

[56] The official launch of ARPANET was a large, very successful demonstration that was organised and presented by Robert Kahn in 1972 during the International Computer Communication Conference (ICCC). Early in the 1970 the French Institut de Recherche enlnformatique et enAutomatique (IRIA), nowadays INRIA, sponsored the creation of the first network based on packet switching the CYCLADES computer network defining the basis for TCP protocol (refer to Louis Pouzin). The first hot application appeared in March of that year courtesy of Ray Tomlinson: electronic mail. Tomlinson wrote the basic email message send and read software, which was intended to aid cooperation between the distributed research team working on the network project.

the Internet and the World Wide Web. Since the beginning of computer user'scommunication, a sense of community arose and a common feeling on behavioural rules was implemented.

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), Instagram ('10), SnapChat (11), Telegram (13), Signal (14), TikTok (16),... Social newspapers (e.g. YouReporter ('08), Bambuser ('14), and more, much more.

If the early stage of Internet communication was based on the so-called "netiquette", a kind of Galateo[57] 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 Sovereigntyexists 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, YouTube or even some thematic websites are not allowed. Here apart from political, ethical and philosophical issues may come to the fore the economic and financial aspect of entering that market adhering to the requested censorship or not[58].

It may happen even the reverse, entire countries or regions can be banned by platforms and applications as well as single groups or members of the social network community. Such restriction can be motivated by political or security reasons as it happens mainly for countries, counter culture, terroristic groups or criminal organisations. In recent times the option to "silence" community members have been extended even to political leaders[59], this raised the issue to regulate the sector of social platforms, the ownership of them even if private does not allow to operate without any responsibility[60] and duties.

The Internet Revolution gave a boost to data creation and dissemination, MAC addresses, web logs, and intentional or unintentional[61] applications to websites and services, and social platforms ignited the sedimentation of personal and many times sensitive information apparently lost in the cyberspace[62] [20, 21]. Very soon the first drawbacks come on stage: privacy infringements, stalking, hacking, cyber-crimes, stolen identities, darknet businesses and more[63] [22].

[57]Monsignor Giovanni Della Casa was a Florentine poet, writer on etiquette and society; Galateo overo de' costumi was inspired by GaleazzoFlorimonte, Bishop of Sessa.

[58] 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.

[59]It is well known the case of the US President Donald Trump (2020)

[60] A number of crimes including suicides perpetrated iue to "games", "imitation games" and "challenges" promoted by influencers.

[61] Time ago frequently associated to apparently different choices.

[62]Pimienta D (2014) Redefining digital divide around information. Literacy and linguistic diversity in a future context of access provision, internet and socio cultural transformations in information society. Interregional Library

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. Few years ago, a typical “laptop gadget” was the shutter to blind your laptop camera, even useful in the video-conference time, the pandemic period, to avoid unexpected intrusions on your private life. 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 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[64]” directed and interpreted by Orson Welles in 1941 outlined the relevant “power” of journalism[65], the movie “Network[66]” directed by Sydney Lumet outlined the power of television in 1996 and perhaps “The Net[67]” and “S.Y.N.A.P.S.E.[68]” together with “The Social Network[69]” started to outline the power of the Internet.

Cooperation Centre, Moscow. ISBN:978-5-91515- 061-3 // Prado D (2014) Towards a multilingual cyberspace, internet and socio-cultural transformations in information society. Interregional Library Cooperation Centre, Moscow. ISBN:978-5-91515- 061-3

[63] Bohn RE, Short JE (2009) How much information? 2009, Global Information Industry Center. University of California, San Diego

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

[65] 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.

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

[67] “The Net”, directed by Irwin Winkler (Columbia Pictures Industries Inc.—1995).

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

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

Computer biometrics is nowadays very advanced; so, starting from the Apple tools to recognize people appearing in your pictures once you gave the system two or three samples, a group of Russian developers released in recent times a powerful application, FindFace, that performs in real time the face recognition even of multiple persons and connects them to their V-Kontakte, the Russian version of Facebook, page. This enables users to take a picture with the smart phone on the street on in a disco and immediately discover the identity of the subjects. Is this a potential infringement of privacy? Is this a powerful tool for stalkers? Technological evolution does not have limits; it is already available for the professional market, e.g. law enforcement, a full version of FindFace offering far better performances without the limitation to V-Kontakte subscribers.

News and Media are key elements in the global society. CNN, BBC, Al Jazeera[70], Al Arabiya[71] are writing the history of the planet 24/7 and on the grassroots side YouReporter[72] and Twitter 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 a sequel of the movie "Wag the Dog[73]" 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.The evolution of on-line news due to the social web and the birth of "prosumers" did the rest. Twitter, YouTube, Facebook, Instagram and blogs represent a real revolution in the domain of news, this to do not consider the role played by the so-called "influencers".

As already stated, the Internet is much more a counter-power than a power; the common idea about the Internet is the network as a powerful tool of freedom and democracy. This is probably true but the opposite is even true, the misuse of the network and misinformation disseminated and empowered by the Internet and its powerful mechanism.Cyber IDs allow multiple IDs and potentially Dr Jekyll and Mr Hyde. We are flooded[74] by user-generated content (UGC) largely without any qualification and certification of the source. Many times, the drawback attributed to the amanuenses is affecting even web publishers: information and content is re-used and re-published adding or replicating errors and bugs. The short content production chain, sometimes even limited to a "one-stop shop", does not include an editor in chief or a supervisor; so far, the overall quality of prosumer content and information is quite low.
As an IBM top manager told recently on the occasion of the Global Forum: "*Do not trust in any information coming from unknown source.*"

[70] www.aljazeera.com/ [Accessed 8 Feb. 2021].

[71] www.alarabiya.net [Accessed 8 Feb. 2021].

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

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

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

- ## 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. This aspect may be crucial both in developing and developed countries because even “information” is “power”.

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[75]” 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 [21 – BBC], legal framework, security, even OSINT [18 – Central Intelligence Agency 2001] [19 - Central Intelligence Agency 2010]and more [20– Hock R. 2020].
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

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

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 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 [28 – 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 [24 – My Data] information is relatively new[76]. 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.

[76] Wsa-mobile.org. (2016). *World Summit Award Mobile - WSA-mobile | The World’s Best Mobile Contents*. [online] Available at: https://wsa-mobile.org/ [Accessed 8 Feb. 2021].

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” [23 - 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-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.

- **Internet “Prosumers” Initiative: My Data Belongs To Me**

Concerns about data ownership and potential re-use do not only pertain to inter- national institutions or governments; it is an issue coming even from the grass roots. In 2014 the World Summit Award (WSA) [24 – My Data 14], an organisation closely linked with WSIS grouping hundreds of “digital authors” coming from more than 170 countries around the world, launched “My data belongs to me”, an initiative through its global multi-stakeholder network, to push forward personal data ownership and big data issues at UN discussions. On the occasion of open discussions, such as the one held on the occasion of WSIS Forum 2014 in Geneva, the WSA invited participants to share views on issues with the current system of data use, the need for permissionbased access, and steps for further action. This initiative underlines the consciousness about the ownership of personal information too many times shared among social platforms and business services.

- **EU Data Protection Regulation And Personal Data Re-Use**

Updating and extending previous regulations[77] in 2016[78] the European Commission issued a data protection Directive [25 Protection - 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 [21 – 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 [29 – UNESCO-WSIS].

[77] Europa.eu. (2013). *Consolidated TEXT: 32002L0058 — EN — 19.12.2009*. [online] Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML [Accessed 8 Feb. 2021].

[78] 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.

- **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 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" [31 - 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[79].

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

[79] It is wise to recall and underline the difference between medical devices and wellness devices, the latter not strictly regulated with reference to data collection and use.

or free Wi-Fi connections asking for your identity, e.g. typing your mobile phone number to gain access to the Internet, so they can 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 [30 - 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 [27 – 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. In western countries 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[80] 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.

[80] Guardian staff reporter (2016). *French workers win legal right to avoid checking work email out-of-hours*. [online] the Guardian. Available at: https://www.theguardian.com/money/2016/dec/31/french-workers-win-legal-right-to-avoid-checking-work-email-out-of-hours [Accessed 8 Feb. 2021].

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[81] 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[82] 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 on March 28, 2017[83].This joint resolution nullifies the rule submitted by the Federal

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

[82] http://www.eleas.fr/expertises/gestion-des-tensions-au-travail/ [Accessed 8 Feb. 2021].

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

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."[84] [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" [17 – Brunton] is an application[85] 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[86].

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.

• GAIA X

A consortium of European partners created a proposal for the next generation of a data infrastructure for Europe: a secure, federated system that meets the highest standards of digital sovereignty while promoting innovation. GAIA-X is a project initiated by Europe for Europe. Its aim is to develop common requirements for a European data infrastructure. Therefore openness, transparency and the ability to connect to other European countries are central to GAIA-X. Representatives from seven European countries are currently involved in the project.

[84] GovTrack.us. (2021). *Summary of S.J.Res. 34 (115th): A joint resolution providing for congressional disapproval under chapter 8 of title 5, ... - GovTrack.us*. [online] Available at: https://www.govtrack.us/congress/bills/115/sjres34/summary#libraryofcongress [Accessed 8 Feb. 2021].

[85] 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".

[86] Makeinternetnoise.com. (2017). *Internet Noise*. [online] Available at: http://makeinternetnoise.com/index.html [Accessed 8 Feb. 2021].

- **Privacy And Security In The Cyber World, A Paramount**

One of the potential infringements of privacy is due to breaches in your personal device security (smart phone, tablet, etc). 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.*”

It is worth to clarify few concepts in the field of “security” and much more in the field of “cybersecurity”, the first one, as already stated, is that there is no “absolute” security. Second aspect is that security is always directly related to the specific risks, this involves risk analysis and the design of security measures addressing the specific risks. It is worth to understand the differencesamongsecurity, protection and risks; we a dealing with aspects strongly related each other something that appears well protected might be unsecure due to the high-risk environment.

Traditionally cybersecurity is ensured by secret codes or credentials many times the weakest part is due to humans, secret codes annotated close to the security check points, passwords easy to identify and a number of social engineering tricks make easy to break to code. For quite a long-time default password used both by software companies and system administrators were “password” or “admin”, to do not mention air carriers’ companies use the two letters ID of the company as the password to access their systems.

Today we face some new concerns, the use of social media 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 [6 - 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 [6 - 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!So, the connection with your social networks will follow you in a kind of “social-shell”.

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 [8 – 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 [5 - 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"[87] effect starting from social media and 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, the use or misuse of social media appears easy natural, no concerns about potential drawbacks. 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 and 2020)[88], a couple of workshops on the occasion of the WSIS Forum[89] (April 2019 and 2020), and IST Africa[90]

[87] Bad ambassador effect: drawbacks in the early phase of a new technology addressing people to do not further use that tchnology.

[88] 34987131 (2019). *CFF Cyber Future Dialogue Resolution and Spring 2019 Update*. [online] Issuu. Available at: https://issuu.com/cyberfuture/docs/2019_cyber_future_dialogue_resoluti [Accessed 8 Feb. 2021].

[89] Itu.int. (2019). *Highlights & Outcomes | WSIS Forum 2019*. [online] Available at: https://www.itu.int/net4/wsis/forum/2019/Home/Outcomes#documents [Accessed 8 Feb. 2021].

[90] Ist-africa.org. (2019). *IST-Africa*. [online] Available at: http://www.ist-africa.org/Conference2019/ [Accessed 8 Feb. 2021].

(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.

More in general Governments should invest in media information literacy [22 – 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[91] 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[92] from e-Government to e-Health [6 - Ronchi 2019]. 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.

• 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

[91] Polizia di Stato (2011). *YouPol.* [online] Google.com. Available at: https://play.google.com/store/apps/details?id=it.poliziadistato.youpol&hl=en&gl=US [Accessed 8 Feb. 2021].

[92] Ronchi Alfredo M. (2019), e-Services: Toward a New Model of (Inter)active Community, ISBN 978-3-030-01841-2, Springer

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

There are two main keywords this year: pandemic and resilience. Social media played a key role on the occasion of the pandemic both ensuring, sometimes, the only connection between citizens, especially elderly and infected, and their families and friends. Of course, this is even true and relevant to ensure social experiences among citizens, the creativity expressed in such a situation is incredibly relevant, virtual guide to museums, virtual jam session and concerts virtually joining on line musicians, cooking and wellness courses. All these social activities boosted the resilience of society in a situation that many times forced people to stay at home for long period of time and broadcasted a feeling of insecurity and uncertainly about the future.
Posing the focus on education the crisis generated by the pandemic, but we could extend the discussion even to natural or human disasters, warfare, criminal events and more, impacted young generations lowering the effectiveness of courses and training. In the educational environment similar situations will impact pupils and young people from kindergarten to university including hospitalised and disabled guys.

Last but not less relevant, education sector faced some problems far before the pandemic due to the existent gap between traditional courses and new generations interests and abilities.Generally speaking the response of Universities to the pandemic was quite good and the switch to distance learning including exams and degree was prompt and generalised. Similar but less sophisticated solutions are in use in middle schools and colleges, no specific solutions both for kindergartens and some primary schools.

Now is the time to think about the future organization of the education system by taking advantage from the experience gained and adopting the best solutions to achieve a resilient education.What do we mean as resilient education system? A system that, in the event of a crisis, will ensure 100% of the performance or a sufficient level of “education continuity”? and what about infrastructures ? Think about a general long-lasting electricity black out, as it may happen in case of natural disasters, or simply a hacking attack to the network infrastructure, how to ensure “education continuity”? Probably a similar situation is very difficult to be solved.

Apart from these extreme circumstances that, by the way, have been solved in some cases. One of the aspects to be carefully considered is an affordable and easy access to the network infrastructures both wired or wireless. Strictly connected to this we find, in general, a significant market penetration of ICT due to smart phones, tablets, and laptops. Of course, a good network infrastructure and diffuse computational resources are not enough, a key role is played by human factors, mentors' literacy in digital-media (we assume a proper skill in pedagogy and didactics) as well as digital awareness of students. Lastly but not least, availability of quality content and easy access to professional digital libraries.We must not forget the key role played by social media, they were already a powerful tool among students both as information providers and social life active means, but on the occasion of the lockdown they became much more relevant to empower cooperative learning.Anyway, as a positive follow-up of the present crisis we can envisage different benefits: first of all, the acceleration of the switch to distant learning on the way to an improved resilience of the educational system but even an empowered knowledge transmission and acquisition from the end of the crisis onward. Distant learning is nowadays de-facto based on digital technology, typical approach, was and still is, to port to digital means traditional formats based on texts, still images, sometimes video clips. These applications are suitable for both live lectures or on-demand lectures, of course on-demand lectures offer a limited interaction mainly based on Q&A. Anyway, I would like to point out the relevance of video recording lectures, this feature enables students to attend courses even if they are in a different time zone.

- ## 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 [32 – 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 Airbnb 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 tightly connected with the social-side is the use of “crowds” to provide data and services not foreseeable before the Internet; simply think about APPs like Tripadvisor[93] 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[94], crowds and platforms. This approach enabled innovative solutions like project funding or collaborative film production[95]. In the global society crowds are playing the role of “public services” [32 - 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 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

[93] Tripadvisor. (2021). *Tripadvisor: Read Reviews, Compare Prices & Book*. [online] Available at: https://www.tripadvisor.com/ [Accessed 8 Feb. 2021].

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

[95] HugeDomains. (2021). *WreckAMovie.com is for sale | HugeDomains*. [online] Available at: https://www.hugedomains.com/domain_profile.cfm?d=wreckamovie&e=com [Accessed 8 Feb. 2021].

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

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

[6.] Ronchi Alfredo M. (2019), e-Services: Toward a New Model of (Inter)active Community, ISBN 978-3-030-01841-2, Springer

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

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

[9.] Moritz E (1990) Memetic science: I. General introduction. J Ideas 1:1-23

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

[17.] 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

[18.] 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

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

[20.] Hock Randolph, Internet Tools and Resources for Open Source Intelligence – 2020 - OSINT, http://www.onstrat.com/osint/

[21.] 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/

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

[23.] Mayer-Schönberger Viktor, Delete: The Virtue of Forgetting in the Digital Age, ISBN-13: 978-0691138619, Princeton University Press 2009

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

[25.] Protection of personal data in EU, http://ec.europa.eu/justice/data-protection/

[26.] 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

[27.] Thompson Herbert H., "How I Stole Someone's Identity", Scientific American, August 2008

[28.] UK Government Service Design Manual: Open Data, https://www.gov.uk/service-manual/technology/open-data.html

[29.] 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/

[30.] Universal Declaration of Human Rights, http://www.un.org/en/universal-declaration-human-rights/

[31.] Warsaw Declaration, http://www.coe.int/t/dcr/summit/20050517_decl_varsovie_EN.asp, Council of Europe Warsaw Summit May 2005

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

CYBER RESILIENCE, CYBER DISASTER MANAGEMENT - THE WAY FORWARD

- **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. 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".

Keywords: *Cyber Resilience, Natural Human Disasters, Terrorism, Cybersecurity, Cyber Attacks, Culture of cybersecurity*

- **Setting The Scene**

Cyber technology is pervasive and its key role is growing up every day, citizens consider cyber technology as a commodity. 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. Extremely user-friendly devices are nowadays used by formerly digital divided citizens having no idea about potential drawbacks. As a side effect of globalisation and massive cyber services the number of crimes both perpetrated at local and global level is growing up. The discontinuity ignited by cyber technology and its pervasiveness created the fundamentals for a completely new scenario where the malicious use of digital technologies is becoming a new business opportunity not only as a direct mean to steal "assets" and take control of smart objects but even under the format of "cyber-crime as a service", at the same time terrorists found in cyber technology the best mean both to run their activity and to enrol new "adepts".

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[96]. 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[97]. This situation illustrates the problem of lack of preparedness organisations face in defending effectively against cyberattacks.

- **Cyber Resilience?**

I won't just deal with cyber-attacks ...Nowadays "resilience" is one of the most used keywords. There are a number of definitions of resilience (accordingly with Cambridge English Dictionary):

[96] Keysight (2018). *Network Visibility and Network Test Products*. [online] Keysight. Available at: https://www.keysight.com/in/en/cmp/2020/network-visibility-network-test.html [Accessed 8 Feb. 2021].

[97] Verizon Enterprise. (2021). *Business Insights and Resources*. [online] Available at: https://enterprise.verizon.com/resources/?page=1 [Accessed 8 Feb. 2021].

“*The capacity to recover quickly from difficulties; toughness*”
“*The ability of a substance to return to its usual shape after being bent, stretched, or pressed*”

Nowadays, in the pandemic time, as much important as the physical meaning are the phycological aspects:
“*The ability to be happy, successful, etc. again after something difficult or bad has happened*”;
“*Resilience is the psychological quality that allows some people to be knocked down by the adversities of life and come back at least as strong as before.*”ICT can play a relevant role in offering a second chance to come back.

The term resilience has as much definitions as the sectors involved, if we consider the cyber sector, cyber resilience means “*the ability to prepare for, respond to and recover from cyber-attacks*”.
Even something that is perceived far from the usual idea of resilience, in the specific domain of software interfaces resilience that can be summarized as: *the system should provide some resilience to user errors and allow the user to recover from errors. This might include an “undo” facility, confirmation of destructive actions, ‘soft’ deletes, etc.*

- **Cyber Disaster Management**

This term is usually tightly linked with cybersecurity and cyber-attacks and express the ability to recover after a cyber disaster,a relevant cybersecurity breach that caused one or more of the typical lockdowns of cyber activities (Denial Of Service, network communication breakdown, general malfunctions, etc.). We must not forget the human factor in such situations, often the weakest link in the chain.

Typical examples were WannaCry, Petya that we all know.Through the time a number of cyber disasters have been recorded: loss of US Votes, loss of “citizens” on the occasion of census, loss of sensitive data.

- **Not only Cyber Attacks**

Cyber resilience in case of cyber-attacks is an interesting topic involving specific infrastructures, plans (governance), risk assessment and mitigation actions, CSIRT, cyber ranges exercises and more, nevertheless there are additional causes of cyber disasters.

Dealing with cyber resilience and cyber disasters it is wise to extend the possible causes to natural and human disasters, terroristic attacks, technological malfunctions and design problems, intrinsic digital fragility and more.

Some years ago, on the occasion of the WSIS Forum His E. Mr Yasuo Sakamoto, Vice-Minister for Policy Coordination, Ministry of Internal Affairs and Communications (Japan), said: on the occasion of natural disasters ICT is the lifeblood to ensure citizen’s safety; and, on the same occasion, Mr. Sunil Bahadur Malla, SecretaryMinistry of Information and Communications in Nepal, told us on the occasion of his contribution: ICTs were crucial in recovering the territory during and after the recent earthquake.
That’s for sure true, the point is to ensure cyber services continuity even in the event of a disaster.This means that in addition to preventive measures addressed to face any kind of hacking attack we must put in place solutions to ensure “business continuity” even in case of other causes.

Cyber resilience in an event of disaster or terroristic attack involves an a priori identification of critical infrastructures and a specific risk analysis identifying all the potential vulnerabilities and combination of vulnerabilities. Once we have a list of specific vulnerabilities for each “node” we match them with local dangers considering both the pipeline of vulnerabilities/dangers and the cross action of different vulnerabilities/dangers on different interconnected nodes (e.g. power supply, net devices, fibreoptic,etc). to map the overall risk.

Specific solutions have been studied to overcome possible problems in case of disasters including satellite connections, deployment of emergency network nodes both wired and wireless, switchboards connecting different digital phone lines (landlines, 4/5G, UHF, CB, OM, air band, Tetra).Of course, as a key “partner” of technical solutions we must put in place a strong flexible organisation on the human side.

The recent pandemic, for instance, was a significant stress test for network infrastructure and data servers, typical approaches to the design of the network infrastructure and data servers were not sized for a mass access to the infrastructure and pervasive use of it generating huge volumes of data transfer both in and out.

The extended use of lockdown boosted the access to on-line services ranging from government offices to on-line shops to buy goods and receive food and drinks at home including a massive use of music and video streaming throughout the whole day.

An additional must is to ensure as much as possible business continuity enabling, when applicable, on-line working sessions, many times this requires video conferencing tools to enable many to many interactions.

All these activities require an adequate network infrastructure ensuring enough bandwidth ideally to all the internet users connected in audio-video streaming, a similar situation it is not foreseen by the actual technical specification so to do not collapse the network the bandwidth must be carefully used,for instance, switching off video connections on conferencing platforms.

Similar overcrowding problems can affect interaction with e-services, for instance, e-Gov services resulting in a Denial Of Service (DOS) many times due to the inadequate servers.

These problems are usually due to architecture design specifications not to technological limits; a number of global platforms having an adequate network connection and server farm use to operate properly even in case of global “Black Fridays”.

Drawing some conclusions, cyber resilience is already a must since we “moved” in the cyberspace a number of critical services. Resilience under cyber-attacks is a paramount, it is a “glocal” problem to be solved both at global level because national cybersovereignty does not lock cyber frontiers at the same time on local level a number of well-defined infrastructures and actions must be activates, a tight cooperation among states must operate.

Cyber resilience in an event of disaster or terroristic attack involves a far wider range of protection measures, as already described, an a priori identification of critical infrastructures and a specific risk analysis identifying all the potential vulnerabilities and combination of vulnerabilities.
Considering the trend toward smart-home / cities / energy / mobility the risks due to the merge of cyber technology controlling a number of infrastructures is far higher than in the past.

- **Cyber Ranges**

A Cyber Range provides a simulated environment to conduct tests and rerun exercises to enhance cyber defence technologies and skills of cyber defence professionals, in addition their simulation features will offer a global situational awareness on the risk-chain and related attack surfaces.

These platforms provide tools to test the resilience of networks and systems by exposing them to realistic nation-state cyber threats in a secure facility with the latest tools, techniques and malware, this facilitate the testing of critical technologies with enhanced agility, flexibility and scalability, it helps to strengthen the stability, security and performance of cyber infrastructures and IT systems used by governments and private organisations.

These platforms enable to conduct force-on-force cyber games/exercises, cyber flags; provide an engineering 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 cyber ranges will offer to cyber professionals the opportunity to develop the skills facing a relevant number of cyber-attacks and their overall impact. A cyber range allows organizations to learn and practice with the latest techniques in cyber protection, practitioners will be able create and test different strategies customizing sophisticated testing protocols in short time. As a follow up of the training session practitioners, after the result of their countermeasures may receive suggestions on the best practice in the specific situation as identified by the platform or retrieved in the knowledge base.

Main outcomes obtained thanks to cyber ranges are: improved situational awareness of cyber warfare scenarios, rapid identification of zero-day vulnerabilities, environment for the development of countermeasures, training environment for practitioners.

Communication networks can deeply influence a relevant number of services and the combined effect of such effects may led to serious and sometimes unpredictable consequences.

There is a need to develop an international/global Cyber Range Network to share knowledge and information enabling an improved approach to countermeasures and tactics. Cyber Ranges are designed to easily create virtual environments devoted to cyberwarfare training and cybertechnology development. Such platforms, in line with typical simulator’s features, are fed by real case study and create a knowledge base of cyber threats, related extended effects and mitigation/counteractions. A specific useful feature to be incorporated is the identification of the zero-day vulnerabilities in order to reduce or eliminate the Window of Vulnerability (WoV) and identify main attack vectors.

- **Europeans Cyber laws**

Since 1996 a number of countries decided to enact cyber laws. On 23 November 2001 the Council of Europe issued the European Treaty Series No. 185 entitled “Convention on cybercrime”. Some of the paragraphs are devoted to: Illegal Access, Illegal interception, Data interference, System interference, Misuse of devices, Computer-related forgery, Computer-related fraud, Offences related to child pornography, Offences related to infringements of copyright and related rights, Attempt and aiding or abetting.

European societies are increasingly dependent on electronic networks and information systems. The European Commission considered, since the announcement of the "Information Society" model, cybersecurity as an enabling tile of such a model, protecting from criminal activity what threatens citizens, businesses, governments and critical infrastructures alike: cybercrime.

Cybercrime is borderless and could be ubiquitous, committed even thanks to a mobile phone. In order to combat cybercrime a number of actions are required: legislation, specific law enforcement units, active and passive protection, education – a "culture" of cybersecurity and more. The European Union has implemented legislation and supported operational cooperation, as part of the EU Cybersecurity Strategy released in 2013.

Later on, in 2017 the Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" builds on and further develops the EU Cybersecurity Strategy. As outlined in the Communication (2017), the European Commission continues to work on effective EU cyber deterrence, by, among other actions, facilitating cross-border access to electronic evidence for criminal investigations. If we focus on evidences it is evident that "traditional" physical evidences may be collected in a proper way and safely stored in warehouses; digital evidences are quite different; they are often distributed on line and hosted by different organisations and servers, in addition they are "fragile" and may disappear[98] along with elapsed time. A specific problem is due to privacy issues and trust relations between IT (hard and soft) companies and customers. As an example, let's consider smart phones or social media companies; they protect the privacy of their own customers so many times, they do not provide access to specific potential criminal content to law enforcement agencies. Here comes the eternal fight between security levels implemented by companies (telecom, social media, etc.) and governments; governments must be few steps forward and have potential access to private information to keep restricted information undisclosed and ensure citizens' safety and security.

As a specific European law enforcement agency fighting cyber-crimes the European Commission has played a key role in the development of European Cybercrime Centre (EC3[99]), which started operations in January 2013. EC3 is part of Europol[100] and "acts as the focal point in the fight against cybercrime in the Union, pooling European cybercrime expertise to support Member States' cybercrime investigations and providing a collective voice of European cybercrime investigators across law enforcement and the judiciary."

Back to national approach to cyber laws, we will consider the Chinese approach to cyber technology introducing the "Cyber Sovereignty" approach. A similar overall approach is shared with India[101] as well. The Indian Parliament enacted the Information Technology Act 2000 (ITA-2000) on October 2000; it was the first law in India dealing with cybercrime and electronic

[98] Simplyconsiderdigitalpreservationaspects.

[99] Europol. (2020). *European Cybercrime Centre - EC3*. [online] Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [Accessed 8 Feb. 2021].

[100] Europol - European Union's law enforcement agency. (2020). *Home*. [online] Available at: https://www.europol.europa.eu/ [Accessed 8 Feb. 2021].

[101] WSIS Forum 2017 | Information and Knowledge Societies for SDGs (2017). *WSIS Forum 2017*. [online] WSIS Forum 2017. Available at: https://www.itu.int/net4/wsis/forum/2017/Agenda/Session/254 [Accessed 8 Feb. 2021].

commerce. The reference model of ITA-2000 is the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model).

On July 2017 The Times of India published an article entitled “One cybercrime in India every 10 minutes”; according to the Indian Computer Emergency Response Team, 27,482 cases of cybercrime were reported from January to June 2017. These include phishing, scanning or probing, site intrusions, defacements, virus or malicious code, ransomware and denial-of-service attacks. In order to favour the report on cyber-crimes, on April 2017, the Ministry of Electronics & Information Technology (MEITY) published in the International Journal of Science Technology and Management a specific article entitled “How to report cyber-crimes in Indian territory”. New Delhi hosts since 2014 the International Conference on Cyber Law, Cyber Crime & Cyber Security, a key international event organised and chaired by Pavan Duggal, Advocate at the Supreme Court of India, world-class expert in this field.

Estonia has invested time and resources to develop a sound regulatory framework in the field of cyber. Germany decided to focus mainly on critical infrastructures protection while Russia promoted the idea that Russian data must reside on the Russian territory. To conclude this excursus on cyber laws we may include two more countries like Bahrain and Zimbabwe; they both developed specific cyber laws. On 12 February 2015 Bahrain enacted the new cybercrime law; it seeks to reduce crimes by establishing penalties to protect public interest. Under the law is considered a criminal: anyone who gets illegal access to an IT system or part of it, anyone threatening to cause damage for personal gains, anyone convicted of entering, damaging, disrupting, cancelling, deleting, destroying, changing, modifying, distorting or concealing IT device data concerning any government body, anyone convicted of embezzlement of funds, receiving favours for oneself or others, forging documents. For online distribution of pornographic material, the sentence is doubled if the pornographic material targets children.

An additional short list of what kinds of activities are considered computer crimes may include but it is not limited to:

- Improperly accessing a computer, system, or network;
- Modifying, damaging, using, disclosing, copying, or taking programs or data;
- Introducing a virus or other contaminant into a computer system;
- Using a computer in a scheme to defraud;
- Interfering with someone else’s computer access or use;
- Using encryption in aid of a crime;
- Falsifying email source information; and
- Stealing an information service from a provider.

While bullying, sexual harassment, and child pornography are long-standing crimes and societal problems, the Internet and social network sites have introduced a whole new arena for predators to practice their trade. These last three crimes are expanding due to the Internet; so far, they represent a typical issue for cyber-laws.

A synthetic description of Cyberbullying is: aggressive harassment that occurs using electronic technology, including cell phones, tablets, and computers using social media sites and chat sites. Cyberbullying includes the sending of unwanted, abusive text messages, photographs, personal information, defamatory and libellous allegations and rumours, and the creation of fake profiles intended to harm victims. Child pornographers and child molesters have unfortunately found the Internet to be a useful tool to prey on children as well.

In the United States the Department of Justice has a special task force devoted to catching these predators, and if your child has been targeted, you should contact law enforcement right away. The Department of Justice has published a Citizen's Guide to Child Pornography to outline the laws and your remedies. Victims should report the crime to parents, network providers, schools, and law enforcement. Hate crimes are the most heinous of the various cyberbullying crimes, and they carry their own distinct set of penalties in most states, including additional jail time and sometimes mandatory prison time if connected to another felony. Hate crimes also pique the interest of the FBI, which prosecutes hate crimes and maintains statistics on the proliferation of hate crimes and other forms of civilian terrorism. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, published by Cambridge University Press, is the most comprehensive analysis of how existing international law applies to cyber operations. The drafting of the Tallinn Manual 2.0 was facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence[102].

- **Closing remarks**

To conclude let's recap the key points outlined within this paper, cyber technology is nowadays pervasive and at different level present all-over the globe, digital data creation in the different formats (text, graphic, audio, video, etc.) are growing exponentially,as a consequence of the tight relation between cyber technology and our everyday life. A significant investment in digital literacy starting from primary schools is a paramount, young generations are exposed to many threats because of their intensive use of technologies without and adequate knowledge of potential drawbacks and risks. The capillary presence of "extreme" user friendly cyber-devices enabled "digital divided" citizens, not aware about potential risks, to access the cyber-world.

Cyber security together with cyber laws, when necessary, are a pre-condition to safely exploit e-Services. E-Government, e-Business or e-Health are in danger and may act as bad ambassadors if cyber security is not ensured technically and legally.

At global level the malicious use of cyber "troops" may design a credible warfare scenario reserving traditional warfare scenarios to minor local conflicts still based on conventional weapons. In such an actual and future scenario on the defence side it seems a must to maximise the potential of cyber defence, one of the opportunities is offered by Cyber Ranges both to assess cyber infrastructures resilience, test new countermeasures, launch force to force and cyber flags exercises and last but not the least active training of practitioners.

Apart from pure cyber defence there are some other relevant actions to intercept potentially dangerous trends, future threats and more. One of the main approaches to act "ex-ante" thanks to the pervasive role of digital technologies and related data exchange is the advanced in-depth analysis of big data streams, social media, open source intelligence, socio-economic and geo-political factors, human factors, potential influencers, crowd sourcing, and remote sensing. This task will be carried out thanks to enhanced data analytics, machine learning and artificial intelligence.

In conclusion we are already in the arena of cyber "warfare" where troops, tanks, ICBM, choppers are the "cleverest" bit and bytes assaulting or defending our resources and life style. To extremely simplify the basic scenario, it is not conventional war, it is not guerrilla warfare, it is not terrorism

[102] Ccdcoe.org. (2021). *CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.* [online] Available at: https://ccdcoe.org/ [Accessed 8 Feb. 2021].

where one single man can create relevant damages somewhere, it is a new treat in which one single man located anywhere can create relevant damages globally.

- **Bibliography**

1) Babel C (2015) Tackling privacy concerns is key to expanding the internet of things, Wired Innovation Insights, Feb 2015
2) Critical Link is building a network of volunteer emergency First Responders, who are dispatched through SMS and Mobile alert to save lives when people are injured in Dhaka. https://play.google.com/store/apps/details?id1⁄4com.ionicframework.critical ink453552
3) Damico Tony M (2009) A brief history of cryptography. Inq J 1(11): 1/1, 2015 Student Pulse. All rights reserved. ISSN: 2153-5760
4) Diffie W, Hellman ME (1976) New directions in cryptography. IEEE Trans Inf Theory 22 (6):644–654
5) Duggal P (2018) Cyber Law 3.0, LexisNexis, Gurgaon, India, ISBN 978-81-3125-366-3
6) European Commission (2017) Resilience, Deterrence and Defence: building strong cyber-security for the EU, JOIN (2017) 450 final
7) Fyffe S, Abate T (2016) Stanford cryptography pioneers Whitfield Diffie and Martin Hellman win ACM 2015 A.M. Turing Award, Stanford News Service, Stanford University, Stanford, CA
8) Grillo (Cricket) – Grillo’s alerts will tell you when the earthquake will arrive and how strong it will feel where you are. http://grillo.io
9) High Representative of the European Union for Foreign Affairs and Security Policy (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final
10) Kahn D (1997) The Codebreakers: the story of secret writing. Scribner, New York. ISBN:978-1-439-10355-5
11) Milanov E (2009) The RSA algorithm, accelerated (honors) advanced calculus. University of Washington, Seattle
12) NATO Cooperative Cyber Defence Centre of Excellence (2017) Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press
13) Ompall, Pandey T, Alam B (2017) How to report cyber crimes in Indian territory. Int J Sci TechnolManag 6(04), April 2017, ISSN 2394-1537
14) 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
15) Ronchi Alfredo M., (2019), e-Citizens: Toward a New Model of (Inter)active Citizenry , ISBN 978-3-030-00746-1, Springer (D)
16) Ronchi Alfredo M., WSIS Forum 2015, High Policy Statements. https://www.itu.int/net4/wsis/forum/ 2015/Content/doc/outcomes/Policy_Statements_Booklet_WSIS2015.pdf
17) Ronchi Alfredo M., Duggal P et al, WSIS Forum 2016 Outcomes. https://www.itu.int/net4/wsis/forum/ 2016/Outcomes/
18) Ronchi Alfredo M., (2019), e-Democracy: Toward a New Model of (Inter)active Society, ISBN 978-3-030-01596-1, Springer (D)
19) Ronchi Alfredo M., (2019), e-Services: Toward a New Model of (Inter)active Community, ISBN 978-3-030-01842-9, Springer (D)
20) 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
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),, TAS: Trust Assessment System, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018

23) Ronchi Alfredo M., (2018), Hybrid treats: defence line from the grassroots, NATO STO Issue no. 3: Defence Technology Foresight, Bulgarian Defence Institute, 2 Prf. TsvetanLazarovblvd. Sofia, Bulgaria

24) Ronchi Alfredo M., (2018), High-level Track Facilitators (HLTFs), WSIS Forum 2018: High-Level Track Outcomes and Executive Brief, ISBN 978-92-61-25171-0, pag. 3,6 © ITU, International Telecommunication Union ITU, Geneva, CH

25) Ronchi Alfredo M., (2018), . . .1984 won't be like "1984"?, ISBN 978-5-91515-068-9, Interregional Library Cooperation Centre, Moscow

26) Ronchi Alfredo M., (2018), Thematic Workshop: ICTs for Safety, Security and Disaster Recovery, ISBN 978-92-61-25151-2, International Telecommunication Union ITU, Geneva (CH)

27) SAS report on The Internet of Things. http://www.sas.com/it_it/offers/ebook/iot-visualise-the-impact/index.html

28) Thawte (2013) History of cryptography, an easy to understand history of cryptography. Thawte

29) Thiesmeier L, Capture and readiness of slow-onset disaster information in Southeast Asia. https://www.itu.int/net4/wsis/forum/2016/Content/AgendaFiles/ document/7ea0c767-3a4b-40fe-8a30abd09b80c666/5_THIESMEYER_WORKSHOP_172.pdf

30) UNESCO (2014) Human development report 2014. Sustaining human progress: reducing vulnerabilities and building resilience

31) Virgo – Safety device for the protection of operators working in risky environment. http://www.intellitronika.com/virgo/

DIGITAL TRANSFORMATION – NEED OF TODAY'S TIME

- **Abstract**

Digital Transformation is one of the recurring buzzwords, starting from the early experiences carried out by forerunners the document outlines the role of platforms and the impact of them on society and occupation. Information as outlined far in advance by Bill Gates is the new wealth, how much information you access including personal data too often disclosed by users without knowledge about the potential drawbacks. Social media, IoT, CCTV, Open Data: is privacy evaporating? What about the impact of DT on government and education? Not only positive effects of this transformation, who is leading this process, where are we going?

Keywords: *Digital Transformation, Data Ownership, Privacy, Ethics, Cybersecurity, Culture of cybersecurity*

- **The Recurring Buzzword**

Nowadays there is a recurring buzzword:Digital Transformation (DX or DT) – it is an opportunity or a nightmare? The pandemic strengthened this trend, digital transformation will help to mitigate the effects of the crisis,improve resilience. "Resilience", by the way, another recurring term in the pandemic time.We all agree on the meaning of the term "transformation" but "Digital"has different meanings.Jim Swanson, CIO of Johnson & Johnson says "Digital*is a loaded word that means many things to many people*".

"*Say 'digital'to persons and they think of going paperless; another might think of data analytics and artificial intelligence; another might picture Agile teams; and yet another might think of open-plan offices*".A comprehensive definition of the term Digital transformation should be the integration of digitaltechnology into all areas of activity, from business to public sector, fundamentally changing how we operate and deliver value to customers or citizens.

- **The "Brave"Forerunners**

This paper will not consider the early stages of computer-based archives and accounting systems, as a legacy of that period of time we will mainly outline the difficulties and, some time, frictions encountered in the cooperation between humans and computers. We must remember that humans that times were skilled computer scientists playing the role of interfaces with employs.

To better introduce digital transformation, as we consider it nowadays, a first step was experienced by industries integrating digital technology mainly in the initial part of the value chain, from design to production and testing phases, later on, in factory automation, integrated management systems up to robotized warehouses and delivery systems.

The adoption of digital technology represented a true competitive advantage, literally "*Competitive advantage refers to factors that allow a company to produce goods or services better or more cheaply than its competitors. These factors allow the productive entity to generate more sales or superior margins compared to its market competitors.*"

Computer aided design systems allowed to speed up the design process, bettering the quality of the product through the opportunity to re-design and fine tune of the product in a fraction of time.The ability of computers to perform calculations enabled the "revolutionary" switch from empirical design methods to accurate mathematical dimensioning, sometimes adding even some best practice. Automated laboratories and test facilities, many times designed ad hoc from scratch, allowed to improve the performances and quality of the products or to acquire reliable information from testing machinery. Of course, these “transformations” were not “zero cost” for the companies, they needed to rethink the workflow, train personnel and more.

- **Impact On The Society**

Nowadays digital transformation impacts the whole society. It'sa cultural change that requires organizations and even citizens to continually challenge the status quo, experiment, and get comfortable with failure.Furthermore,on the citizens’ side, even and more significantly, it is required the willingness to “go digital” even if sometimes this choice become a“must” to do not be “cut off”. It is evident that digital transformation it is not a process “one size fits all”, each specific sector and even activity requires aparticularapproach and custom solution; this starting from the three main branches: citizens, companies, public administrations.

Because digital transformation will look different for every company, it can be hard to pinpoint a definition that applies to all. Sometimes this means walking away from long-standing business processes that companies were built upon in favour of relatively new practices that are still being defined.In such a situation the “trial and error[103]” finding by continues improvements the optimal solution is the practical approach.

Furthermore, everyone experienced in “ICT based innovation” knows that “It is not only a matter of technology”. Human factors are an essential tile of the whole process as well as a re-thinking of the whole organisation and process. We must keep humans in the loop and carefully consider the social and economic impact due to digital transition.

One of the potential benefits considered in the early phase of digital transformation was the unique opportunity to pour in the software procedures some knowledge about methodologies and procedures. Methodologies, or better, know-how accumulated in years and years of diligent activity traying to bridge the generational gap, this in addition to traditional coaching.

A different approach was generally used dealing with procedures, procedures must be reconsidered from scratch making “tabula rasa”. This mainly because procedures are, very often, the result of a “stratification” of layers of “reference points” included in the pipeline; this reshaping many times causes some friction due to the loss of some “power-nodes” within the organisation.The design phase must carefully reconsider one by one the “steps” checking the function of each of them within a well-defined rationale framework. The benefits using a platform is to guarantee the optimised workflow and offer to the citizens the opportunity check the progress of the process and related timing.

- **The Power Of Platforms**

Change in technology and user profiles cannot avoid impacting the market. The market is evolving in a very significant way. One of the first effects was the transition from the purchase of plastic boxes on the shelves containing DVDs plus printed user manuals to the on-line purchase and download of applications with pdf or eBook manuals. The idea to buy something “immaterial” on line transferring the right to use in an immaterial way is now largely accepted by the market.

[103]“a way of achieving an aim or solving a problem by trying a number of different methods and learning from the mistakes that you make” – Cambridge Dictionary

Reshaping, in an IPR/Biz compliant version, NAPSTER concept, iTunes, as a kind of rule breaker, promoted this approach in the field of the on-line music market many[104] years ago. Amazon followed a different path starting from the idea to sell on-line books in paper format, a kind of e-mall devoted to books but the real turning point was to extend the e-mall to almost every good overtaking eBay that was originally opening that market mainly on pre-owned items.

The diffusion of mobile position-aware devicescan be considered a kind of third digital revolution after the first transition from mainframes to PCs and, in the middle of 1990s, the second one thanks to the popularisation of the Internet under the motto "Where do you want to go today?[105]". At the same time, we witnessed a significant shift from few expensive software solutions to many "tiny" and cheap APPs.

The consumer software market changed getting closer to the music market. A short list of main changes is:

- Location-aware devices enabled a complete new set of services;
- Social media is pervasive and each new application that enables an active participation to cyber life is welcome (e.g. Snapchat[106], Tik Tok);
- People are looking for the Top 10 Apps;
- The consumption of Apps is continuous;
- Voice interfaces in natural language are gaining more and more success;
- The market model is now based on low costs/big numbers;
- The IPR management is evolving in order to self-adapt to the new trends;
- Data are migrating from local storage to clouds;
- Crowdsourcing offer a new paradigm in software development and services;
- Open and big data open a new frontier to added value services;
- The most popular applications are embedded as components of the Internet browsers;
- The new generation of "makers" is entering the market
- Digital media are evolving ... enhanced reality and artificial intelligence are back, etc., etc.

This happened after a long period of time, software developers were mainly cut out from the market and the necessary skills and efforts to develop applications were relevant (hundreds thousand code-lines).

This is in some way related to the interesting re-opening of the software market to single and small groups of software developers due to the availability of new successful development platforms to be "populated" by applications and the advantage of the new software market model based on online distribution and support. The last aspect has relevant effects on the software industry because it bridges the gap between micro and small software enterprises and medium and big companies, both offering a set of very well-known e-Commerce platforms and creating business opportunities for compact and well-focused applications. This may recall the dilemma between multipurpose devices, many things at an average level, or ad hoc devices, few things in the best way. Many years ago, "many" of course in the ICT time scale, a "guru" in the field of interaction design, Donald Norman,

[104] Many years in the ICT time scale of course!

[105] Microsoft Windows 95 advertising campaign, was launched in November 1994 through the advertising agency Wieden+Kennedy

[106] Snapchat.com. (2021). *Snapchat - The fastest way to share a moment!* [online] Available at: https://www.snapchat.com/ [Accessed 8 Feb. 2021].

proposed his own solution to this problem creating the iPod. Apps in general used to follow this last approach; you may need many single apps in order to accomplish a number of different tasks.

We are in the age of “platforms”, platforms make the difference. Platforms are the real “silver bullet” that created major 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 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 Airbnb or Uber but the list is almost endless. We all know the drawbacks created, and already evident, by some of these platforms, for instance, a number of local governments posed some limitations to Airbnb in order to avoid the risk to reduce the number of residents in some cultural cities or to ensure the opportunity to find available apartments to be long term rented.

This is not a full description of the power of platforms, apart from the transformation of the market there is the full control of social media and on-line digital communication, on one side these technologies are nowadays pervasive and everyday commodities on the other side due to the lack of legislation private tycoons have the full power to disconnect, emarginate, disable end users and even Governments or entire countries. Due to the increasing key role played by cyber technology and platforms there is a clear need to create and establish a global legal framework to regulate this sector, even if such global companies are private organisations they cannot rule the market without constraints.

A relevant part of digital transformation relies on platforms and standards, these aspects are directly linked with the “owners” of such platforms and standards, this can be considered a kind of monopoly not yet regulated, a kind of grey zone, so in the digital transition there is a potential risk to fall under control of few key players.

- **DT Impact On Occupation**

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, this to do not consider the fiscal benefits they usually enjoy compared with the traditional retail system.

This new model led to positively evaluate and size on the market companies having a relevantnumber of “customers” paying zero money to the company, this is mainly valid for services not based on a triangular market model service/user/advertisement. This is part of the new “economy”, Mc Donald’s core business is in the real estate market, Ducati is a communication company, car manufacturer core business is finance and so on.

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”? Environment experts and activists are carefully considering the impact of “cyber” and its specific “footprint” (energy, waste, etc).There is a clear andurgent need to rethink the role of technology together with ethical[107] and social issues.

- **Walking On The Clouds**

Another relevant innovative trend in DT is the use of “crowds” to provide data and services not foreseeable before the Internet; simply think about APPs like TripAdvisor[108] 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[109], crowds and platforms. This approach enabled innovative solutions like project funding or collaborative film production[110]. In the global society crowds are playing the role of “public services”.

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 access. Such services were almost unthinkable before. To conclude, we cannot forget that the computer scientist concept of “Clouds” captured the users, so we moved from local storage and processing to cloud computing in its various declinations (SaaS, PaaS, IaaS, Haas); a number of hardware devices, such as tablets and smart phones, offer cloud services to their users. So, clouds are now populated by business data as well as by back-ups, photo albums, video clips and songs. Apart the rest of useful services, the introduction of clouds solved a typical nightmare of e-Citizens, the need to change their personal device, phone, tablet, or computer because it doesn’t work anymore, it was stolen or they bought a new model. The diffuse use of “clouds” contributed to adding another degree of freedom to e-Citizens; many times, this was a seamless transition, so the idea to show their “selfies” or share a document wherever they are and whenever they want from a notebook, a tablet or a smartphone is a consolidated habit and a powerful driver of innovation.

- **Information: The New Gold Rush**

November 1990, on the occasion of COMDEX Fall, Bill Gates introduced the vision of “information at your fingertips”; few months later, to stress the concept, he said that the real wealth in the future will be access to information; people will no more ask “how many dollars do you own” but “how much information can you access to”. In a glimpse, this vision become reality and many years later “information” is still a powerful “transversal” asset: business, trade, policy, security, tourism, health, . . . rely on information, reliable information. Historically speaking, the idea of even

[107] Christoph Stuckelberger, Pavan Duggal (2018), Cyber Ethics 4.0: Serving Humanity with Values, ISBN 978-88931-265-8, Globethics net

[108] Tripadvisor. (2021). *Tripadvisor: Read Reviews, Compare Prices & Book.* [online] Available at: https://www.tripadvisor.com/ [Accessed 8 Feb. 2021].

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

[110] HugeDomains. (2021). *WreckAMovie.com is for sale | HugeDomains.* [online] Available at: https://www.hugedomains.com/domain_profile.cfm?d=wreckamovie&e=com [Accessed 8 Feb. 2021].

owning information is relatively new. 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 eighteenth 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.

- **Is Really Privacy Evaporating?**

Lastly and equally concerning, we all are active or passive users of digital technologies, when we make a phone call or walking along the street in the eye-field of a CCTV.

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, does this mean that privacy evaporated?In the "Appification[111]" 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.

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. 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.

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. This is not enough; what it is not collected by APPs will be collected in a seamless mode by IoT; of course, IoT will add a lot to our life but this will cost us a significant part of our privacy. The even increasing ability to interpret and correlate tiny portions of information create accurate profiles framing us. 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?

Digital transformation directly involves the transition from "citizens" toward "e-Citizens" ignited by cyber technology; as a general feedback we will have a positive trend but it is worth considering even some drawbacks that are becoming evident.

As sometimes happens after revolutions, revolutionaries wonder if what they have got is actually what they were hoping for. The original idea of computer scientists in the "hippies" counterculture era was aimed to empower citizens and provide them much freedom. The perspective in the early phase of ICT was probably to be "here and there", immersed in the core of the business while lying

[111] Kind of neologism stressing the incredible proliferation of APPs.6

on a hammock hanging between two palm trees on a Caribbean island, having much more quality time thanks to technologies. An Apple advertisement on the occasion of the launch of Macintosh in 1983 recalled George Orwell's[112] most famous novel, stating "On January 24th Apple Computer will introduce Macintosh. And you will see why 1984 won't be like '1984'".

Almost forty years later, after the chimera of the "happy cyber-world", some of us have started thinking that the foreseen "1984" has simply come true ten, fifteen years later: globalisation, always on devices, position tracking systems, CRMs and users' profiles, CCTVs and IoT; are those technologies framing citizens?

Thoughts for some time have circled around how the speed of the new information revolution renders us less capable develop a critical approach able to foresee the social, ethic, economic impact of such revolution in a long-term perspective. So, in recent times we started facing a wave of criticism about the evolutionary path of the information and knowledge society, for quite a long time ICT gurus and humanists didn't interact too much, the true power of cyber technology was largely unexpressed, there were some alerts as Artificial Intelligence, Machine Learning, Virtual Reality, Robots often seen by humanists as potential danger for the mankind, but nothing concrete happened. As we have seen the turning point was probably the exploitation of the Internet and the dissemination of information. As a consequence of a lack of "culture" in the use of emerging technologies now we have to deal, among the others, with serious problems related to information ownership, use, abuse and misuse, not mentioning cybercrimes. An additional drawback is due to the deep technological intrusion affecting our daily life, we feel framed by cyber devices more than supported.

Some evident outcomes of this feeling are the "right to disconnect[113]"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"[114]. All these to do not mention the cultural, social and economic impacts not always positive especially in a long-term perspective.

Technologies originally conceived by idealists to provide much more freedom and wellness to humans took then a wrong path framing humans due to all the constraints placed upon us with new technologies. For instance, as liberating as they areby providing flexibility and instant connectivitywe have become enslaved to our devices, fearful of losing out information and access in an increasingly competitive and fast-paced world. Consequently, our bodies have suffered, as have our minds (due to information overload), what of our work-life balanceand this is just to begin with! Ranjit Makkuni's paper "Betrayed IT Revolution" outlines a vision for new design of devices, clutter-free access to web documents to create deeper learning experiences. At the implication level, the project rethinks implications for new design of web mark-up languages that support the creating of 'privacy' based secure browsing.

As a follow-up of the active discussion raised by the "IT betrayed revolution" panellists and some distinguished participants decided to activate a working group to further discuss about this relevant

[112] George Orwell, Eric Arthur Blair's pen name, English novelist, essayist, journalist, and critic. Most well-known novels: Animal Farm (1945), Nineteen Eighty-Four (1949).

[113] the Guardian. (2018). *Personal finance and money news, analysis and comment | Money | The Guardian*. [online] Available at: https://www.theguardian.com/uk/money [Accessed 8 Feb. 2021].

[114] Mayer-Schönberger Viktor , Delete: The Virtue of Forgetting in the Digital Age, ISBN-13: 978-0691138619, Princeton University Press 2009.

topic identifying the WSIS as the perfect framework to approach the human wellness centred development of the information society. The seeds for such a debate were already present since the 2003 Geneva phase of the WSIS, at that time Ethics and Info-Ethics have been a key discussion topic. The actual “visual” trend is producing an incredible amount of photo/video documentation of our everyday life; does this mean “goodbye privacy?”

- **Public Administration / Government**

Through the centuries, many centuries from the ancient Greeks, people studied many different forms of implementation of democracy; among them two major forms arose; direct democracy and representative democracy. Of course, the ideal concept of a power structure ruled by citizens, direct democracy, is hard to implement even in the Internet era; the usual way to solve the problem is to elect a representative structure in order to mediate between citizens and the political power. This structure is usually termed representative democracy. The concept of representative democracy arose largely from ideas and institutions that developed during the European Middle Ages, the Age of Enlightenment, and later on was further developed during the French and American Revolutions. More countries than ever before are working to build democratic governance as a potential tile of digital transformation. Their challenge is to develop institutions and processes that are more responsive to the needs of ordinary citizens, including the poor, and that promote development.

Nowadays a large number of states are ruled by representative democracy, structured in different manners, always structured on different layers of representative bodies directly or indirectly elected by citizens: town government, regional or county governments, etc. Sometimes this “interface” between citizens’ wills and expectations and everyday life generates a bad feeling and sentiment about bureaucracy and government.

In the following part of this paper we term governance the decision-making process that defines the guidelines of the government, we term government the implementation of the decisions and guidelines and the infrastructure of interaction with citizens.

What is e-Governance good for? The notion of e-Governance has its roots in attempts in many countries to ‘modernise’ government in response to perceived citizen dissatisfaction or disengagement. The manner of this disengagement varies, but has been reflected in many countries in falling voter numbers, and particularly in the ‘Anglo Saxon’ democracies, in a perception that public services are failing and of poor quality. This can result in ‘opting out’ on the part of the more affluent in favour of privately provided services including education and healthcare, with a consequent fracturing of the social consensus on the provision of these services.

This notion of ‘modernisation’ was intimately connected with what was sometimes called ‘joined up’ or ‘holistic’ government. The benefits of this were felt to be twofold: it was an attempt to reconstruct government in the interests of the citizens, rather than the producers, moving away from ‘departments’ and ‘silos’ towards ‘personalization’ and ‘life events’.

Secondly, there is widespread agreement that many social problems, from crime to poor educational performance, are the result of multiple interactions and the only way to tackle these issues more effectively is to understand these interactions better. And this means ‘joining up’ the information that we have so that, for example, if we know that much petty crime is committed by children who play truant from school, we can identify truants at an earlier stage (or even the behaviour that leads to truancy) and hopefully prevent some crime.

This means having an integrated view of the information that is held on citizens, a sort of social "knowledge management", that was impossible before the advent of widespread ICTs. This means basically a fully integrated information system collecting data from different sources, including real-time information from sensors and Internet of Things. These solutions must evidently carefully consider privacy issues.

Sophisticated ICT systems are leading to a greater decentralisation of government. This can be particularly observed at the local level, where neighbourhood offices, one-stop shops[115] and call centres are replacing the walk to the town hall or housing benefit office. These newer forms of neighbourhood offices, or "one stop shops", seek to provide access to a complete range of servicesrather as the bank branch does to the banking network. This relies on having accurate information on citizens available across the system, but the opportunity it opens up is greater responsiveness to local needsoften at the neighbourhood level. The closer to the 'front end' that decisions about service provision can be made, the closer they can reflect local needs.

In order for citizens to become really active users and indeed co-producers of public services, citizens have to be increasingly involved in and aware of the information on which decisions are made. Citizens can select different public service 'packages' in return for revealing different levels of personal information. This is an acknowledgement that joined up government requires a large degree of information about individual citizens' needs and preferences and that citizens can be empowered to decide what level of trade-off they want to make. Of course, there are dangers that over-personalised public services risk atomisation and reward those citizens that are easy to serve, make little demand on services and can use the Internet proficiently. In the public sector the data collected by personalisation is primarily a social resource and should be used for collective benefit. Thus, if we collect evidence that people who do X are more likely to do Y, we should be able to reduce the costs of production processes, by targeting resources more effectively—not just at individuals, but at society at large, by developing education programmes to demonstrate the benefits of doing X. A positive approach demonstrating the benefits of a particular behaviour instead of putting blocks, limits and fines is always better and provides the rationale and citizens' cooperation. These trade-offs are likely to become even more apparent as smart card technology increases as a delivery vehicle. The utility of such cards is related to the amount of personal information they hold. Some early experiences in the use of smart cards[116] were carried out in the nineties opening the way to a wide range of services like mobile phones, digital signature, social security and more.

Among the new organisational vehicles that are resulting from e-Government are public/private partnerships, which bring together private sector systems and technology expertise with public sector services and values. Although the 'branding' implications of that may worry some local governments, it has been instrumental in turning around the perception of an authority that was failing and is now seen as more dynamic.

[115] The idea of the "one stop shop" was one of the first innovations due to e-Government; it was in some way a reverse of the paradigm, no more to expose the internal structure of government as the direct interface with citizens but the interface with citizens shaped to better serve citizens. One single entry point (one stop shop) will provide the complete feedback/service to citizens.

[116] Back in 1988, a group of Thomson Microelec- tronics engineers founded, after preliminary studies on smart cards carried out at Thomson, the Gemplus14 company with the aim to further develop "smart cards", a thin microchip embedded in a kind of credit card. Originally marketed as gadgets to open entry doors in clubs and lounges, smart cards become a key technology in 1990 thanks to the adoption of SIM (Subscriber Identity Module) cards by GSM mobile phones; the contract for the first million cards was signed with France Telecom. From that time onward, smart cards flooded the market, embedded in credit cards, identity cards, voting IDs, badges, etc.

Further benefits are flowing from partnerships with other public sectors or civil organisations. One aspect of being able to offer a better service is access to a significantly wider range of information, much of which sits outside the Local Authority. Services produced at a reduced cost, or made more widely available, are becoming a feature of these e-Governance experiments, but genuinely transformed services are rarer. This is partly a result of uneven access to technology and again re-enforces the point that the bigger payoffs will only come when access is at, or close to, being universal. This is because running parallel systems remains expensive and because a (virtually) universal service, like income tax, cannot be transformed in part; the whole system has to be re-engineered.

- **What About Education 2.0 ... 4.0?**

Dealing with digital transformation and future society it is wise to focus on digital transformation in education from kindergarten touniversity both degree and PhD levels. The pandemic has forced educational institutions to switch to online teaching, on the road to a better resilience of the educational system but very less efforts were devoted to an enhanced transmission and acquisition of knowledge.Nowadays after a sufficiently long period of test online education, as it was implemented on the fly due to the pandemic, showed some limits and drawbacks. We must adequately consider the different format due to different topics: anatomy, mathematics, physics, literature, etc. Main ICT approaches, of course, refer to a typical ex-cathedra lecture having a limited interaction with students, if we consider subjects that require a higher interaction such as design or architecture, that are much more maieutical processes, these solutions are not directly applicable.Researchers are looking for better solutions, some technologies are enabling new communication formats. Virtual reality, for instance, offers the opportunity to let humans interact with intangible objects bridging the gap between the two methods in cognitive sciences the perceptive-motory and symbolic-reconstructive. Today, people have the opportunity to create digital objects, a new class of objects from an ontological point of view. They can be infinitely duplicated and transmitted or accessed world-wide. A typical example is represented by virtual laboratories enjoyable by big number of users ideally all-over the world. With the spread of the coronavirus, the education system is facing a new crisis, extended school closures may cause not only loss of learning in the short term, but also further loss in human capital and diminished economic opportunities over the long term.

Before the outbreak of the coronavirus pandemic, the world was already dealing with crisis in the sector of education,traditional education methodologies were already outdated. An educational and communication divide was already on stage between millennials (generationY) and the educational system. It is a common understanding that recent generations represent a discontinuity if compared with the past ones. Such discontinuity or, if preferred, singularity is recognised both by adults complaining because their children do not pay attention or are getting bored by learning and, by adults, that discovered new skills and capabilities in young generations. People that grown up playing video games, browsing the Internet, chatting and looking for help on line in communities, they use technology seamlessly. A new model for communication processes is required. This is a side effect of their special skills acquired in hours and hours of digital tasks. Social psychology offers compelling proof that thinking patterns change depending on an individual’s experiences. A sufficiently long training may activate this phenomenon. In fact, some researchers believe multi-sensory input helps kids learn, retain and use information better. So, the Apple motto “think different!” is much more than a motto.

As already outlined a renovated approach to education it is not only a matter of network infrastructure and computers, it’s a matter of humans so both students and teachers need to adapt to collective online learning, improve emotional and behavioural self-regulation. Having the evidence that traditional didactic doesn’t match with young’s expectations we need to take advantage from the additional need to make educational activities more resilient to start reshaping the system in order to fit with both requirements: resilience and generation Y compliance. Education system must cope with such requirements and take advantage from similar new skills even if there are some “side effects” that must be amended or at least mitigated.

Direct access to information and related hyperlinks may create some drawbacks, among the others, a kind of “surface knowledge”, many times more suitably identifiable just as “information”, without the required contextualization and logical connections with other items, plus the risk to lose the logical path related to the key topic. The overall effect is to create “archipelagos” or even “islands” of “surface knowledge” without connection with the rationale background or deep knowledge on the specific topic. In addition to this both the social networks and online resources could provide fake or unreliable information many times in absence of critical thinking on the student’s side. So, in parallel with the setup of education innovation, that is nowadays led by ICT, we must improve student’s critical thinking and technology awareness. The latter includes specific knowledge about potential risks associated to an improper use of technologies.

Mentors need to upgrade their knowledge in ICTs possibly bridging the generational gap as much as possible that means to use social media activating a tight and multilateral interaction with students. Leading the change having proactive approach to the natural evolution of the content domain. Time will solve this problem, in fact the early generation X is coming on stage.
On the client-side students quickly learned how to use, sometimes everyday tools, as educational means. Accordingly, with the typology of the education institution chatting apps were used or multipoint conferencing systems.

To conclude, on the way of the digital transformation of the educational sector the global lockdown represents a unique opportunity to bridge a number of gaps and reshape our future, thinking out of the box, identifying what is useless, deleting biases due to habits, rethinking processes and protocols. Education system can take this opportunity to develop a new approach to improve its resilience and “generate deep knowledge” in millennials.
This is the time for action, the question is “Leading the change or missing the opportunity?”

- **The Role Of Social Media**

The idea to share something with someone else, a group of people, sometimes generates a sense of belonging to a “community”. Memetics used to consider this “something” as the “meme”. A meme is a cognitive or behavioural pattern that can be transmitted from one individual to another one. Consider young people that wear clothes in an unconventional way or use signs and gestures that show that they belong to a particular community. The basic mechanism is very simple; since the individual who transmitted the meme will continue to carry it; the transmission can be interpreted as a replication. A meme carrier, known as a replicator, is created when a copy of the meme is made in the memory of another individual. Replication or self-reproduction is the basis for the memetic life cycle. This leads to the spread of memes to more and more individuals, such that the meme acts as a replicator, in a similar way to the gene, today this looks familiar if we refer to virus and pandemic effect.

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[117], but communication is the key player in the creation of communities and due to this, communities directly dealing with communication means are facilitated. In the early stages of computer intercommunication, apart from exchanging signals and data, a basic text messages service was implemented. Ancient timesharing computer systems had local “mail” services so its users could communicate. But the real power of “electronic” mail came true when mail could be distributed to distant computers and all the networked users could communicate[118]. Late in the 1980s the increasing use of bulletin board systems (BBS), file transfer protocol (FTP), Telnet and other communication tools such as Veronica and Gopher prepared the playground for the massive use of the Internet and the World Wide Web. Since the beginning of computer user’scommunication, a sense of community arose and a common feeling on behavioural rules was implemented.

As already outlined social media are one of the milestones introduced in the digital domain and represent a powerful innovation without a “twin” the analogic world. Social media are the key of success of the digital domain, 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), Instagram (’10), SnapChat (2011), Telegram (2013), Signal (2014), Tik Tok (2016) ... Social newspapers (e.g. YouReporter, Bambuser), and more, much more.This “addiction”, sometimes and in some social contexts, blurs the line between reality and cyber world, so a mix fake news, small communities pretending to represent the whole population, distortion of reality due to the long chain of word of mouth delivering news and theories, become “the reality”.

Of course, freedom of expression is one of the most appreciated opportunities offered by the Internet and it is already evident that any kind of top-down censorship or control does not succeed even if the concept of Cyber Sovereignty exists and is promoted. If the early stage of Internet communication was based on the so-called “netiquette”, a kind of Galateo[119] 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. 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 websites are not allowed. Here apart from political, ethical and philosophical issues may come to the fore the economic and financial aspect of entering that market adhering to the requested censorship or not[120].

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

[118] The official launch of ARPANET was a large, very successful demonstration that was organised and presented by Robert Kahn in 1972 during the International Computer Communication Confer- ence (ICCC). Early in the 1970 the French Institut de Recherche en lnformatique et en Automatique (IRIA), nowadays INRIA, sponsored the creation of the first network based on packet switching the CYCLADES computer network defining the basis for TCP protocol (refer to Louis Pouzin). The first hot application appeared in March of that year courtesy of Ray Tomlinson: electronic mail. Tomlinson wrote the basic email message send and read software, which was intended to aid cooperation between the distributed research team working on the network project.

[119] 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.

[120] 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.

The Internet Revolution gave a boost to data creation and dissemination, MAC addresses, web logs, and intentional or unintentional[121] applications to websites and services, and social platforms ignited the sedimentation of personal and many times sensitive information apparently lost in the cyberspace. Very soon the first drawbacks come on stage: privacy infringements, stalking, hacking, cyber-crimes, stolen identities, darknet and more.

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, how many of you use to carefully read the privacy agreements and contracts plus related periodical updates before clicking on "accept"? 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 access, 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; hedoes nothing with this information, simply stores it in his notebook, he is unseen and you will never face him and discover his activity; basically in doing so he didn't break any law. His behaviour is unconventional but still legal. If you act in public spaces or visible by public there are no laws that state that you are the sole proprietor and owner of the information regarding your public life; the collection of this information doesn't violate any right. If we look in law, the closest legal offence in such a situation is stalking even if this offence usually is directly connected with harassment; but the unseen observer does not ever interfere with you so no harassment, no stalking even because the unseen observer is your smartphone and it can't be convicted of stalking you. This is what happens when some "autonomous" on-line applications start showing you your yesterday's paths across the city showing some geo-referenced pictures you shot asking for the reason you went there and what you did in the 15 minutes you spent stopping on the way to your destination. Of course, the system recognises your friends in the pictures and next time probably will ask you why you met them.

Anyway, on the reverse there is a real risk of abuse, misuse and misinformation thanks to these technologies. The movie "Citizen Kane[122]" directed and interpreted by Orson Welles in 1941 outlined the relevant "power" of journalism[123], the movie "Network[124]" directed by Sydney Lumet outlined the power of television in 1996 and perhaps "The Net[125]" and "S.Y.N.A.P.S.E.[126]" together with "The Social Network[127]" started to outline the power of the Internet.

[121] Sometimes the "applicattion to the service" is activated by hidden links or linked to the activation of a basic service.

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

[123] 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.

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

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

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

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

Computer biometrics is nowadays very advanced; so, starting from the Apple tools to recognize people appearing in your pictures once you gave the system two or three samples, a group of Russian developers released in recent times a powerful application, FindFace, that performs in real time the face recognition even of multiple persons and connects them to their V-Kontakte, the Russian version of Facebook, page. This enables users to take a picture with the smart phone on the street on in a disco and immediately discover the identity of the subjects. Is this a potential infringement of privacy? Is this a powerful tool for stalkers? Technological evolution does not have limits; it is already available for the professional market, e.g. law enforcement, a full version of FindFace offering far better performances without the limitation to V-Kontakte subscribers.

- **The Role Of News And Media**

News and Media are key elements in the global society. CNN, BBC, Al Jazeera[128], Al Arabiya[129] are writing the history of the planet 24/7 and on the grassroots side YouReporter[130] and Twitter 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[131]" 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. 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.

As already stated, the Internet is much more a counter-power than a power; the common idea about the Internet is "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[132] by user-generated content (UGC) largely without any qualification and certification of the source. Many times, the drawback attributed to the amanuenses is affecting even web publishers: information and content is re-used and re-published adding or replicating errors and bugs. The short content production chain, sometimes even limited to a one-stop shop, does not include an editor in chief or a supervisor; so far, the overall quality of prosumer content and information is quite low.

[128] Aljazeera.com. (2021). *Breaking News, World News and Video from Al Jazeera*. [online] Available at: https://www.aljazeera.com/ [Accessed 8 Feb. 2021].

[129] Alarabiya.net. (2021). □□□□□ □ □ | □□□□. [online] أخبار الع
Available at: https://www.alarabiya.net/ [Accessed 8 Feb. 2021].

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

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

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

As an IBM top manager told recently on the occasion of the Global Forum: “Do not trust in any information coming from unknown source.”

- **Wrapping Up The Overview**

Digital transformation will deeply impact our daily life, our activities, social relations, spare time. It will increasingly impact economy, labour, distribution of wealth. A significant "injection" of human and social sciences, including ethics and philosophy, is needed to lead the process, looking forward to identify “where” we are going and what the results of the "transformation" will be.

- **Bibliography**

1. Anderson C (2012) Makers the new industrial revolution. The Random House Group Limited. ISBN:9781847940650
2. Babel Chris, Tackling Privacy Concerns Is Key to Expanding the Internet of Things, Wired Innovation Insights, Feb 2015
3. Burrus Daniel, Who Owns Your Data?, https://www.wired.com/insights/2014/02/owns-data/
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. Duggal P (2018) Cyber Law 3.0, LexisNexis, Gurgaon, India, ISBN 978-81-3125-366-3
6. Google - Privacy & Terms, https://www.google.com/intl/en/policies/privacy/
7. 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/
8. Information for All Programme (IFAP), International Conference on Media and Information Literacy for Building Culture of Open Government, http://www.ifapcom.ru/en
9. Mayer-Schonberger Viktor, Delete: The Virtue of Forgetting in the Digital Age, ISBN-13: 978-0691138619, Princeton University Press 2009
10. My data belongs to me, http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-discussion-personal-data-virtualisation-society-wsis10-review
11. Dawkins Richard (1995), The Selfish Gene, ISBN 9780586083161, Orio Publishing Co, United Kingdom, London
12. Moritz E (1990) Memetic science: I. General introduction. J Ideas 1:1–23 and Moritz E (1995) Metasystems, memes and cybernetic immortality. In: Heylighen F, Joslyn C, Turchin V (eds) The quantum of evolution: toward a theory of metasystem transitions. Gordon and Breach, New York (J Gen Evolut Spec Issue World Futures 45:155–171)
13. Norman DA (1988) The psychology of everyday things. Basic Books, New York
14. Norman DA (1994) Things that make us smart: defending human attributes in the age of the machine. Addison Wesley, Reading, MA. ISBN:0-201-58129-9
15. Norman DA (1998) The design of everyday things. Basic Books, New York. ISBN:978-0-262-64037-4
16. Norman DA (2007) The design of future things. Basic Books, New York
17. Protection of personal data in EU, http://ec.europa.eu/justice/data-protection/
18. 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
19. Ronchi Alfredo M., (2019), e-Citizens: Toward a New Model of (Inter)active Citizenry , ISBN 978-3-030-00746-1, Springer (D)
20. Ronchi Alfredo M., (2019), e-Democracy: Toward a New Model of (Inter)active Society, ISBN 978-3-030-01596-1, Springer (D)

21. Ronchi Alfredo M., (2019), e-Services: Toward a New Model of (Inter)active Community, ISBN 978-3-030-01842-9, Springer (D)
22. Ronchi Alfredo M., (2018), . . .1984 won't be like "1984"?, ISBN 978-5-91515-068-9, Interregional Library Cooperation Centre, Moscow
23. Christoph Stuckelberger, Pavan Duggal (2018), Cyber Ethics 4.0: Serving Humanity with Values, ISBN 978-88931-265-8, Globethics net
24. Surowiecki J (2004) The Wisdom of crowds: why the many are smarter than the few. Doubleday, Anchor. ISBN:978-0-385-50386-0
25. 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/
26. Merriam Webster: Ethic, http://www.merriam-webster.com/dictionary/ethic
27. Weiser Mark D., The Computer for the 21st Century, Scientific American Ubicomp Paper after Sci Am editing, 09-91SCI AMER WEISER