Presidenza del Consiglio dei Ministri



INFORMATION AND COMMUNICATION TECHNOLOGIES AND *BIG DATA*: BIOETHICAL ISSUES

25 November 2016

TABLE OF CONTENTS

Introduction 3
1. Preamble 5
2. Prospects for development and emerging ethical issues 6
2.1 Processing of personal data: challenges to privacy and informed consent 8
2.2 Transparency: the ethics of algorithms and network neutrality 12
2.3 Truthfulness and quality of information: possible bioethical implications 13
2.4 Addiction: a further bioethical implication 16
2.5 Participatory Justice 17
2.6 Governance 17
3. Recommendations 19
Annex: Legal note 21

Introduction

The advancement of information and communication technologies and the development of informatics are paving the way to new possibilities of knowledge, use and application in different fields, including healthcare. The expression big data refers to a massive volume of digital data constituted by the traces of personal information released into the environment through the use of information technology: this huge amount of data, coming from heterogeneous sources, is generated at great speed with pervasiveness.

The document discusses the enormous opportunities for development now opening up, especially in healthcare, with telemedicine, precision medicine, and the development of healthcare policies. The Committee also outlines some critical issues regarding the difficulty in governing the huge amount of data in the collection, analysis and use of data, particularly when it is used and applied differently from initial collection or without user awareness. Information technologies can present challenges regarding primarily processing and protection of private life and personal data, transparency, quality of information, addiction, the principle of participatory justice and governance.

The CNB, in view of an "appropriate" use of data, respectful of fundamental human rights, makes some recommendations: defining the responsibility of providers; verifying data quality and transparency of algorithms; identifying efficient instruments to request user consent or dissent to the processing of data; implementing an effective recognition of the right to be forgotten; involving citizens in emerging ethical issues, with special attention to young people, calling for the development of guidelines for the proper use of social technologies; promoting research for innovation of the ethical approach to the design of social technologies; guaranteeing all those who are willing to make use of new technologies conditions for access.

The Opinion calls for the development of legislation for the protection of personal data and the safeguarding of citizens/users against the social risks of misuse of data.

The annex includes a legal note retracing synthetically and in a critical manner the current situation of European and national regulation.

The subject and original draft of the Opinion was brought to the attention of the Committee by Prof. Rosaria Conte in April 2015.

Prof. Rosaria Conte presented in an internal consultation session the state of scientific and ethical discussion.

The group met twice in 2015. The preparation of the Opinion was interrupted because of Rosaria's ill health and death in the summer of 2016, which has left a great void.

Profs. Antonio Da Re, Lorenzo d'Avack, Laura Palazzani and Carlo Petrini have supplemented and completed the Opinion.

The Opinion was approved unanimously by those present on November 25, 2016, Profs. Salvatore Amato, Luisella Battaglia, Stefano Canestrari, Antonio Da Re, Lorenzo d'Avack, Riccardo Di Segni, Silvio Garattini, Marianna Gensabella, Assunta Morresi, Laura Palazzani, Monica Toraldo di Francia, Grazia Zuffa.

Dr. Maurizio Benato, Dr. Carlo Petrini, ex officio members , have also expressed their approval.

The Opinion was subsequently endorsed by Profs. Carlo Caltagirone, Cinzia Caporale, Carlo Casonato, Bruno Dallapiccola, Mario De Curtis, Carlo Flamigni, Paola Frati, Andrea Nicolussi, Rodolfo Proietti, Lucetta Scaraffia and ex officio members, Prof. Maria Teresa Palamara and Dr. Carla Bernasconi.

1. Preamble

In this document, the National Committee for Bioethics (CNB) refers to Information and Communication Technologies (ICT: Information and Communication Technologies) or the set of methods and technologies for the digital transmission and processing of information that enables or improves interaction between and with users at different levels (individuals, groups, communities, companies, organizations, institutions, etc.), with specific reference to the phenomenon of big data in relation to people's health.

The advancement of information technology (with the increase and acceleration in the collection, storage and processing of information) and the development of "data science" (i.e. the use of computing and mathematics with statistical techniques and algorithms) are opening up new possibilities of knowledge, use and application in various fields, including healthcare.

Particular reference will be made to: a) Social Technologies, i.e. the technologies employed by users to share content and technologies that provide information on possible partners for exchanges and cooperation (social networks); b) providers; c) search engines; d) user profiling techniques, which obtain/ derive/mine (relying on the use of complex algorithms) information from users, for diversified applications, including commercial applications, within the context of the so-called "digital revolution"[1].

In this context, the expression big data refers to massive digital data constituted by the traces of personal information released into the environment through the use of information technology[2], which is characterized by certain properties:

heterogeneity: different types of digital data and diverse supply sources (computers, mobile phones, the Internet, mobile devices and sensors, etc.); to traditional medical data (the results of laboratory testing, clinical records, epidemiological investigations) medical data coming from new technologies are added (genomic tests, results of body imaging or internet of the body, electronic records, remote monitoring technologies or telemedicine);

numerosity: quantitative increase of data, it is becoming increasingly difficult to keep up with the updating of the unit of measurement (terabytes, petabytes, exabytes, etc.);

speed: exponential increase of connections and the data generation rate (it is very likely that in 2016 the number of connections on social networks will reach almost 19 billion);

ubiquity: unlimited expansion potential of data within the global network, and pervasiveness or invasiveness of possible data collection in all spheres of people's lives;

possible untruthfulness: the scarcity and possible lack of verification work on authenticity, accuracy and quality of information.

---

[1] S. Spiekermann, A. Acquisti, R. Boehme, K-L. Hui, *The Challenges of Personal Data Markets and Privacy*, in "Electronic Markets", 2015, 25, pp. 161-167.

[2] Not subject to analysis is the issue of *big data* from information derived from the use of genetic tests, *genome-wide tests*, which is analyzed in the Opinion *Managing "Incidental Findings" in genomic investigations with new technology platforms*, 2016.

Users are induced and encouraged to provide information in exchange for other information; since any user action in the system turns into signaling, giving access to user features, users release a large amount of information to the benefit of the operators of these systems. ICT systems are therefore generators of collectively produced public and private information.

However, we will not be dealing with:

= educational platforms (such as MOOC, Massive Open Online Courses, or those supplied to specific telematic institutions) or entertainment systems (Secondlife, World of Warcraft, etc.), as they are not based on the collective provision of information[3];

= big data in developing countries with emerging economies, given that many problems have different connotations;

= security systems and systems of exchange and sharing (such as electronic markets and sharing economy systems), which despite being based on information provided by the user, and raising ethical concerns in a broad sense these do not present specific bioethical problems, which fall within the focus of attention of the Committee;

= systems that use big data to detect collective political sensitivity and orientations, in order to achieve consensus and steer electoral choices.

The CNB has already partially dealt with some of these issues in previous Opinions: Ethics, health and new information technologies, 2006. The identification of the human body: bioethical aspects of biometrics, 2010 and Mobile Health Apps: bioethical aspects, in 2015.

2. Prospects for development and emerging ethical issues

Information technologies offer significant opportunities for economic and social development, and significantly enhance the individual's ability to acquire information and connect with other individuals as well as social and institutional entities, etc..

The expansion of ICT enables and will enable worldwide communication in the so-called "digital" society and allows digital citizens to obtain broad information in a simple manner, in their own language and in indefinite quantities. Major ICT systems in the future will lead us into an age of choices and unprecedented possibilities with a larger number of available data. The "explosion" of data and the "data revolution" will have spillovers on the world of politics, economy, and education.

At the same time, easy access and use of ICT permits almost everyone to use them. The only existing limits come from accessibility to the necessary technology (mobile phone, electricity) and a certain level of education so as to enable use (so-called "digital literacy"). The increasingly pervasive use of new information and communication

[3] Moreover, in these systems, the high number of users is not as explosive as for other types of ICT (in 2015, 1 million on *Secondlife*, 5 million on *world of warcraft* compared to 1 and a half billion on *FB*). Finally, the actual functionality of these systems is controversial: *secondlife* is for example considered by some a failure (https://it.finance.yahoo.com/notizie/che-fine-fatto-secondlife-07524429.html), even if the number of users of this system is not growing, neither is it reducing (http://www.downloadblog.it/post/21761/secondlife-dimenticato-dalla-stampa-ma-rimasto-solido-ed-amato).

technology in everyday life (everything we do leaves an informatic trace), makes us consciously or unconsciously, "users/contributors" of big data and our "digital" addiction, both personal and collective, tends to increase. On the other hand, it is not a question of stopping everything or moving backwards: not only is this impossible, but it would mean curbing a development process with enormous potential and promise.

Particularly significant paths of development in the field of health are taking shape with so-called "Data-driven precision medicine", (still the subject of study and research and currently not extended to all aspects of biology and medicine) this is the possibility to make, based on the amount of data collected, predictions and simulations of diagnosis and treatments for individual patients in specific contexts or for stratified groups of patients (so-called personalized/stratified medicine or precision medicine), but it could possibly be extended to the definition of healthcare policies for public health and to prevention in particular. Moreover, ICT can improve and increase the efficiency of health services. As a matter of fact, there is a growing interpenetration between health care, information technologies and decisions taken regarding treatment. Cybermedicine is the all-encompassing term denominating this phenomenon, it is used to indicate the networking of a wide community of interests between various increasingly interdependent subjects who need this communicative exchange (national and local institutions, public health agencies with their own territorial organizations, private health organizations, health professionals, pharmacies and all the pharmaceutical sector, service companies and the suppliers of non-profit companies, voluntary and citizen associations).

Although we live in a deeply interconnected world, its modes of interconnectedness are only very broadly known to us: not only are we not in a position to know enough about the procedures and the paths that form our data as individuals, we are also not fully informed about how the data will actually be used, stored and for how long, who will use it and for what purpose, via which paths, who is responsible and to what extent. It is the existence of big data as such that makes it impossible to be truly and fully aware of this new universe.

However, a number of ethically problematic issues arise in relation to big data with specific reference to collection, analysis and use of data, particularly when it is used and applied differently from the initial collection or without the user's knowledge[4]. Information technologies can involve risks mainly related to the processing and protection of privacy and personal data, transparency, quality of information, addiction to ICT, even of a pathological kind, the principle of participatory justice and governance. The dangers relate mainly to: the misuse of data which causes harm to individuals, undue surveillance, stigmatization or discrimination. The scenarios may, therefore, be complex and in some respects disquieting and yet insufficiently explored, especially regarding the impact on the health of citizens/clients.

[4]For emerging ethical issues in ICT, see: European Group on Ethics in Science and New Technologies (EGE), *Ethics of Information and Communication Technologies,* 2012; reference to big data on *The Ethical implications of new health technologies and citizen participation*, 2015.

2.1 Processing of personal data: challenges to privacy and informed consent

Contact with the virtual world starts from birth and entire stages of life are fixed in time and potentially made digitally visible to everyone. The exposure of "personal data" and "personal life" on the network raises the issue of privacy, minors especially are often unaware of this. The problem becomes even more complicated to tackle in a society which welcomes, values and promotes data "sharing" (information, images, videos).

The need for protection of the confidentiality of certain information and the means to defend one's virtual privacy should be highlighted from the earliest years of life, especially with the help of parents and educational systems. An education to active citizenship, which strives toward adaptation to our time (a kind of "Civic Education") cannot, by any means, underestimate the importance of these issues. Consequently, the recommendation to set up educational programs to enable users to develop this awareness within the context of acquiring a technical culture on instructions for internet use, is especially significant. This is particularly true as citizens risk losing much of the control they have on their private information in this virtual space through the expansion of data. The challenge presented to digital users lies in their gaining critical awareness of the problem, determining which devices and instruments they are able and willing to use, in order to avoid, as far as possible, losing control over their privacy.

One of the first ethical issues raised in the ethical and legal debate regarding ICT was the need for people to have sufficient control of their data when using the Internet, especially so-called sensitive data , including health data. The first regulations in the sector have specified the conditions applicable to the processing of data at the time of the request for information, which, should always be accompanied by explicit informed consent. This implies that there is transparency, completeness and simplicity in the information given by those who use and process information: they should specify who is collecting the data and who will use it, which data, how the data is collected, where it will be stored, for how long and for what reason and purpose. Consent must always be revocable, without producing negative consequences for the user; and, unless the expression of consent provides otherwise, the right to access, rectify and delete personal data (so-called right to be forgotten) must remain5 so that it is no longer accessible to the public in any form (copy or reproduction). Consent must always be able to provide an alternative computationally, i.e. refusal of consent (to provide information), setting out

[5] As argued in the CNB Opinion *The identification of the human body: bioethical profiles of biometrics, 2010*, "it must become an aspect of the fundamental right to personal identity, the right not to be catalogued, classified, possibly irreversibly marginalized on the basis of information obtained without one's knowledge, through non-transparent criteria and for largely unknown objectives. The growth, in terms of efficiency and security, biometric acquisitions should therefore be accompanied by a proportional increase of the possibilities of protection and hopefully of public awareness. If one cannot claim anonymity, it is essential that at least the conditions to be forgotten are guaranteed. " The document by The European Group on Ethics in Science and New Technologies (EGE), *Ethics of Information and Communication Technologies,* cit., suggests replacing the prevailing expression "*right to be forgotten*" with "*right to data deletion*".

the implications. This means, in other words, transferring the concept of "traditional" informed consent from biomedicine to information technology.

In the age of big data we are witnessing a radical digital transformation which demands a change to both ethical and juridical approaches, with the re-signification of traditional categories; "privacy" being distinctly one of these. Many speak of "the end of" privacy, or of a concept destined to "evaporate". Even informed consent in its digital form is much more complex and requires structural rethinking. It is a matter of working out the new scenarios in which we find ourselves in the age of big data.

1) What information is collected?

The information requested of digital users is of an absolutely heterogeneous nature: for example, the information related to socio-demographic data (gender, age, marital status, education, affiliation, etc.) differ significantly from those relating to religion, political and ideological affiliation, and these in turn differ from the information concerning emotional states, attitudes, aptitudes, preferences and so on. What kind of information, therefore, is referred to when one authorizes the processing of personal data in the digital environment? The very concept of privacy is changing: it no longer just refers to the protection of "personal data," information relating to an identified or identifiable, also indirectly, natural person by reference to any other information including a personal identification number and demographic information, but it extends to consideration of "personal life" or "private life" (which also includes information on biological data, behaviour, thoughts, feelings, personal communications, movements, groups etc.). Today, privacy means without any interference in private life, it is an appeal to discretion and confidentiality.

With specific regard to the data concerning health, consideration should also be given to the fact that boundaries between the strictly medical and non-medical spheres are becoming increasingly blurred, like those between health and society: information on lifestyles and behaviours tends to become increasingly more relevant to health even within the perspective of prevention. In this sense, health information is considered to be not only the results of laboratory tests or epidemiological data, but also the general news that comes from social networks.

2) How is information collected?

Whatever the type of information, it is difficult to ensure the individuals' full awareness at the time of consenting to the processing of their data: in the everyday practical use of network services, users are inattentive and in a hurry, they do not stop to carefully read the contracts they sign (frequently displayed on a screen, written in small type, in multiple pages) in order to access the service that is of interest to them. In addition to this: users - and this is particularly true in the case of network information managers - do not know how this information was obtained, nor what specific uses it allows, they do not know or do not remember if and what they previously consented to. For instance, the case of the information that can be obtained by clicking on like once users are signed up on social network pages. Even if those registered know that their like

can be a valuable source of information for that particular service provider, they do not know how these like are treated. At the same time users can not be said to be completely free when faced with the alternative of either handing over their data or being compelled to terminate use of the social network service. Or indeed, when free services (e.g. access to music etc.) are offered in exchange for the "bestowal" of data.

3) Who collects and stores the data? For what purpose? Where are they stored?

As regards the quantity of data collected and processing modalities, the individual user is hardly able to understand the potentialities held by those collecting this data. It is generally not explained to the user who collects the data (the phone company if collected by cell phone? the provider if collected by computer?). "Network information managers" (both public and private) collect data in aggregate form, with the ability to mine information (this is the basis of the economic attractiveness of data). It must also be taken into account that, currently, online platforms (in particular private managers) can forward or sell the data as "macro-aggregates" to other companies (if not legally prohibited) without asking for specific and precise consent, with the result that people communicate information about their lives to a much greater extent than they are actually aware of.

There is "in principle" a difference between the potential uses of data and the associated risks: their use differs for commercial purposes (e.g. the use of data to identify categories for advertising and marketing purposes) or scientific use (e.g. the sharing of health information within services/pathways of care, for the purpose of clinical-epidemiological research). It is not easy to make this distinction; in most cases the boundary between scientific research and market research becomes blurred and indistinguishable, at the expense of the unwitting digital user (e.g. think of the "PatientsLikeMe" platform, where scientific research and commercial research are closely and indistinctly connected).

Moreover, even assuming the possibility that all information is clearly expressed and communicated to users (regarding the collection, storage and use of data), there is the problem of its actual intelligibility, given the quantity of information and the complexity of content (just think of what it means to explain and understand the meaning and functionality of an "algorithm" or to explain the concept of a person's private life and dignity), and given the lack of interaction with the user to allow for assessment of suitability (as opposed to informed consent which is obtained after information is given by the doctor to the patient).

This results, inevitably, in a "challenge" to informed consent as it has been traditionally understood, which by contrast requires reformulation following new paths, possibly providing for differentiated modalities of informed consent according to the context.

Informed consent, in the field of big data, cannot be specific (as in the case, for example, of "traditional" medical consent) ; it, inevitably, calls for characteristics of "broadness" given the impossibility of accurately anticipating the paths of research (similar to what occurs within the framework of biobanks): it is therefore a "dynamic" and "flexible" consent, which identifies similar areas of research directly or indirectly related to

the original path. Broadness, dynamism and flexibility do not mean "blind" consent to whatever research.

One could perhaps rethink the very expression "Informed consent" in the digital world, limiting it to an "awareness" or "acknowledgement" that the data will be collected, in the critical consciousness of the impossibility of anonymity (re-identification is always possible, i.e. by crossing information user identity is traced back), in the non-precise a priori determination of the method of use, storage, and analysis of data, and the impossibility to guarantee security and confidentiality in all circumstances.

It should also be considered that the need to introduce, in a precise manner, the use of consent for each specific step in the use and application of data could provoke exactly the opposite reaction in the digital user: instead of increasing the user's attention to problems, it could increase haste and divert attention away from the actual subject matter of the consent. Consider the use of consent to cookies: one can not fail to point out that faced with the legitimate concern over the use of the information obtained by "clicking" on various web pages, the request mechanism has become so pervasive that the user generally does not read the disclosures and ends up giving consent indiscriminately whenever so requested. Web browsing would, otherwise, be dedicated most of the time to reading disclosure documents on privacy.

Given these uncertain scenarios, and in particular the blurred boundaries between scientific research and commercial research, it is possible to envisage that individuals may a priori express themselves at least under certain "minimum conditions", with a request for a posteriori verification: by requiring that data be provided only on condition that both the subject acquiring it (distinguishing at least between public and private institutions) and the purpose of the data transfer are known; demanding transparency and interactive participation (with online portals that facilitate communication), dynamic communication of research findings, the possibility to "opt-out" or exit the research if it takes paths that the user does not agree with and, consequently, delete the data from that moment; defining the areas of research to which the user objects (for example, objection to the use of information for research in the military sphere or other sphere).

We must remember that the individuals themselves are willing to "share" information, not keep data private and actively participate in research. The important thing is their being aware of the possible implications of this active participation and sharing and the actual possibility of opting out of any research.

An emerging specific problem in healthcare is the relationship between mandatory transfer/sharing of data and insurance. The customers/digital users should be free to send or not send information about their habits, lifestyles, preferences: insurance tend to encourage the sharing of data, and to adjust costs/premiums on the basis of sharing and lifestyle habits. Therefore the customer/insurance relationship is shifting from the recording of medical data to even sharing lifestyle habits, which can lead the unsuspecting user into hidden forms of control which limit individual freedom on the basis of a predefined "standardisation" of behaviour considered to be "best" (but who should define the standards?; should this not be assessed on a case by case basis?). The same

problem arises in the context of the employment between workers or potential workers and employers.

2.2 Transparency: the ethics of algorithms and network neutrality

One of the most ethically problematic elements of big data, particularly in the context of health applications, consists in the use of algorithms. Massive data collection is generally random and based on the statistical frequency of behaviour, but the selection in the use of data/information, the creation of (non- causal) relationships between information and predictions (i.e. the configuration of likely future scenarios, behaviour, etc.) are built from algorithms, developed by mathematicians and computer scientists. Algorithms calculate on the basis of variables, seeking correlations, outlining predictions.

It is important to introduce some considerations. Selected behaviour is only frequent behaviour: frequency is the key element of statistical survey. With the result that infrequent (isolated or rare) behaviour risks being marginalized in the digital age, with the possibility that people tend, in order to be recognizable in the digital world, to conform to the most common or repeated behaviour in society. The pressure of homologation, conformity of behaviour (as well as the pressure to share) highlights the reduction of the space for freedom in the era of big data. Instead, we should make the digital user conscious of the fact that algorithms construct correlations and predictions regarding (mathematically calculated) "probability" that does not coincide with reality (or evidence, causality, unpredictability, which must remain possible and imaginable). Algorithms construct an identity that becomes ever more collective. We speak of group identity. It is profiling, which identifies the major and minor probability or propensity to act in certain ways, of certain stratified groups of individuals.

What criteria form the basis on which algorithms are constructed? The ethical importance of transparency in the use of the algorithms used by providers relate to the release and processing of personal data.

An important aspect therefore concerns the full publication of all the factors which research algorithms take into account. Is it acceptable that the trade secret should be extended to cover even the factors that come into play in the algorithm used by the search engine? This question is of ethical importance for at least two reasons. In the first place, only a part of the factors in question are currently in the public domain, encouraging in users the illusory belief that these are, or predominantly are, the factors used. Secondly, network information providers play an increasingly decisive role in the formation of so-called public opinion. However, the opacity of the factors upon which search engines are based does not allow the monitoring of the quality of information and possible manipulation of public opinion itself via the network.

The lack of transparency therefore takes on greater significance on the ethical level when we consider the role of advertising in ordering the results of a network search. Nothing prevents from associating the advertisements that pay more to the most comprehensive websites in terms of information. The opposite - that is, ordering websites by taking

into account advertisements that provide the greatest income to the provider - is ethically untenable.

It is one of the most complex questions, connected with transparency: Who has the power to decide what information is appropriate to be shared and what should be amended, even temporarily? There are opposing views on the matter. Some believe that a certain level of supervision is necessary for any computer platform, if you want it to play a positive role in society. Others believe that it is tangibly impracticable and cite the illegal activities of hackers. But they also add that if there is a central organization or interest or pressure groups that establish or promote the release of information, then there is the risk of non-transparent information, controlled by the ideas and ideologies of those taking such decisions and this is true no matter how transparent or neutral the actual platforms may be. These concerns, growing in non-democratic political regimes, lead to the belief that data maintained over time constitute a "control" system by society to the powers that be, even in the face of negative consequences (security threats, scarce protection of privacy, the interests of organizations, etc.). The more extensive the documentation is, the greater the possibility of obtaining exhaustive information, making conscious choices, informing future generations.

The latter thesis has not to date been accepted among governments and Western societies, concerned about the risks involved with deficient information security. It follows that, it is possible to note the investment of resources increasingly aimed at improving the protection of data and documents.

2.3 Truthfulness and quality of information: possible bioethical implications

Some IT phenomena show the problematic nature of truthfulness and the quality of information, highlighting the "opacity" of certain technologies. Examples are the information bubble and the hidden factors within the framework of search engines, which can have negative health implications.

Search engines are services that enable the identification of websites of interest to the user, in exchange for profiling the actual user[6]. These search algorithms are the subject of debate within the scientific community and beyond. In particular, their properties generate at least two[7] fundamental problems:

[6] There is a search engine that does not track our data, that is, which does not commercially exploit our input, differently from what , for example, Google does. It is a search engine (https://duckduckgo.com) already available online and immediately available to the citizen browser; for more information on this, see the article published in http://www.fastweb.it/web-e-digital/duckduckgo-il-motore-di-ricerca-che-tutela-la-privacy, dedicated to the operational aspect of the search engine and its history. Duckduckgo.com is an interesting and concrete reality on which to reflect, a reality that is growing, which is not a niche (something like 10 million daily searches). It could be a temporary remedy offered to citizens for better protection of their privacy and their browsing, an easy remedy to apply, with an immediate impact.

[7] Instead a third effect is not univocally confirmed known as googlearcy or googlocracy. According to some scholars, the *PageRank* would produce a *power-law* distribution of information: the pages with high rank would be more likely to be visited, creating a vicious

Information bubble

Through the search algorithm used by providers and the properties of social networks, users are progressively separated from information that contrasts with their point of view and are intellectually isolated in their "information bubble". Someone searching on the internet for "BP" obtains information on the investments of British Petroleum, while someone else may obtain information on the disaster of the Deepwater Horizon of 2010 also known as BP disaster. The web pages can also be very different from each other. The information bubble works as a "personal" ecosystem or as an "ideological"[8] frame. It is potentially harmful for the individual and for society, restricting the spread of counter-arguments, rebuttals, evidence of opinions and accepted hypotheses. Since one of the algorithm filters is the personal characteristics of users, they end up being trapped in an information bubble. One could speculate that the "weakest" individuals are more prone to this effect because their searches on search engines can be used/exploited for commercial purposes, that is, for advertising goods to them to compensate or solve their "difficulties". These may be “difficulties" of every kind: affective and relational deficiencies, diseases, economic poverty, etc. In this case, the "weak" are those who (i) have such difficulties and who (ii) have less information or fewer computer skills or less computer malice, i.e. teenagers, the elderly, adult users who have started using the internet and social networks, without prior training.

Hidden factors

According to some sources, the pages at the top of the ranking are those which associate advertising from which the company receives the most money[9]. These affirmations have not been denied.

PageRank is transparent, but there is a list of criteria that IT companies will take into account[10] that also contains hundreds of factors. This list is not official. Some specialists in the field of search engines have developed a hypothetical list based on their own experience and on empirical data[11]. Officially, IT companies merely declare to take into consideration factors in the ordering of pages, but they do not publish the algorithm, as it is a trade secret. The user therefore does not know how

---

circle, i.e. boosting the popularity of the most popular sites. The topic is controversial in reality. According to other scholars, the use of search engines could even have an egalitarian effect, when compared with a random search algorithm on the web or with the research done by users starting with known sites.

[8] *In The Filter Bubble* (E. Pariser, *Il filtro. Quello che internet nasconde*, Il Saggiatore, Milan 2012) we observe how, through filters, " the creators of customization offer us a made to measure world, every aspect of which corresponds perfectly to our tastes. It is a reassuring way, populated by our people, things and favourite ideas " (E. Pariser, *Il filtro*, p. 16). According to the author, filter bubbles harm society because they make people more vulnerable and exposed to propaganda and manipulation.

[9] See, for general explanations and detail, respectively: https://support.google.com/adwords/answer/2497976?hl=en&ref_topic=3121763 and https://support.google.com/adwords/answer/1752122

[10] See the list by following the link http://www.searchenginejournal.com/infographic-googles-200-ranking-factors/64316/).

[11] An example of a study performed to identify the factors and the relative importance is reported in https://moz.com/search-ranking-factors. Every two years or so, Moz carries out an investigation to identify the most important factors influencing research in https://moz.com/search-ranking-factors network. A more precise study on the time scale is reported in http://www.cnet.com/news/testing-googles-panda-algorithm-cnet-analysis/.

these data are used and aggregated. We only know that PageRank is one of these factors.

What are the bioethical implications of these critical issues? Think of a sick person searching for cures through these search engines. This allows the search engine to gather this input and customize the future online browsing of the sick person (i.e. the dynamics of the information bubble), forcing him (i) to think and mull over the illness every time he browses the internet (ii) display advertisements of unsubstantiated treatments; (Iii) lead to the increased belief in the reliability of these adverts ("I saw it on the Internet!" , "Dr. .... who also has a personal website with testimonials from the cured smiling patients!", "If this announcement is so recurrent, it must be reliable") with the possibility of renouncing to the care channels close to him that are, above all, consolidated (e.g. general practitioner, pharmacist, emergency department, etc.). This mechanism can also be found in other particularly " weak" figures, as previously outlined. In summary, the "weakest" can get into a vicious circle fuelled by their "difficulties", but accelerated by indexation for commercial purpose (big data) that search engines and social networking use. The information bubble becomes a kind of (well hidden) trap for those who are "weakest".

Consider then that 72% of people who use the Internet, use this tool for biomedical information[12], but unfortunately the number, variety, and impact of biomedical "scams" is rather staggering[13]. It is not just about therapeutic scams - which represent a large subset of misinformation in the biomedical field - but also myths and conspiracy theories, pharmaceutical "discoveries" that have been proven to be outright frauds; fallacies in diagnostic reasoning and identification of apparent diseases; false information concerning the correlation between existing diseases or on prevention methods - foremost among all being vaccines; crusades against official therapies (in the case of chemotherapy, against which often healers and charlatans are active).

The easy money made from bogus therapies and useless, if not dangerous, practices, are not apparently the only reason for the prompt and broad dissemination of misinformation in the medical field (which apparently has an ancient history[14]). Some properties of large communication technologies facilitate the dissemination of scams. The quality of the information in circulation, upon which public health is dependent, depends largely on the properties of the technological instruments at our disposal. One, alarming proof: the impact of the anti-vaccine movement measured by the cumulative number of new cases of measles per month in the USA, for each year from 2001 to 2014. According to CDC data, last year alone, there were 644 new cases of measles in the 27 states of the Union. This is the largest number of cases

[12] Cf. Http://slideplayer.it/slide/3649692/.
[13] http://medbunker.blogspot.it/;
[14] Salvatore Casillo, Federico Di Trocchio, Salvatore Sica, Falsi giornalistici. Finti paletta e bufale Quotidiane, Guida, Milan 1997.

ever seen for over a quarter century[15]. Vigilance is needed on information tools to protect the quality of information and, ultimately, public health[16].

2.4 Addiction: a further bioethical implication

A critical issue of evident bioethical importance is the fact that ICT can also create various forms of addiction. There is talk about Internet Addiction Disorder (IAD). In the scientific community there is substantial convergence in the recognition that internet addiction has negative repercussions on an individual's life; above all, the relational dimension of life is affected, as it is strongly compressed and actually hinders the real conditions of everyday life, from work to family, to being generally more present in society. It is more problematic to establish whether these certainly negative effects represent a real disorder, comparable for example to drug addiction. In this regard, it should be noted that the latest edition of the Diagnostic and Statistical Manual of Mental Disorders (DSM-V) does not include Internet Addiction Disorder within the diagnostic category of behavioural addictions, suggesting therefore that at present there is insufficient evidence about it. Internet Gaming Disorder, has, however, been included with the specification that it is still necessary to develop additional research to determine whether it can be considered in all respects a pathological disorder.

The fact is that up to a certain point the negative effects of compulsive Internet use were assessed in relation to specific activities such as online pornography and gambling; subsequently it has been suggested that these effects also affect uncontrolled browsing in general, carried out in the most diverse contexts[17]. There are seven symptoms that may indicate some form of disorder linked to the use of the internet: personal satisfaction derived from the time spent web browsing, little interest in other activities, anxiety and depression when without access to the

[15] Data from http://www.gravita-zero.org/2015/01/vaccini-negazionisti-movimento-antivaccini.html.

[16] In confirmation of the above, on 09.10.2016 we carried out a review of the results that emerge from the Google search engine by typing the combination " vaccine/autism." The resulting data are certainly interesting (and worrying). Considering that the first ten sites resulting from the combined research of both terms, one can argue that five dismiss any justification for the alleged correlation between vaccination and the onset of autism; three instead are openly opposed to vaccination, they use a highly polemical and alarmist tone, and allude to the existence of possible conspiracies, as such obviously not verifiable; two sites instead remain on a more descriptive level, reporting of some cases in the news. It may be reassuring that the majority presence in the top ten, well-documented sites recommend the use of vaccination, based on proven scientific research and the reference to significant epidemiological data; however it is disconcerting to discover that the three anti-vaccination sites are respectively placed in second, third and fourth place, therefore in the most immediate positions, ready to be clicked. Of course, these sites omit to recall that "the scientific publications that supported a causal link between vaccination and onset of autism have been reprocessed and (...) the lead author of this theories has been convicted of fraud" (National Bioethics Committee , *The importance of vaccinations*, the motion of April 24, 2015).

[17] Cf. K.W. Müller et al., *A Hidden Type of Internet Addiction? Intense and Addictive Use of Social Networking Sites in Adolescents*, "Computers in Human Behavior", 2016, 55, pp. 172-177; K. Yung et al., *Internet Addiction Disorder and Problematic Use of Google Glass ™ in Patient Treated at a Residential Substance Abuse Treatment Program*, "Addictive Behaviors", 2015, 41, pp. 58-60.

network, urgent need to control events on the web, increasing frequency of use of the internet compared to usual habits, long connection times and network usage even in the event of concrete work and social impediments.

Five profiles have been detected according to the addiction: cyber-sexual addiction (related to pornography), net-compulsion (gambling and shopping), information overload (frantic search for information), cyber-relations addiction (social networking abuse) and computer addiction (excessive use of online games).

2.5 Participatory Justice

Another issue worthy of mention is that of the access to these technologies. There is, today, a "digital divide" because of age, socio-economic status, and geographical area: the elderly, the less educated, the inhabitants of developing countries are the most vulnerable in the digital age.

Given the positive elements of being connected to the internet, equal access should be guaranteed, allowing everyone to acquire the tools, knowledge, skills and motivation to use new information technologies in order to participate democratically within the global society and not be marginalized from the network. At the same time, there must be guarantees - at least temporarily, pending the implementation of technology – of an alternative access to services (especially in the health sector) to people or groups who have neither the technologies nor the skills to use them. The objective should be to enable everyone to participate according to the principle of equality, equal opportunities and non-discrimination.

What needs to be avoided is the so called "two-speed medical system": fast for those who have new technologies at their disposal and slow for those who can not join in. Together with equal access, there should also be equality in educating to access ICT in a conscious and critical manner in relation to emerging ethical issues. Furthermore, the positive results of ICT use for health should be shared by everyone, according to the increasingly consolidated principle in global bioethics of "benefit sharing".

There should, therefore, be implementation of the instruments which stimulate users to take part in digital initiatives that provide new opportunities for comparison, sharing, and knowledge. Think of the new platforms created to allow the subjects participating in trials to be constantly updated on the progress of research; to platforms developed to allow sharing among patients, especially useful and valuable in the sphere of rare diseases.

2.6 Governance

ICTs and big data have therefore made problematic concepts like, privacy, self-determination, informed consent and, in the final analysis, also individual rights, as known and treated, until now. This is why the protection of security and privacy (understood, as mentioned, in a broader sense) should be a shared responsibility between users, companies, and

institutions. There is debate about whether IT companies in addition to contending the hosting of genomic data[18], should put in place effective tools which can enable users to gain awareness; there is debate on the importance of institutions to plan effective governance in this area. It will be specifically up to the latter to exploit these possibilities properly in full awareness that, in the face of accumulation of data, non-use results in a loss of privacy and security. Moreover, it is known to computer scientists that the so-called "delete" key does not guarantee the loss of files, e-mails and messages, which can be recovered very easily (data persistence). This digital knowledge of any citizen, carrying out public or professional activities, can and may produce significant consequences within society. The documented past of citizens can be recovered and used to influence their image in the workplace and in everyday life.

The context so far briefly described is already, in itself, sufficient in order to grasp why the governance and regulation of data collection and related storage procedures are destined to significantly affect not only the protection of individuals and groups, but also the interests of those who are intent on economically exploiting such information. Certainly the facilities which organize large data centres, involved in concentrating the space of the information, will be protected, although the logic of centralization makes these data centres very attractive targets for the perpetrators of data theft. In fact, if the information is of commercial value for businesses, if it becomes a bargaining chip between them and partly between enterprises and customers, it is obvious that this information is also sought-after by those who are motivated by the desire to obtain an illegal profit, that is, in a different context, such as the political one, it is a tool that enables outright cyber war.

Therefore, there should be a strengthening of data protection mechanisms and defence of their systems from hackers. However, in the face of a common will, in all countries where the digital economy has gained ground, to regulate precisely this, illegitimate access to data, on the other hand there is a noticeable difficulty in defining the rules governing this matter. We are in a borderline area where, the security needs of individuals, the lobbying interests of sector enterprises, the will of States to guarantee an efficient and secure information ecosystem, all intersect. The balancing of these conflicting requirements, in the global international scene, is achieved with different perspectives in account of the different way to consider and relate the data once as merchandise then as parts of the personality, and also in consideration of the different forms of government, which have an impact on greater or lesser degree of control and protection of personal data (think of repressive models in different parts of the world). However, the sharing of the interests involved may well enable to initiate dialogue on these needs between the various regulatory models, in order to facilitate convergence towards shared solutions. Convergent solutions are increasingly necessary given the globalization of information and inevitable "trans-border" transfer of information.

[18] J.T. Wilbanks, E. J. Topol, *Stop the Privatization of Health Data. Tech Giants Moving into May Widen Health Inequalities Research and Harm, Unless People Can Access and Share Their data*, "Nature", 2016, 535 (7612), pp. 21-7.

However, greater attention to the virtual community is now spreading among technology companies; this attention is reflected in the tendency that all online products and services provide for the user's acceptance of terms and conditions in accordance with contractual guidelines. Even legislators increasingly feel the need to support the assertion of the centrality of consent by establishing specific authorities endowed with analytical and control abilities, which the individual user lacks, and which are capable of influencing the policies adopted by ICT enterprises. But the fact remains that, notwithstanding these efforts in favour of user guarantees, the citizen must be well aware that protecting a person whose data end up on the Web is very difficult, due to lack of effective tools and the fact that protection is mainly in the user's own hands, at the moment of assessing the quality of the product, but also the ease with which companies enable monitoring and guarantee confidentiality.

The difficulty in regulating the matter should not lead the legislator to renounce his duties: drawing up norms to safeguard not only the protection of personal data (confidentiality, discretion, privacy)[19], but also personal freedom[20] with appropriate anti-discrimination laws, which permit to exercise proper supervision of the "social risks" of new technologies. There is a particular requirement for regulatory instruments to punish the misuse of personal data and information on the private life of users or the publicizing of unauthorized computer materials for denigrating purposes; punishing the intentional use of algorithms that on a purely predictive level (compared to habits and behaviours) produce as a result the marginalization of "minority" categories with social stigma.

3. Recommendations

In light of the above considerations, the CNB intends to underline that in the era of big data the problem consists not so much in the use of data, but in the "appropriate" use of data for the good of mankind and health. To this end, the CNB therefore makes the following recommendations:

to Identify and define the responsibility of providers, especially in certain circumstances, in which there are special social conditions of risk: this responsibility should not be restricted to the declaration related to the commercial use of personal data, but it should be extended to review the quality of data and the transparency of search engine algorithms; committing the authorities for information and communication to proper monitoring;

to identify efficient instruments to obtain consent or withhold consent to the processing of user data, based on synthetic and easily readable information about the type of data and method of collection, the purposes for which they are used as well as the related procedures for processing

[19] This is the approach promoted in the document F. Caldicott (ed.), *Information: to Share or not to Share? The Information Governance Review,* March 2013. It underlines the need, in the context of health, to balance the need for privacy with the need for information sharing between doctors and healthcare workers in the interest of the patient and public health.

[20] C. Bock, *Preserve Personal Freedom in Networked Societies. Broad Anti-Discrimination Laws and Practices could Compensate for Failing Data Protection and Technology-Linked Loss of Privacy,* "Nature", 2016, 537 (7618), p. 9.

and analysis. Should such information not be provided, the user must, in any case, explicitly demonstrate his/her awareness of the limits to privacy, the possibility of re-identification, the possible uses including commercial use of data;

to implement effective recognition of the right to be forgotten, establishing through clear and transparent procedures the possibility for the data subject to request deletion of personal data, so that these are no longer accessible to the public under any form (copy or reproduction);

to promote press campaigns, advertising campaigns (e.g. Public Information films), and educational programmes on the functioning of social technologies that handle information between users or between users and managers. The aim is to actively involve users and allow for critical awareness of the emerging ethical issues of new technologies, especially for particularly vulnerable persons, as well as making them aware of possible risks in the networking and sharing of information;

to urge public healthcare institutions at various levels, to prepare and to keep updated an information website, on which citizens may find confirmation or official denial of the accuracy and quality of medical news[21];

to urge the Ministry of Education to draw up and distribute in schools Guidelines for proper use of social technologies. We must foster the emergence of a new "netiquette"[22], which prescribes socially and psychologically sustainable use, ethical awareness of the risks of the Internet and social networks, with a special emphasis on health-related issues. One should from the earliest years of life, especially with the help of parents and school systems, highlight the need to protect the confidentiality of certain information and the means of defending one's own virtual privacy. An education to active citizenship, which aims to be appropriate to the times (a kind of civic education 2.0.) can in no way underestimate the importance of these issues. Consequently the recommendation for the setting up of educational programs that enable users to develop this awareness in the context of a technical culture on the use of the internet[23];

to support research for innovation in the ethical approach to the design of social technologies. So far, ethics in ICT has essentially been confined to the protection of privacy. But as we have seen, this is just one of the ethical problems that social technologies present. Investment is needed for research on bioethically compatible systems. For example, in order to curb the phenomenon of addiction, it is possible to imagine automated alerting systems to alert the user of having crossed a critical threshold in connection time. Even the automatic offer of self-assessment tools, to be administered prior to establishing the connection (a kind of health cookie) could make users more aware of the risks they run;

[21] The Italian National Institute of Health is certainly moving in this direction by setting up a so-called *Knowledge Portal*, which will be available shortly.

[22] The term refers to the *network* (net) and *etiquette* (good manners).

[23] It goes without saying that this kind of *Civic Education* 2.0 could also address topics and issues that have a direct bioethical relevance, consistent with what had been called for by the Memorandum of Understanding between the Ministry of Education and the NBC signed on 15.7.2010. This protocol identified in bioethical education, to be promoted within the school system, one possible exemplification of the more general training devoted to *Citizenship and Constitution*.

to guarantee conditions for access to all those who intend to make use of new technologies, and at the same time guarantee the rights of those who can not/do not want to connect, specifically as regards access to health services for citizens.

Urging discipline for the protection of personal data (based on the protection of privacy and confidentiality, minimization of the use of sensitive data, justification and proportionality of collection, the responsibility of those who use the data); urging also the adoption of regulations aimed at providing adequate anti-discrimination laws, which help to avoid or at least mitigate the social risks of misuse of virtual data: the aim is to protect, not only personal data, but above all the personal freedom of citizens.

Annex: Legal note

In Italy the processing of personal data is protected first by law 675 of 31 December 1996 "Protection of persons and other subjects regarding the processing of personal data", later repealed under art.183, paragraph 1, letter a) subsequent legislative decree no. 196 of 30 June 2003 ("Code regarding the protection of personal data") currently in force. According to the Code the processing of personal data should be based on principles of fairness, legality and transparency and protection of privacy and the rights of those providing them.

Significant changes to the legislation were made by the legislature with D.L. 69/2012 on implementation of the 2009/136/EC directives on processing of personal data and protection of privacy in the electronic communications sector, and the EC Regulation n. No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection. A series of changes that are contextualized in the more general view of the dynamics inherent in the movement of personal data and their exploitation for commercial purposes, in the light of the emerging reform policies in this area both in Europe and in different parts of the world. Specifically, the two central themes at issue in the D.L. are the profiling of users while browsing online, and the management of data breach events and this is because of the growing importance of the predictive key assumed by information, and in particular by personal information, in the most advanced economies.

The Italian Data Protection Authority enacted measures: n. 229 of 8 May 2014 relating to the "identification of simplified procedures for information and the acquisition of consent for the use of cookies" and n. 353 of July 10, 2014 against Google Inc. on the "compliance with the Code of processing of personal data carried out under the new privacy policy"; March 19, 2015 the "Guidelines concerning the processing of personal data for profiling online"[24].

The Guarantor ruled that the network service provider (search engines, email, social networks, cloud, online payments, statistics and visitor tracking website analysis, etc.) shall not use data for profiling purposes, without the consent of the user, and that this activity for

[24] Published in the Official Gazette of May 6, 2015 (Guidelines) See the website: http://www.portolano.it/pcc_newsletters/profilazione-online-le-linee-guida-del-garante-privacy/.

commercial purposes must be explicitly declared. This is the first measure of its kind in Europe, it emerged as part of a coordinated action with other European authorities and following the ruling of the European Court of Justice on the right to be forgotten. In summary, the Guidelines are intended to ensure that all providers of information society services, as well as all those who offer their users online services accessible to the public through electronic communications networks, with specific regard to the processing of personal data relating to the use of the features offered, taking into account in particular: - the information given to those concerned in art. 13 of the Code and as set out in paragraph 3 of these Guidelines; - the prior consent of users and information about them, even deriving from processing, in automated mode, of the personal details of users authenticated in relation to the use of the transmission and reception of e-mail messages service; - the respect of the right of objection provided for in Article. 7 of the Code; - the adoption of a data retention policy compliant with the purposes of art. 11 of the Code.[25]

As part of the processing of sensitive data at European level (although not specifically related to big data) we must remember Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data, subsequently repealed by Commission Regulation (EU) 2016/679 of the European Parliament and of the Council on 27 April 2016[26] (which will be described below) and Directive 2002/58/EC of the Parliament European Parliament and Council on 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, then amended by Directive 2009/136.

Among the most significant documents on the subject adopted by the Council of Europe are: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, 1981 and additional protocol (Additional Protocol to Convention ETS No.108 on Supervisory Authorities and Transborder Data Flows); Recommendation CM/Rec (2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010); Recommendation CM/Rec (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010); Recommendation CM/Rec (2012)4 on the protection of human rights with regard to social networking services; Recommendation CM/Rec (2014)6 on human rights for Internet users; Recommendation CM/Rec (2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality.

[25] For an illustration of the Guidelines and the required measures see http://www.diritto24.ilsole24ore.com/art/guidaAlDiritto/dirittoCivile/2014-07-21/google-garante-trasparenza-profilazione-125008.php?refresh_ce= 1.

[26] European Parliament, EU Council. Regulation (EU) 2016/679 of the European Parliament and of the Council, on 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (general Regulation on data protection). Official Journal of the European Union May 4, 2016, L119: 1-88.

It should also be noted that, the European Union Court of Justice[27] has recently invalidated a previous decision of the European Commission (2000/520/EC), which ascertained adequate protection for privacy even of personal data transferred to the United States (so-called Safe Harbour system). Obstructing de facto national authorities verifying the level of security guaranteed to data overseas and failing to provide any mechanism for updating the Safe Harbor criteria, the decision of the Commission in 2000 was deemed to be detrimental to the essential content of the right to respect for private life, allowing, for example, US public authorities access across the board to the content of electronic communications transferred there, even for profiling purposes. By so doing the Court of Justice has given back to individual national authorities the power to judge the appropriateness of the security levels of transferred data, inviting, at least implicitly, the Commission to renegotiate the agreement on the transfer of data. More recently on July 12, 2016 the European Commission adopted an agreement to safeguard "the fundamental rights of any person in the EU whose personal data are transferred to the United States" and bring about "legal clarity to companies operating transatlantic data transfers". In the EU-US shield for privacy, there have been some specific provisions included on the subject of health data[28.]

Finally, the processing of personal data has drawn the attention of the European Parliament and the Court of Justice also with regard to the protection of natural persons as to the processing of personal data in the course of investigations and detection of crimes and on the free movement of such data. In particular, both the (EU) Directive 2016/680[29] issued by the European Parliament and the Council on 27 April 2016, and the aforementioned (EU) Regulation 2016/679[30] issued on the same date, place at the basis of protection of the parties concerned, i.e. those referred to by the personal information, "the data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which (...) significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject (...)" (art. 38 Directive).

While Directive 2016/680 relates specifically to the processing of personal data by competent authorities for the prevention, investigation, detection and prosecution of criminal offenses or the execution of criminal sanctions, Regulation 2016/679 is of great importance for information and communication technologies because, among other things, it provides the basis for the exercise of new rights and defines limits with regard to the automatic processing of personal data.

---

[27] Judgment of 6 October 2015, Case C-362/14, Maximillian Schrems / Data Protection Commissioner.

[28] Cf. Http://europa.eu/rapid/press-release_IP-16-2461_it.html.

[29] European Parliament, the EU Council. (EU) Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offenses or execution of criminal penalties, and the free movement of such data, and repealing framework decision 2008/977 / JHA. Official Journal of the European Union on May 4, 2016; L191: 89-131.

[30] http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT

The Regulation states that the persons involved in the processing of personal data should be informed of their right to revoke consent to certain processing, including, for example, processing for the purpose of direct marketing. It also stipulates that Internet service providers and social media should seek the consent of the parents or those exercising parental authority prior to the processing of personal information of children under 16 years of age.

Particularly significant in the context of social technologies is the right to "be forgotten" provided for in the Regulations: the interested parties may obtain the cancellation of their personal data, even online, by the data controller on fulfillment of the following conditions: if the data are processed only on the basis of consent; if the data are no longer required for the purposes for which they were collected; if the data are processed unlawfully; or if the person concerned legitimately opposes their being processed. Along with the "right to be forgotten" is, the obligation of the data controller, publisher of the data, to communicate the cancellation request to all recipients processing them, as far as is technically possible. According to the Regulation, the "right to be forgotten" can only be restricted in some specific cases: for example, to guarantee the exercise of freedom of expression or the right to defence in court; to protect a public interest (e.g. public health); or when data, made anonymous, are needed for research.

Furthermore, the Regulation introduces the "right to portability" of one's personal data to transfer from one data controller to another. For example, changing email provider without losing one’s contacts and saved messages.

The Regulation confirms the transfer ban on personal data to countries located outside the European Union or to international organizations that do not meet the required adequacy standards on data protection, in relation to which the Regulation introduces more stringent evaluation criteria.

Also significant for information and communication technologies is the principle of "privacy by design", whereby it is necessary to ensure data protection right from the initial stage of conception and design of a process or of a system.

.