Internet and criminal responsibility in cybercrime. The security breach

Maria Rita Tarola

Graduated in Law, Mediator, Criminologist, I Level Master in Criminology at "La Sapienza" University of Rome and II Level Master in Criminology and Security at UNINT, University of International Studies of Rome, Italy

ABSTRACT

This present work intends to outline an area of criminology regarding the support of investigative approach aimed to the suppression of cybercrime, known as negative and criminal interference in the context of daily social living. In the presence of more and more impetuous modern evolutions that characterize the information field, in the technical sense, and also in accordance with an industry profile. Aiming for the most part to identify solutions, in the various events experienced by the victims themselves, in assessing how much they are willing to grant and sacrifice, in view of obtaining the fairest counterbalanced advantage or claiming what is criminalized, to the drawbacks. An arduous evaluation study of the delicate balance in the light also of the most recent statistical references, between the need to crack down and that to obtain consensus. To safeguard this need, therefore, also the new regulations that, in step with evolution express and regulate the discomfort achieved with the new methodological approaches. If it is true that an evolution of the times makes information less high, due to the growth of interferences and redundancies, it is also true that this has a negative implication that we have to more regulate a better guarantee of what always constitutes respect for data security, if the lack of this, can determine the limit to want to obtain, making it now more than ever with the recent implementation of GDPR 676/2016, through the duty to repress.

RIASSUNTO

Il presente lavoro si propone di mettere in rilievo il potere della criminologia nei suoi vari campi di azione, in particolare quello di supportare un approccio investigativo mirato alla repressione del cybercrime, inteso quale negativa e criminosa interferenza nel contesto del quotidiano social vivere. Al cospetto delle sempre più impetuose evoluzioni moderne che caratterizzano il campo dell'informazione, intese in senso tecnico e anche secondo un profilo di settore. Mirando perlopiù ad individuare soluzioni, nei vari atteggiamenti vissuti dalle stesse vittime colpite, nella valutazione di quanto esse stesse siano disposte a concedere e sacrificare, in prospettiva di ottenere il più equo controbilanciato vantaggio o di reclamare quanto di troppo risulta criminosamente carpito, invece, a tutto svantaggio. Un arduo studio di valutazione del delicato equilibrio, alla luce anche dei più recenti riferimenti statistici, tra il dover reprimere e il voler consensualmente ottenere. A salvaguardia di questa esigenza quindi anche le nuove normative che al passo con l'evoluzione, esprimono e regolano il disagio realizzatosi con i nuovi approcci metodologici. Se è vero che un'evoluzione dei tempi rende un'informazione meno elevata dovuta alla crescita delle interferenze e ridondanze, è pur vero che ciò ha un risvolto negativo che va maggiormente regolato a miglior garanzia di ciò che costituisce pur sempre rispetto della sicurezza dei dati, qualora la mancanza di questa, possa determinare il limite al voler ottenere, realizzandolo ora più che mai con l'attuazione recente del GDPR 676/2016, attraverso il dovere di reprimere.

RESUMEN

El presente trabajo tiene como objetivo poner en evidencia el poder de la criminología en sus varios campos de acción y, en especial, la criminología como apoyo a la investigación contra la represión del *Cybercrime* entendido como la interferencia negativa y criminal en el contexto de la cotidianidad social; vistas las crecientes evoluciones modernas, ya sean en sentido técnico y según un perfil de sector, que están caracterizando el campo de la información. Intentando individuar soluciones, en los varios comportamientos vividos por las víctimas, valorando cuánto estas estén dispuestas a conceder o a sacrificar, con el objetivo de obtener la ventaja más justa o de reclamar, aunque sea a su desventaja, lo que resulte criminalmente robado. Un estudio arduo de valoración de este delicado equilibrio, a la luz de las recientes referencias estadísticas, entre el deber de reprimir y el querer consensualmente obtener. Como salvaguardia de esta exigencia las nuevas normativas, que al paso con la evolución, expresan y regulan el malestar que conllevan las nuevas propuestas metodológicas. Si es cierto que una evolución de los tiempos supone una información menos elevada debida al aumento de las interferencias y redundancias, es aun más cierto que esto implica un resultado negativo que ha de ser regulado para garantizar el respeto de la seguridad de datos. La falta de esta determinará el límite al querer obtener, realizándolo, ahora más que nunca, con la actuación reciente del GDPR 676/2016, a través del deber de reprimir.

Cybernetics

Historical notes and meaning

It is important to emphasize the meaning of cybercrime, with which we intend the crime referring to a very specific context or that of the "Kiber" (the Greek root), which stands for "rudder". Metaphorically we will therefore have to refer to a "guiding one" who "governs", as in Plato's Greece, as in the art of governing a City or a State. In this sense and from this starting point we must refer to the modern term of technology and computer science, making reference to the meaning that comes from elements of automation and control, typical of most modern technology.

We see the first approach to the subject with Wiener[1], even if similar ideas had already been registered by Morse with the telephone and by Marconi with the radio.

In this context the importance that is given to information for the first time is important**,** as an interaction with the outside world in the provision of data, whose cognition and in the individual, determines an experience that memorizes, guides and controls human behavior projecting it into the future. It is precisely on this basis and on this analogy that we approach a unified study of animals and machines, from the point of view of the theory of the automatic control of communication and automatic calculation: with this new field of investigation, we can fix a considerable interest in the observation of the mechanism that started the machinery, so as to allow the reasoning and the calculation of the solution therefore. It is with the study of this phenomenon that we create the need to build machinery able to replace human beings for these functions. A real theory of automatic control begins, like human beings, applied to technology, which bases its debut on the regulation of the functioning of steam engines.

To examine the concept, we have to reference the so-called *retroactivity*, a dynamic system which is able to consider the results of the system, to modify the characteristics of the system itself, or extending its status, moving it in this case to a new point of equilibrium, or preventing a strong deviation from the base equilibrium point. It is studying this interaction that the behavioral comparison between animal and machine determines high techno based logical solutions. Solutions which are tried again and theorized by von Neumann[2] in 1957 inspired by Weiner and developed later in a unitary theory of the brain and calculating machines.

From calculating machines to the computer

Based on the electronic calculator, the structure of the modern computer evolves from that of wired devices, characterized by the presence of physical cables for connections, not programmable through software programs that would allow to update use without the replacement of components. From this technical evolution the information data is generated by electrical impulses in the presence or the absence of electrical current corresponding to only two numbers, considered as a unit of information: the zero and the one. Corresponding to False and True, called Bit (binary digit)[3]. In order to function, the computer must operate through an algorithm that constitutes the set of actions, instructions, commands, considered in the sequence.

These electrical impulses acting on the physical structure of the machinery, the hardware, put into operation a series of commands and instructions of the algorithm adopting a function made possible through the adaptation of the software program to the physical structure of the machinery, so that these can do their programmable functions. The effective executor of the elaboration, the "brain", is called the processor or the microprocessor or CPU *Central Processing Unit*.

John von Neumann proposed the logical model of what was to be a modern computer provided with CPU, a memory, an input and output device.

Data is stored in the memory that can be central or primary and mass or secondary. The central is the fast memory (of work) and the mass memory is the permanent memory. The technological evolution, having allowed an extreme miniaturization of the hardware components of the processors, has determined the passage from the extremely cumbersome electromechanical calculators to the modern personal computers.

Only in the early seventies, microcomputers or computers that were not cumbersome began to be made and at an accessible cost. Followed by home computers for domestic use.

Information

A proper reference must be made in this context to the concept of *entropy* and how this can be explained through the activity of the electronic calculator and then through the computer in providing information.

The necessity which we discussed above. If we consider entropy according to Shannon's theory[4] as the information contained in event x emitted by source X, according to a degree of probability, this event can happen and we observe that the more the event is probable, the more the information rendered is small, while on the contrary the more the event is less likely the more the information rendered is great. So that mathematically, information could be defined as the inverse of probability:

$$I(x) = I / P(X)$$

Considering more appropriate to insert a logarithmic function to better express the concept mathematically:

$$x = \log (1 / PX) = - \log PX$$

The basic factor of the logarithm is 2, to balance unit information, that is to bit (0,1) (two digits only) necessary to represent it. Say for example then for an event that has a certain probability happening the signal consists of a certain number of pulses expressed in electronic impulses (bits).

Being that in physics[5] "it is tradition to measure not order, but disorder, and the measure of disorder is given by the positive logarithm of probability". This positive measure of disorder is nothing else but entropy which also represents the second law of thermodynamics, which states that in an isolated system the probability of the event decreasing is zero. The more likely the event is to happen the more the information rendered is small.

This concept that with Shannon assumed a purely mathematical role with Wiener was covered by the concept of information feedback (*retroactivity)*, whereas Shannon admitted the existence of error and implied the imprecision of the message.

It was understood, however, that using a larger number of symbols (expressed in binary digits), even though redundant, could transmit relatively more precise information, indicating the presence

---

[1] Norbert Weiner: American Mathematical and Statistical Studies (1894-1964). Famous for research on the calculation of probabilities and for developments in information theory, being recognized as the father of modern cybernetics.

[2] Jon von Neumann: (1903-1957) Hungarian mathematician, physicist and computer scientist.

[3] This storage system using numbers 0 and 1 is called *digital.* It is used to store not only numeric data but also any type of information: words, images, sounds, etc. To convert a number from the decimal system to the binary system, divide the number by 2 and note the rest; then the procedure is repeated with the result of the division and so on until 1 is obtained as a result. The corresponding binary number consists of 1 followed by the list of the remains obtained starting from the last one and arriving at the first one: es calculate the track of the num . dec . 67, 67 : 2 = 33 with remainder of **1,** 33: 2 = 16 with remainder of **1,** .... and then get up to 2: 2 = 1 with the remainder **0.** Then proceed to writing all the remains from right to left, making them precede the number **1**. So that the num . dec.67 converted into a binary digit will be: **1000011**.

[4] Claude Shannon (1916-2001) mathematician, US engineer, father of the digital era.

[5] According to Norbert Wiener in "Introduction to Cybernetics" chapter II Progresso and Entropia pg 36.

of noise or interference. It was understood that to realize a good cyphering algorithm (a perfect cryptographic code), that is able to decipher the transmitted information with maximum precision and security, that had to consider a very long cyphering code that only with a higher and more advanced computing potential technology, could be exploited to build completely secure communication methods.

Progress and communication

From this perspective it becomes clear how the need arises to do research into methodologies that make the realization of new technologies in progress in order to guarantee total safety and in the application and results achieved.

The need for progress is strongly felt, even if we move away from the moment of its maximum expression, the times of the industrial revolution, it still leads us towards that activity of research and adjustment of the right evolution of the times. To achieve the right results as already in Wiener and our reflections, we should anchor ourselves to basic values and select those to be discarded, because they are typical of the era but are only momentary or even traditional and to evolve from that.

Once this distinction has been made it will be possible to lay the foundations for the right innovations on that fertile ground; also it is clear that any evolution will be more rapid and felt if the same society, the same events require its existence. An adequate democratic system provide to it, that also would allow a more rapid result of satisfaction in the transparency of its communications.

A system[6] should be created in which adaptability and variability are regarded as a function of improvement. In other words, also allowing potentially capable individuals, to freely express their contributions in evolution. An evolution that will make way for other dynamic actions that act by making the growth achieved malleable and flexible, which in turn looks at the previous one that is now rigid and has to be replaced or evolved.

The law

One of the problems to face, when the system of regulations is influenced by social development in every sense, is its adaptation to the satisfaction of the new regulatory requirements. That is, the new evolutionary developments leading to new realities, determine a need for further and renewed regularization activities, by means of an appropriate legislation that dictates rules and standards. This involves a wide range of problems[7], among which those related to the general aims of lawmaking and those related to the also renewed techniques in which these new considerations of justice and regularization may actually become operative.

The risk identified is that not always possible to adequately implement this correspondence between the new legal system and the new rules applicable to it, if not awaiting a reasonable time during which the new problems that arise complete their essence, to then be resolved, with technical tools even if evolved but consolidated by the new experiences.

We wanted to offer solutions to this problem that a diligent eye in our times would consider opportune and judicious: first of all we believe that beyond the new legislative provision, what must be taken into consideration by the judge as he deals with new cases and when the matter is not regulated, it is the case in point to be applied even in the absence of a solution that is appropriately regulated, because it already exists. He therefore should be assisted by a competent technical assistant, rather than a legal one, who works with him, in cases where legal competence is not sufficient. When also the behavior of the expert does not coincide with the interests of the party, and his activity depends on the judge and the compensation system is detached from any remuneration from the parties but depends on the Court or "from a fund to which both parties contribute".

In fact, as well as Weiner[8]: "when there is a serious discrepancy between the theory upon which the law is founded and the reality of the concrete situation, there is always a glimmer of injustice" and still[9]: "in modern society the greatest opportunities for a criminal, are in this position of dishonest mediator among the interstices of the law".

Violation of security

Risk analysis

Although it is possible to guess that any violation of security can arise from the possibility of a certain event happening, from the concept of "violation" inevitably, also a reference to something unlawful derives, a context that results as violated. And requires in itself a check that once done allows us to recover the existing state before the violation or which is able to prevent it. Both in recovery and in protection, the objectives of the security of the information resources are considered to be aimed at the purposes of *confidentiality, integrity and availability.*

Meaning that for *confidentiality* or even *privacy*, the prevention of access to information but not specifically to data. Information being a correlation of these: an association of one datum to another, referring to the same element, gives information.

Integrity intends the protection of the alteration of information data or of information resources. Data could also be software or a configuration of the hardware system.

Regarding *availability*, the prevention of the possibility that information or IT resources become inaccessible or not recoverable.

So, from what has been said above, it is possible to further distinguish when the violation depends on an accidental or deliberate impact. By defining *the impact,* as the consequence of the threat, we can see that it is in direct relation with the security objectives highlighted above and with the assets we want to protect, as well as with the concept of risk we are examining. When a threat is still entirely at the potential level, what it essentially highlights is only the risk of an event and its consequences, if more or less serious. This is true in every context when we want to refer to the concept of security[10]. Of course what is also prominent in the risk assessment is the *vulnerability* of the object exposed to security risk. Vulnerability, that in the IT context can be referred to: geographical location, systematic errors in hardware/software, design errors, accidental hardware malfunctions, enabling use by-users.

However, it can be considered that the risk in terms of

6 Wiener "Introduction to Cybernetics " pg 73.
7 Wiener Op.cit. pg 129.
8 Weiner Op.cit. chap VII "Law and communication" pg 136.
9 Weiner Op.cit. cap.VII "law and communication" pg 134.
10 In the field of workplace safety , Legislative Decree 81/2008, *e.g.* companies must make a careful assessment of the risks that may cause damage to health or threaten the safety of workers. Evaluation that must be reported in the **DVR**, Risk Assessment Document. The document must contain: 1) a list of all that has been assessed as risky for safety and health. 2) Tools and criteria for the prevention and protection of personnel. 3) Measures to guarantee greater protection. All this also in a prospective and programmatic vision.

information security is the product between the consequence of an event (*impact*) and the probability that it happens (*threat*):

that is R = G x P, where G = consequence of an event (impact), P = probability of the event happening (threat)[11].

Naturally, one will then have to distinguish if the threats are *accidental or deliberate*[12] and the assets to be protected may be: the company's image, hardware, equipment, software, data and information, paper documents, funds, artifacts and other products or personnel.

For a *deliberate* threat you will have P = f (VM)
where
V = vulnerability / M = motivation of the attacker or threat level

For an *accidental* threat you will have P = f (V, p)
where
V = vulnerability / p = intrinsic probability of event occurrence.

In the IT risk assessment we proceed in two phases: 1) Risk analysis; 2) Risk control.

In the *analysis* we proceed with three operations:

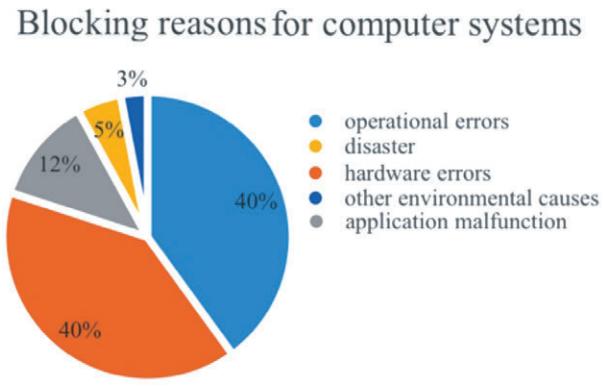
1) Classification of information
2) Identification of threats
3) Identification of the level of risk associated with each class of information identified.

In the risk *control* phase we proceed with establishing the risk management methods related to the loss of a protection objective. For these purposes it is appropriate to use a risk assessment plan according to a model called **PDCA** (Plan, Do, Check, Act), where:
PLAN: Plan, decide what to do, how to do it, in how long
DO: do, do as planned.
CHECK: check, check if you have done everything planned through objective data.
ACT: act, take actions to continuously improve the performance of the processes.

This model can be easily applied to the processes of the *management of information security systems* with the acronym.

GSMS

So a company that has prepared significant interventions to ensure operative continuity will be ready to deal with any disastrous events. But it should be emphasized that among the potentially dangerous events both minor hardware failures and human errors with serious consequences can be identified. Generally, the reasons for a failure of the application systems are: operating errors (40%), hardware errors (40%), application malfunctions (12 %), disasters (5%), other environmental causes (3%).



The management of security systems

As stated above, the techniques to ensure information security have to actually guarantee these essential characteristics:

– the data should be accessible only to authorized persons (confidentiality), and in no way can be disseminated or visible to others (privacy).

ISO/IEC 27001/2017 and Legislative Decree 196/2003 - Data privacy

When we talk about data confidentiality, first what comes to mind is the protection guaranteed to us by Legislative Decree 196/2003. This is also undoubtedly one of the solid points of reference for what concerns the security of information and data in a cybercontext.

However, what concerns the protection of personal data is only one aspect of the protection of privacy in the information technology field.

Internationally there is an ISO /27001 standard that aims to standardize the methods that protect data and information from threats of all kinds and also ensures integrity, confidentiality and availability (the three elements of security).

The company security management system, SGSI can be certified according to the ISO 27001 standard and related updates.

The ISO27001/2017[13], "specifies the requirements to establish, implement, maintain and continuously improve an information security management system (SGSI-document) in the context of the organization. It also includes requirements for the assessment and treatment of information security risks, adapted to the needs of the organization. The requirements included in the standard are generic and intended to be applied to all organizations independent of their type, size or nature".

So the substantial difference between the privacy law and the ISO 27001 standard, is that the Legislative Decree 196/2003 (code Privacy) protects personal data, sensitive or not whereas, the ISO 27001 standard, requires in its specific previsions, that there is this protection according to the afore mentioned decree, but also takes care of the organization's business data in order to safeguard the company's commercial and financial activities.[14]

General Data Protection Regulation - Year 2018

With the coming into force of the *General Data Protection Regulation* (GDPR)[15] (EU Regulation 2016/679) the abrogation of each "minimum measure" has been established, to be understood as a basic rule to respect the known standards of the protection of personal data of the citizen. Therefore also with reference to the data of all European Union citizens and residents of the European Union, both inside and outside the borders of the Union. The complete

[11] That is, the risk becomes very high when, at a high impact, the threat is very likely to occur, while it will be very low if the probability of the threat occurring is very low.

[12] Among the accidental that sometimes could have the characteristic to be deliberated remember: Bombardment, Fire, Weapons, Power failure, Water interruption, Air conditioning interruption, Hardware failure, Software failure, Instability of electric current, Failure of the Network provider, Incorrect use of the Software, Personnel errors, Illegal use of the Software, Malicious Software, Theft.

[13] From the "Summary" of the ISO / IEC 27001/2017 text.

[14] Control A.18.1.4 of the ISO 27001 text provides: "Data and privacy protection must be guaranteed as required by legislation, standards and, if applicable, in contract terms".

[15] EU 2016/679 Regulation of the European Parliament and of the Council - of 27 April 2016 - relating to the protection of individuals with regard to the processing of personal data, as well as the free movement of such data and repealing Directive 95/46/.

effectiveness of the aforementioned document, having been established for May 25, of the current year will provide for the effective abrogation of any legislation concerning the application of minimum standards. With these, therefore the *Code for protection of personal data* will be abrogated with the incompatible ones. A specific reference to automated data processing is provided in art. 2 1c: in which: "this regulation applies to the processing of all or part of automated personal data and to the non-automated processing of personal data contained in an archive or intended to be" and in 3c there is a specific reference to the EC regulation 45/2001 regarding the processing of personal data by institutions, bodies, offices and agencies of the Union. With regard to the level of security protected, it is necessary to deduce a generic abrogation of each minimum measure, replaced with the so-called "risk-adequate measure", therefore established specifically in Article 32 section 2: **security of processing: 1)** "Taking into account the state of the art and implementation costs, as well as the nature, object, context and purpose of the processing, as well as the risk of various probability and seriousness for the rights and freedoms of individuals, the holder of the treatment and the responsible put adequate technical and organizational measures in place to ensure a level of security appropriate to the risk that includes, among others if necessary: 1) *the pseudonymisation*[16] *and the encryption of personal data* 2) the ability to ensure on a permanent basis the confidentiality, integrity and availability and resilience of processing systems and services 3) the ability to promptly recover the availability and access of personal data in case of physical or technical accident 4) a procedure to regularly test, verify and evaluate the effectiveness of technical and organizational measures in order to guarantee the safety of the treatment. **2)** "In evaluating the appropriate level of security, special consideration shall be given to the risks presented by the processing resulting in particular from destruction, loss, modification, unauthorized disclosure or accidental or illegal access to personal data transmitted, stored or otherwise processed".

Therefore, when we appropriately consider the provision of the GDPR regarding risk assessment, it will no longer be sufficient to ensure that it is reduced to a minimum, but it will be necessary to act positively in the manner explained and in the adequacy of the risk and not just by applying the contexts indicated so far in the articles 33 and 34 legislative decree 196/2003.

Protection of personal data: Legislative Decree 196/2003

One of the main objectives of computer security is to guarantee the privacy of users and services, and therefore the confidentiality of personal data related to the user's network activity. All the code regulations already set out above actually aim to a large extent to safeguard the confidentiality of data and information of the user as well as to regulate the offenses, such as criminal offenses given the relevance of the protected object and of the injured interest. A prevention activity, however, is desirable, for the negativity of the implications that may be generated by the realization of the risky event that we want to avoid.

The purpose of the protection of privacy (confidentiality) is to allow anonymity and secrecy and through this function we aim to achieve the typical objectives of efficient prevention, of the risk to which data and information are subjected.

It is dutiful at this point to give a proper definition of *data* as well as *information* since it is the same privacy law in detail to define the "datum", it goes without saying the resulting "information"[17]. However, it is to be noted that the aforementioned privacy legislation will be abrogated or effectively integrated only starting on 25/05/2018, when the GDPR will be fully implemented. Therefore we must emphasize what the additions are as we will also observe in the field of definitions.

Definitions

P*ersonal data*: any information relating to an identified or identifiable natural person, even indirectly, by reference to any other information, including a personal identification number. Ex art. 4 GDRP 676/2016 we will also specify the following: " it is considered identifiable the natural person who can be identified, directly or indirectly, with particular reference to an identifier such as a name, an identification number, location data, an identifier on line, or to one or more characteristic elements of his physical, physiological, genetic, psychic, economic, cultural, or social identity".

Identifying data: the personal data that allows the direct identification of the interested party.

Sensitive data: personal data capable of revealing racial and ethnic origin, religious or philosophical or other beliefs, political opinions, membership of parties, trade unions, religious, philosophical or political associations or organizations or unions, as well as data suitable to reveal the state of health and sexual life. Ex art. 4 GDRP 676/2016, there will be a specification relating to health data to better understand data related to physical health, including the service of health care, which reveals information related to their state of health.

Judicial data: the personal data suitable for revealing measures pursuant to Art. 3 c.1, letters from a) to o) and from r) to u), of Presidential Decree no. 313 dated 14 November 2002 concerning criminal records, records of administrative sanctions depending on the offense and pending charges, or the status of the defendant or the person under investigation, pursuant to art. 60 and 61 of the criminal procedure code.

for *Blocking*, the retention of personal data with temporary suspension of any other processing operation.

Databases: any organized set of personal data, divided into one or more units located in one or more sites.

From Article 4 of the Legislative Decree g) bis, the concept of *Violation of personal data is understood*, meaning by this "a violation of security that also involves the accidental destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed in the context of the provision of a communication service accessible to the public". The addition with the GDPR 676/2016 of the following definitions is

---

The Regulation is an act of European Union law, binding, addressed to all Member States as well as to individuals. According to the art. 288 of the TFEU, (Treaty on the Functioning of the European Union), it has general scope and discipline in an objective manner of abstract situations. The characteristic of the general scope implies that the regulation is applicable to all member states. The regulation being mandatory in all its elements. Once entered into force, that is, it will produce binding effects on all those who are subject to the European Union. Therefore, a Member State can not adopt internal measures which imply a limitation of the rules. The rules of the regulation enter into force without there being an act of transposition of the same by the State (norm *self- executing*).

[16] Pseudonymisation: The processing of personal data in such a way that personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and subject to technical and organizational measures to ensure that such personal data are not attributed to an identified or identifiable natural person. From GDPR: -definitions-.

[17] For information we mean the set of correlated data, with which an idea or a fact acquires a form and is communicated … according to the theory of the database, which adopts a relational model, an information is a relationship between two data. Therefore the distinction between the data (a number, a date, a word) and the meaning that can be given to this data is fundamental, putting it in relation with one or more data. V. also Cap. I prg 1 3.

significant: *genetic data and biometric data,* intending to the former: personal data relating to the hereditary or acquired genetic characteristics of a natural person providing unequivocal information on the physiology or health of that individual, and which result in particular from the analysis of a biological sample of the natural person in question. For biometric data, the personal data obtained from a specific technical treatment related to the physical, physiological or behavioral characteristics of a physical person that allow or confirm the unequivocal identification, such as the facial image, or dactyloscopic data (from the GDPR 676/2016).

The Privacy Guarantor and the GDPR

The Privacy Guarantor is *the* Italian national *supervisory authority*. Each State of the European Union has its own supervisory authority which is responsible for claims management, established by the art. 28 of the EC Directive 95/46 with also the working group pursuant to art. 29 of the same directive. The Privacy Guarantor is therefore an independent administrative authority established by the law on Privacy (l.675/1996) in implementation of the EC directive regulate, today by the Code regarding personal data (Legislative Decree 196/2003) to the extent that this is not abrogated by the GDPR in implementation.

With the new regulation, the supervisory authority intervenes primarily ex post, that is, his assessment is then placed next to that of the data controllers. Therefore, from 25 May the institute of prior notification of treatment, which was in charge of our guarantor, will be abolished, replaced by the obligation to maintain a treatment register and independent assessments. Therefore, the supervisory authority as well as the European Data Protection Committee (which actually replaces the Group referred to in Article 29 of the EC Directive 95/46) will have the task of guaranteeing the correct interpretation of the legislation as held for the first time in adequate risk assessment. In particular, the committee will have the task of producing *guidelines* and guidance documents on the various issues to guarantee the adaptations required by the GDPR regulation, eventually made necessary due to technological development. However, a *prior checking* is expected by the supervisory authority if the treatment is characterized by a very high risk and in the absence of protective measures.

In the event that the company had various locations in the European Union, it would adopt the principle of one stop (*one stop shop*) that provides companies that will have to deal with a single authority of the country where they have registered office. But the principle, thus, exposed has detected difficulties in application because of the fact that it would often contrast with the internal legislation that protects the consumer or individual citizen; also regarding the place of the violation, hence, it was considered appropriate to establish its application only in cases where the company has more than one registered office. In this case the principle of the main office would be applied, better known as "leader", *leading authority.*

Some recent data regarding the amount of security investments in Italian companies in 2018

The fact that the entry into force of the GDPR in 2016, has not marked its full effectiveness, has led most of the Italian companies to extend the adjustment of security measures to the criteria imposed by the regulation, resulting, from a survey conducted by *Gartner* experts[18] on a representation of ICT specialists[19] , security managers and business managers until the complete effectiveness of the regulation (25/05/2018) that 76% of the companies that responded to the survey, spent less than 10% in computer security. In particular, most of them, more than 50%, spend an average (of about 6 elements) about 8.5% of the budget for cyber security.

Cyber most significant attacks of 2017 and trends for 2018[20]

The sample taken into consideration, based on data in the public domain, represents a partial situation and is less critical than the reality. This is because a good number of assaults never become of public knowledge, or become so years later when the victims reveal it: in general, the more complex and serious attacks are, the less they tend to be publicized, because in many cases it is in the interest of the targets not to publicize the attacks, unless they are forced to by particular regulations (NIS[21] and GDPR); as is happening in the current year, starting in May when the GDRP will become effective in all aspects. With the application of the instruction relating to the obligation to communicate immediately within 72 hours of the attack under Article 33 GDPR in which: "**Notification of a violation of personal data to the supervisory authority"**: 1) In case of violation of personal data, the data holder will notify the competent authority in accordance with art. 55 without unjustified delay and where possible, within 72 hours from the time it became known, unless it is unlikely that the violation of personal data presents a risk to the rights and freedoms of natural persons. Where notification to the supervisory authority is not made within 72 hours, the reasons for delay are related. 2) The responsible shall inform the holder of the treatment without unjustified delay after becoming aware of the violation".

The sample taken into consideration consists of about 7000 "serious" attacks. These known incidents that took place between 2011 and 2017, of which over 1100 only in 2017. In Italy, although the number of serious attacks is very low, for the reasons above mentioned we recall: the story of the Farnesina[22] , the story of the supposed espionage of the Occhionero brothers, the phishing attack, with malware, against 200,000 victims, almost all Italian, realized in July 2017 by the Andromeda botnet[23] , attacks against users of a primary Telco, and a major bank, the recent theft of nearly 200 million dollars in cryptovalute from an Italian exchange. Outside the Italian territory the recent case of Cambridge Analytica the British company of big data analysis, accused of stealing 50 million Facebook profiles and of having used this information to influence the elections from America to Europe with psychographic technique[24]. From Trump to Brexit, profiles to which a former

---

18 The Gartner is a joint multinational actions worldwide leader in strategic consulting, research and analysis in the field of information technology.

19 ICT: Information and Communications Techology : set of methods and technologies that realize information transmission, reception and processing systems.

20 From the Clusit Report 2018.

21 NIS -DIRECTIVE-UE Network and Information Security 1148/2016, directive on network and information systems security. It represents the first set of rules on unambiguous IT security at the level of the European Union. It is proposed to improve the capacity of the cyber security of the single states of the union. Increase the level of co - production among the member states. To make a risk management obligation and to report incidents of a certain amount by operators of essential services and digital service providers.

22 Italian intelligence sources confirm that a group of Russian hackers would have pierced the defense of the Ministry of Foreign Affairs and managed to seize confidential documents.

23 Botnet : Network of compromised computers (bots) connected via the Internet and controlled by an entity called a botmaster through various channels, communication including IRC (Internet Relay Chat) and P2P (peer-to-peer) networks.

24 Technique that exploits the study of the behaviors and choices of social network profiles to create models to be influenced.

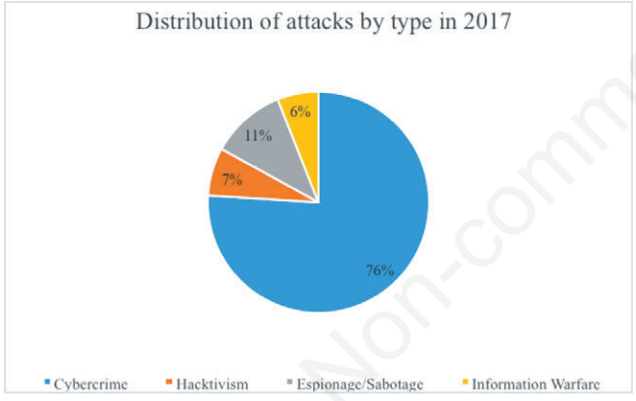
Cambridge student had obtained access for study purposes and then from this divulged. Thus determining the suspension of the Facebook account of the offending company.

Distribution of serious attackers by type

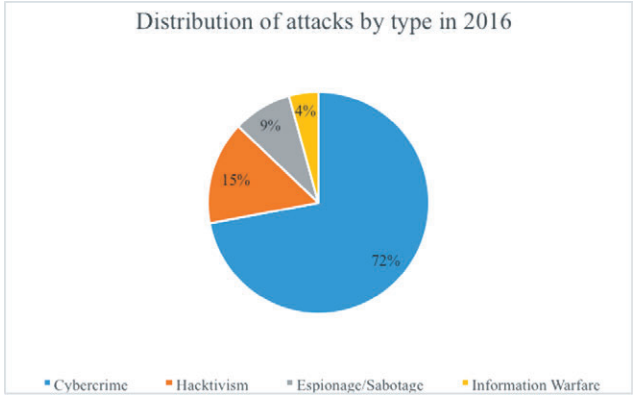
Reporting at global level

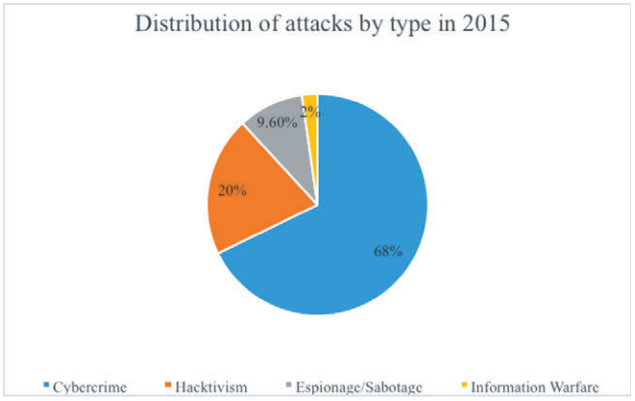
The study is based on a sample set up at the end of the year 2017 from 6865 known attacks that had a significant impact on victims in terms of economic losses, damage to reputation, dissemination of sensitive data (personal or otherwise) or which, however, foreshadow a worrying scenario worldwide (including Italy) since 1 January 2011, of which 1127 were recorded in 2017 (240% more than in 2011), more than 30% compared to 2014 and more than 7.33% compared to 2016. To define an attack as "serious", more restrictive criteria were used, compared to the criteria applied in the years 2011-2013, considering that in this period there wasn't a significant evolution of the prospects and some categories of attacks that could be considered serious in 2011/2013 are now becoming routine, such as defacement (disfigurement, changing the homepage of websites) on websites[25].

Attackers by type	2014	2015	2016	2017	2017 changes on 2016
Cybercrime	526	684	751	857	14.11%
Hacktivism	236	209	161	79	-50.93%
Espionage / Sabotage	69	96	88	129	46.59%
Information warfare	42	23	50	62	24.00%
Total	873	1012	1050	1127	7.33%

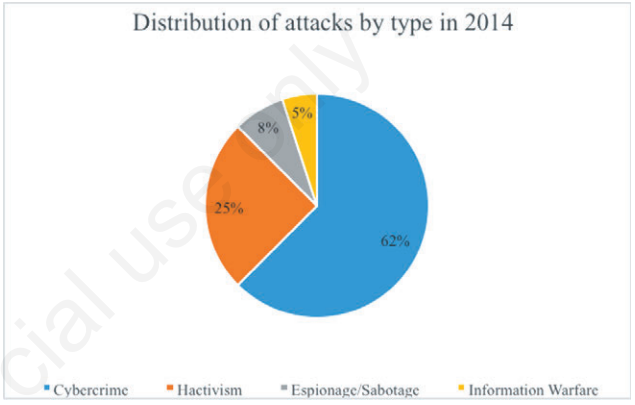


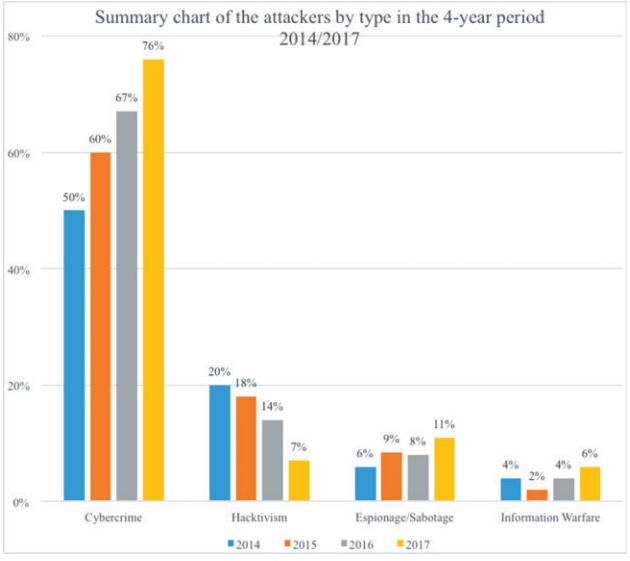
In 2016 there is a percentage distribution of cybercrime relative to 94% of the total, thus recording a percentage of about 6% due to other types of cybercrime.





In 2014, we note a cybercrime distribution of 80% of the total, recording a percentage corresponding to 20%, referring to other types of cybercrime, presumably less serious.





The graph reveals the following: there is a clear priority of the Cybercrime in account of the whole quarter, with an evident growth in 2017. A steady decline in the years starting from 2014 to Hacktivism, an increase of Sabotage / Espionage in 2017 compared to 2016 and also an increase of Information Warfare in 2017 compared to 2016.

[25] From Clusit Report -2018-.

Non-commercial use only

The movement for transparency: The WikiLeaks case

Digital citizenship

With the Internet we have come to develop a new concept of the presence of the individual in the world. Its range of action, now requires a much wider space than it used to occupy, even with a sort of redistribution of power. Based on these changes and therefore on the basis of this redistribution of social power, even the rights of access to the network have to comply with the scope of these extensions, by conferring on those who exercise a broader field of action and possibly open series of management.

With the mandating of 7 August 2015/124, it was decided to issue the legislative decree 13 December 2017/217, with which amendments were issued concerning the Digital Administration Code referred to decree of 7 March 2005/82; introducing, among other things, the concept of "*Digital Citizenship*". A concept that is characterized, mostly by an idea of citizenship intended in a dynamic sense, subject however to all changes determined by the scientific and technological evolution of cyberspace. Determining itself, in the individual's ability to participate in the on line society who like any member of a society, becomes the holder of rights and duties.

Article 9 (*Electronic Democratic Participation*) of the CAD[26] thus expresses: "The subjects referred to in art. 2 c2 (of the Legislative Decree 2005/82)[27] , encourage all forms of use of new technologies to promote greater participation by citizens, including those living abroad, in the democratic process and to facilitate the exercise of political and civil rights and to improve the quality of their actions also through usage where required and within the resources available under current legislation of forms of electronic consultation on the forms of acts to be taken". Even only the art. 21 Cost. guarantees the right to freely express their thoughts with the word, the written and any other means of broadcast. Thus also the art. 19 of the *Universal Declaration of Human Rights* of the UN highlights the right to "search, receive and spread information and ideas through every means and regardless of frontiers."

As for the Internet, everything that is said becomes specific; it goes without saying that respect for a true democracy and with this, for a net neutrality, has to be seen in the actual possibility of accessing it with the normal means and with the required skills, being the characteristics necessary for the explanation of the complete democracy expressed by the new means of social communication. Therefore the rights of the individual will be in the secured network, if he himself raises his status as a competent digital individual, in an appropriate manner and able to make his condition free.

After all, it is difficult to list the wide range of rights that with the technological evolution of the medium of expression, the individual as now "digital", has seen him to be conferred in the different and multiple nuances. Worthy of consideration under this point of view is *The Declaration of Independence of Cyberspace*[28] in which the new concept of civil civilization of cyberspace is clarified, relating to a civilization of the mind, without a physical space created beyond the current boundaries bordered by the physical power of governments[29]. Therefore we have "a people of the network which has a new power able to manage the existing democracy at the base, in a new future perspective able to touch and go beyond the ethical and physical boundaries of the usual social space.

Edward Snowden[30]: Datagate

On the basis of these ideas, a function can be identified that can be expressed in the network through highly democratic forms of expression, matured in creative minds and appropriately linked to cyberspace. One of these is undoubtedly the figure of Edward Snowden, a former CIA agent interviewed on behalf of the newspaper "T*he Guardian*" by the journalist Glenn Greenwald.[31]

The thing that intrigued the journalist was the reason why a former CIA agent had decided to broadcast news that was secretly stolen from his work environment and to then become an informer, a sort of spy, a real *whist blower* ..... *"When you are in a job position of privileged access like a system (assistant) administrator, can have for this type of intelligence agency, you're exposed to a lot of extra information and on a much higher scale than the employees average, and for this reason you can see things that can be disturbing... when you pass everything in front of you, you realize the normal frequency of events and you spontaneously ask yourself: are not these things real abuse truly? And when you talk to people in the trade for whom this is normal, there's a tendency to take things seriously. So leave it alone. But with the passing of time this consciousness that there is something wrong increases, accumulates, until you feel obliged to talk about it. And the more you talk about it the more they tell you that there are no problems, until when you finally realize that these things must be perfectly decided by the public. Not from someone who is higher up than the government".*

Another question asked was about the operation of the NSA, the intelligence agency for which it had worked: *"The NSA, like any intelligence in general, is in principle careful to gather informations from any source and with any means possible. It believes, on the basis of a kind of self-legitimation, to serve a national interest. At first we have seen that their interest is contoured with great accuracy and information that are collected overseas. But more and more often we realize that information is collected at home too and to do these agencies, and more specifically the NSA, they monitor everyone's communications and not just by default. They collect what they say or write through filters, keywords, collect them, analyze them, put them together and save them for a certain period of time, simply because this is the simplest, the most efficient and the most profitable way to get what you are aiming for. So why could they be interested in targeting and controlling someone who has dealt with the government? Or someone who they suspect is involved in terrorism? They collect all your information in order to do something like that. Any analyst, at any time, can decide to control anyone and also any selector, anywhere. From where these*

---

[26] CAD - code of the digital administration - legislative decree 7/3 / 05-82 updated to the amendments of the Lgs 217/2017.

[27] Article 2 of Legislative Decree No. 82/2005 with amendments to Legislative Decree 217/2017: "purpose and scope of application": C2: "The provisions of this code apply to... public administrations... to managers of public services...

[28] by John Perry Barlow co-founder of the Electronic Frontier Foundation.

[29] from the Declaration of Independence of Cyberspace: "Our world is different: Cyberspace is made up of transactions, relationships, and pure thought, arranged like a permanent wave in the web of our communications. Ours is a world that is simultaneously everywhere and nowhere, but it is not where our bodies live. Our identities do not have bodies. Our power will emerge from ethics.

[30] Edward Snowden - US Technical thirties entered in possession for labor relations as a consultant to Booz Allen Hamilton agency linked to the CIA and the NSA and working with the Department of Defense, confidential documents on surveillance projects globally, deciding to make them public gave birth to the so-called *Datagate* and the largest dissemination of confidential information suffered by US intelligence.

[31] Full text of the exclusive interview by Edward Snowden to Glenn Greenwald and Laura Poitras, "the Guardian", 06/11/2013.

communications will be collected and intercepted depends on the degree of reliability of the network used on the authority of the analyst, because not all analysts are allowed to do whatever they want. I, at my desk, am certainly authorized to intercept anyone, from someone like you, to your accountant to the federal judge and even to the President if I intend to enter his personal email".

Even Greenwald is surprised about why he has not chosen to remain anonymous to give the public confidential information: "*I believe that an explanation has to be given to the public, we must give the reasons behind this type of operations outside the democratic model. When the power of the government is completely overthrown, something really dangerous is committed against democracy. If done in secret with assiduity as the government does because it wants to take advantage of an action done in secret, practically you confer a sort of official mandate, a bit like telling the press: say this, say that, so that the public opinion is always on our side. But they rarely do it when illegality occurs. All this deludes individual citizens and of course this means lying to them. You think that informers are against the country and against the government. But not me. I'm not different from anyone else. I do not have any particular skills, I'm just like any other guy who, day after day, sits in the office watching what's happening and finally comes to think: it's not up to us to decide on this sort of thing. Public opinion has to decide whether these policies are right or wrong. And I will go on to defend the authenticity of these things, I have not modified anything. This is the pure truth. This is what is happening. You have to decide whether we should or should not do what we are doing".*

At this point the journalist asks him how the government could react to this behavior. *"Of course, I know I could be targeted by the CIA. I could be monitored. They could be hunting me. Or they could have it done somewhere else, as they collaborate with many other nations. All you know is that they can make you pay. Anything can happen to me. They have agents, they have the means. This is a fear with which I will have to live forever, no matter how long. It is not possible to go against the most powerful intelligence agency in the world and be completely safe from danger, because they are so powerful that no one can even dream of opposing them. If they want to catch you, they will catch you. But at the same time, one has to also make a decision about what really matters to you. If you live in a non-free but comfortable way then it is probably something that you are willing to accept. And I think so for many of us, this is human nature, you can get up every morning, go to work, cash your salary, doing relatively little at work, going against the interest of people and then go to bed quietly after watching television. But if you become aware that in the end this is the world that you yourself contribute to create, and that things will go from bad to worse from generation to generation, because by doing so you expand, the very configuration of this total repression, consequently you realize you are willing to take any risk. And you do not care anymore what will happen, as long as public opinion can really choose firsthand if these policies are right and usable".*

Moreover, Greenwald asked him what are the considerations of the spied individuals and why it should interest them to know how they are spied on: "*Why? Even if you're not doing anything wrong, they're watching you and recording you. And the ability of this system to store all this information increases incessantly, year by year, in an enormous way and is becoming more and more immense. What will it bring us to? You do not necessarily have to have done something wrong. It may very well be that you simply become a suspect, even if you dial a wrong phone number. And at that point the system can go back in time and evaluate every single decision you have taken in your life, all the friends with whom you have discussed a given topic and at that point can attack you on these assumptions, inducing a sort of indirect suspicion and at that point even those who lead the most innocuous life can be depicted as one who is committing something wrong.*

The journalist asked Snowden then what exactly he was aiming for, when he decided to publish those documents and who whom he wanted to hit: "*Anyone who has access to this information with my technical skills could obtain private information and pass it to the market, expose it. There are always open doors for things like that, as we also keep them open. I could have access to whole archive of anyone working at the NSA or of the entire intelligence community and at all secret locations around the world, at stations, at the content of the various missions and so on. If I had only wanted to damage the United States, it would have been enough just one afternoon to put the entire US surveillance service out of the game, but that is not my intention. I believe anyone who wants to support this thesis, must think of putting themselves in my place. They must think of living a privileged life, in Hawaii, in a real paradise, earning a lot of money. Well, what could ever get you to leave all this behind? My greatest fear in relation to the possible outcome of all this for America, the outcome of these revelations, is that nothing changes. People will come to know all these revelations through the media, they will know that the government takes possession of power and that it is really capable of keeping American companies and global companies under control, in the true sense of the word. But it will not be willing to take the risks necessary to stand up straight, to struggle to change things, to force its representatives to effectively take a position in its own interest, that of people. And in the coming months, over the next years, things will only get worse, until the end, one day, the time will come when politics will have to change. Because the only thing that binds and sets limits to the surveillance activities of the population is politics. Although we agree with governments in other countries, we believe that it is an invention of politics rather than a convention of the law because of this a leader will be elected. In just a snap of the fingers, like flicking the switch and it will be said that because of the crisis, of the dangers we face in the world, new threats for the moment still unpredictable, new authorities are needed, or other powers. And at that point there will be nothing more that people can do to oppose it".*

The news leakage allowed by Snowden in 2013 provoked the phenomenon known as "*datagate*", consisting of a series of revelations on mass surveillance activities, against US and foreign citizens made by the US intelligence agency NSA from 2001. Activities continued at least until 2011 and beyond through the following phases:

On June 6, 2013 the Guardian and the Washington Post reported (the complaints are subsequent to 2011) the indiscriminate collection of telephone records of millions of US citizens obtained with the complicity of the telecommunications company Verizon and without the authorization of any judge, publishing much of the material. The same newspapers reveal that the NSA also has direct access to data from Google, Facebook, Apple and other US technology companies to monitor conversations, as part of a mass surveillance program called *Prism*. All data is recorded and catalogued thanks to a secret software. Companies participating in the Prism project are: Apple, Facebook, Google, Microsoft, PalTalk, Skedpe and Yahoo. The violations rouses activist protests, because of citizens' privacy abuse. Edward Snowden reveals that he is the informer of the Guardian and the Washington post and claims to have begun to secretly download the top secret documents of the NSA on April 12, 2012 and to have contacted the journalists Glenn Greenwald and Laura Poitras in the following months. Justifying himself by saying that he did so to protect the privacy of citizens and the US Constitution.

On June 27, 2013, the Guardian writes that the Obama administration has allowed the NSA to check email metadata for more than two years thanks to another program called *stellar wind*.

The program is authorized by a law of 1978, the *foreign intelligence surveillance act*, reintroduced by Bush in 2004 and extended by Obama in 2012, hence the involvement of the British intelligence agency. The NSA defends its activities by stating that they are not illegal, as provided by *the security law* approved by the Bush administration in 2001 after the attacks of 11 September, but many activists and lawyers disagree as the telephone records are under control and therefore the privacy of citizens is violated.

Then again in 2013, the scandal increased and the *cryptome* website revealed that the agency intercepted about 46 million calls in Italy and 60 million in Spain. The Washington Post revealed that the NSA regularly infiltrates the data centers of Google, Yahoo and other US technology companies by strengthening their cryptographic systems as they ask the US government for a law to protect users' privacy. In 2014, President Obama announced a reform of the NSA, while a court in the United Kingdom, established that from 2007 until December 2014 the British secret services GCHQ illegally used the information collected through the global surveillance program, implemented by the United States also controlling Internet traffic. According to *the investigatory powers tribunal*, GCHQ's access to interceptions collected by the US security agency NSA is a violation of human rights.

In May 2015 a US Court of Appeals stated that the interceptions made by the NSA government agency are illegal, according to the judges the program was not authorized in any way by the congress, reversing the sentence according to which the program of the NSA respected the Constitution. In June 2015 the Senate approved the *freedom act*, the reform desired by Obama. The control of the telephone records returned to the hands of the US government and the archiving is up to the telecommunications companies, *which can consult them only after having received the authorization of a judge.*

WikiLeaks and digital democracy

What we note first of all in this system is the open line between what could be considered legitimate to do and what could be prevented if the more normal rights are observed ordinary citizens', subject to this kind of target. To protect them, therefore, from the mass surveillance used against them, a redraft is necessary on this attitude of control. Nothing illegal if the disclosure of news is then carried out for these purposes. The UKUSA agreement was also aimed at obtaining information on an illegal basis, then to be disclosed or better communicated. What is however considerable in the phenomenon of the *datagate* above mentioned is that disclosure has a broader subjectivity, being carried out against a broader context: digital citizenship, that thanks to its skills and its ability to access the network can be informed of this information and exploit their own and mutual control over the data thus perceived. What then are the differences? The basic elements have already been identified: that is to say the objects: the data, the information, that in any case and for the various reasons could interest the entire digital community. What can be the subject of change or variation, is the digital world, which can be defined as the means to confer this power of evaluation to the citizen who interacts with it. With the technological and scientific evolution of the various means of communication, even the power transmitted, grows within its limits, giving wider margins of expression and even content.

If the Guardian newspaper and The Washington Post had played an essential role in the beginning of this need for communication of data and news, with the evolution of the medium represented by the Internet and also with the expansion of the audience of requests, further and more efficient solutions have interested those who wanted to make it a human means, a creator and a voluntary promoter. I'm talking about *Edward Snowden* and the agencies that are interested in the phenomenon. Another figure, however, in this context has to be held authoritatively in consideration and that is that of *Julian Assange* and the phenomenon he triggered that goes under the name of WikiLeaks.

Julian Assange, for the purpose of more timely and accurate information, claims to have created Wikileaks in 2006, substantially for the same purposes identified in the *datagate* phenomenon. Wikileaks being a non-profit organization of online information. This is a website that at the beginning, provided (being managed by its creator) and published hundreds of revelations and documents of strategic importance, including over 6500 reports of the Research Service of the US Congress, the majority of which are available only to deputies, as well as documentary evidence of corruption of senior government officials and violation of human rights in Kenya; of confidential material of a major Icelandic bank, which revealed its role in the financial collapse of the country, of a confidential manual on force procedures in the prison of Guantanamo.

In January 2011, the account Twitter of WikiLeaks threw a curious call for help: "encrypted videos of US bombs dropped on civilians. Many other computers are needed". Later, an independent video was released, on an independent site, the *Collateral Murder.com* (collateral assassination), the video was made by the US army and then decrypted, and it showed two Apache helicopters that on July 12, 2007 fired on a dozen Iraqi civilians massacring them. Assange was too concerned to present the video during a press conference in which he specified further information, namely that according to which the Pentagon had pronounced on the content of the video, considering it entirely legal and produced and carried out according to military standard. The video then attracted the attention of the online community on the WikiLeaks website. Assange and its organization decided to put a strong editorial stamp on the material instead of just spreading online on all the other newspapers (Twitter and other websites). He made sure that a team of volunteers worked for the preparation of the video. Also going to Iraq to talk with the families of the victims of the air raid. Assange expressed himself: "The promise we make to our sources is that we will not limit ourselves to protecting them with every available means, but we will try to obtain the greatest possible impact at a political level from the material they provide".

Who had actually provided this information, who had managed to steal video clips object to military secret and then deliver them to the media and get them to Assange and WikiLeaks?

During 2010, the soldier *Bradley Manning* was arrested in the military base in which he was stationed, near Baghdad, suspected of having given WikiLeaks documents and videos protected by military secrecy as well as hundreds of thousands of cables[32] reserved for the US Department of State. The suspicion about Manning resulted from a chat that he had with an exponent of a newspaper, in which he explained the how he had taken the film on the helicopters, at the same time as the other information related to negative considerations by the military exponents, on the WikiLeaks website. Despite Manning publicly stating that the receiver of his revelations was "the white-haired fool": Julian Assange, in January 2011, federal investigators could not find any clear proof linking Manning to Assange.

According to some other informers, however, Manning delivered the video on the helicopters after reviewing it carefully because initially it looked like it was "just a helicopter shooting at a group of Boys".

[32] Cablogramma: telegraphic message that is sent through a submarine cable. It is printable and is easily comparable to the more well-known paper-based telegram.

Over the following months after the release of the helicopter video, WikiLeaks published an unprecedented amount of documents relating to US authorities that had remained secret until then. The Guardian wanted to help WikiLeaks by using its frameworks during the review and selection of material supposedly still provided by Manning. Assange proposed the direct involvement of the Guardian and the New York Times. Thereafter WikiLeaks spreads around 75,000 documents with historical records of military operations. Throughout the year (2011) publications followed in collaboration with the aforementioned newspapers, of a few thousand of the 250,000 diplomatic confidential cables that Assange had obtained, still presumably, from Manning.

Assange was soon defined as a "high-tech terrorist", that is high tech. The President of the Senate National Security Committee began threatening WikiLeaks service providers including Amazon, whose servers hosted the Assange site. In a short time, well-known companies, including Amazon, PayPal, Visa, MasterCard and Bank of America, had cut the bridges with WikiLeaks, although this had not been condemned for breaking any laws. So that WikiLeaks found refuge on some other sites located in Switzerland that supported his work, among other things also defended by the activity of some affiliates called "*anonymous"*, who launched a counterattack to the websites mentioned above (Amazon, PayPal, Visa, Master Card), blocking all online activities, thus unleashing what was considered "*the first information war"*.

Refereces

Antolithean Francis - Manual of Criminal Law. General Part, Giuffrè Editore, Milano.

Fiandaca Musco (1989) - Criminal Law General Part II, Zanichelli Editore, Bologna.

Mastronardi Vincenzo, Palermo George B. (2008) The Criminological Profile.

Wiener Norbert (1966) Reprint 2001 - Introduction to Cybernetics, Boringhier Blues.

Storchi Mario R. (2017) The new ECDL, Full Standard Editions Manna.

Correspondence: Maria Rita Tarola.
E-mail: merixa@alice.it

Key words: Cybercrime, safety, responsibility, privacy.
Parole chiave: Cybercrime, sicurezza, responsabilità, tutela della Privacy.
Palabras clave: Cybercrime, ciberdelito, seguridad, responsabilidad, tutela de la privacidad.

Received for publication: 18 June 2018.
Revision received: 3 August 2018.
Accepted for publication: 20 August 2018.

This article is distributed under the terms of the Creative Commons Attribution Noncommercial License (by-nc 4.0) which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

©Copyright M.R. Tarola, 2018
Licensee PAGEPress, Italy

Rivista di Psicopatologia Forense, Medicina Legale, Criminologia 2018; 23:36
doi:10.4081/psyco.2018.36

Borrini Andrea (2017) Formatica, New ECDL- IT. Security - Syllabus 2.0, Hoepli-informatica.

De Cataldo Luisella Neuburger (2008) - Examination and cross-examination in the criminal trial, Cedam.

Corso Piermaria, Alibrandi Luigi (2015) Code of Criminal Procedure and Complementary Law, The Tribunal.

Corso Piermaria, Alibrandi Luigi (2017) Code of Procedure and Criminal Law and Laws, The Tribunal, Italian Constitution 1948, US Constitution September 15 , 1787.

Chiusi Fabio (2011) No secret, Nimesis, The coffee of philosophers

Ferrua Paolo (2015) Trial in the Criminal Process, Vol.1, Giappichelli Editore.

Formatical (2013) EN Administrator. Fundamentals. The manual of the Systems, Engineer-Maggioli.

Greenwald Glenn (2014) Under Control, Edward Snowden and mass surveillance, Rizzoli Editore.

Neri Giovanni (2014) Criminology and Computer Crimes. Profiles of Criminal Law of the Economy, Jovene Editore.

Chieppa Roberto (2014) Code of Administrative Law, Giuffrè Editore, Milano.

Rodotà Stefano (2014) The world in the network. What are the rights, what the constraints, Laterza Editore.

Saccardi Giuseppe, Di Blasio Florio (2018) Information Security & Data Protection, REPORTEC.

Sifry Micahl (2011) over WikiLeaks - The future of the Transparency movement, Egea.

Ziccardi Giovanni (2015) Internet. Control and Freedom, Transparency Surveillance and Secret in the Technological Era, Raffaello Cortina Editore.

Gambini Musso Rosanna (2009) The US Penal Process III, Giappichelli Editore.

Webliography

www.ilcappellopensatore.it
www.formiche.net
www.ansa.it.cronaca
www.TG24
www.garanteprivacy.it

Other sources

Summit CLUSIT, Milan 13-15 March 2018, Report Clusit 2018, ASTRA Milan.

INAIL, valuation and Management of Stress related work risk Manual for use by companies in implementation of Legislative Decree 81/08-2011.

Essay on traineeship carried out at the RSPP Pref. Rieti year 2017 *Safety at work -DVR fire risk - work related stress.*

Non-commercial use only