POSITION PAPER

Cybersecurity and protection of the citizens: regulatory instruments, models of intervention and interests at stake.

Contents: 1. Introduction. - 2. The focus on regulatory instruments of on-line public surveillance in relation with the security of the citizens: comparison between EU and US. - 3. The intervention of the Italian legislation, in particolar: the Decree Law on Counterterrorism. - 4. The balance between individual rights and collective interests achieved through non-regulatory instruments - 5. Conclusions.

1. Introduction.

Cyberspace is of central importance for the management, within it, of the political, social and economic life of all countries, and the interconnection of its ICT systems requires, for each of them, to take in great consideration the issue of security. Initially conceived as an immaterial space not subject to any rules, the cyberspace is now subjected to conflicting regulatory initiatives which are expressions of the various interests involved whose spokespersons are States, international organizations and supranational bodies. A careful analysis of the actual situation shows, however, that it is increasing the need not only for a specific regulation of the activities within the cyberspace - this also because of the hermeneutic action of jurisprudence and doctrine that have been able to apply, to the changed technological environment, tailored laws for the analogic reality - but rather for those which are carried out of them and, taking advantage of the bugs of the web, they feed with the intention of undermining the order and certainty of the fundamental norms of democracy.

Statistical data show, in fact, as cyber attacks to websites and ICT networks are made more and more with the help of unaware users who become unsuspecting tools for carrying out illegal activities ranging from of subtraction of information style to the promotion of terror organizations. The possibility to spread in "real time" and around the globe information means that cyberspace turns into an anonymous amplifier for the recruitment of individuals, already committed to carrying out criminal activity, or for the persuasion of subjects easily influenceable, although politically and geographically distant from the outbreak of war (so-called foreign fighters). In this context, the compliance by the public authorities to the fundamental freedoms of the web-users, such as the right to anonymity, inviolability of communications and home computer, makes Western countries vulnerable, as shown by the recent events that have hit neighboring France.

According to these events, it becomes even more urgent the need to analyze the issue of cybersecurity, with the task of describing the outlines of possible remedies and tools of intervention, by looking to the possibility of using, in addition to the usual regulatory instruments, also tools and technical information shared and adopted on a global scale. The revelations on the activities of filtering and monitoring conducted by the NSA without the knowledge of other countries, it has shown that a non-adequately-coordinated activity is not able to bring real benefits in terms of prevention of terrorism. This need, however, has been represented by the President of the Italian Republic, Sergio Mattarella, who, during his inauguration speech, said: "global threats need global responses" recalling that "preachers of hate and those that recruit assassins do use internet and more sophisticated media, that escape, by their very nature, from a territorial dimension." To achieve this result is unfailing result, we need shared global rules that, starting from the technical characteristics, prove to be regulatory instruments able to balance the interests at stake.

2. The focus on the regulatory instruments of on-line public surveillance in relation with the security of the citizens: comparison between EU and US.

The EU interest in the subject of cybersecurity was born in the aftermath of the events that hit Madrid in March 2004 and London in July of the following year, where a series of Islamist terrorist attacks were coordinated to hit the local public transport system and the users of the service. After these tragic events, the European Union has realized the need to strengthen the network of public security and it has, to this end, set up a special agency, the European Network Information Security Agency (ENISA), which has been entrusted with the delicate study and preparation of a common security strategy for all the countries of the Union. The works of the Agency have been adopted by the European Commission which then transmitted them to the European Parliament, the Council, the Committee and the CR, with the Communication (2009) 149, an act that marked the formal start of the legislative process concluded with the drafting of the Directive proposal for a European strategy on cyber security of February 7th 2013, approved with amendments by the European Parliament on March 13th 2014.

The Directive NIS (Network and Information Security), as a result of the Joint Communication of the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy for the Parliament and the Council, it represents the legislative asset at the European level. The rationale of the intervention is to embody the various EU Institutions with the principles of the proper balance of interests in future initiatives, with particular reference to the relationship between the protection of public security and the protection of privacy and personal data. Proof of this is that, not surprisingly, the proposed Directive was drafted in conjunction with the European Parliament Resolution on EU - USA relations on personal data.

Although the approved directive deviates for several aspects from the text originally presented by the European Commission, it identifies as its main target the Internet infrastructure providers who are under the obligation to notify "accidents", intended as circumstances or events with an adverse effect on the ability of a network or an information system to resist, with a certain level of certainty, to accidents or malicious acts that could compromise the availability, authenticity, integrity and confidentiality of data stored or transmitted, or related services offered by or accessible via these

networks and information systems. That provision - as emphasized - necessarily burdens on operators of infrastructure as they are the only ones in possession of information that can trace the origin of the signals, such as going to check the IP address of a user who has posted on a blog a message intended to incite racial hatred or who has tried to illegally access to a confidential government database. Except for the provision cited above, however, still legitimized by unfailing technical requirements, the proposed Directive does not contain provisions to require to the operators of infrastructure further obligations of *facere*, keeping instead the requirement of general cooperation, to deal with the level of voluntary involvement, based on the exchange of mutual information (so-called info sharing). On the other side of the Atlantic there is a legislative initiative, the executive order "Improving Critical Infrastructure-Cybersecurity" of February 12th 2013, with which it has started a process of public consultation led by the various agencies of the sector designed to create a shared regulatory framework regarding cybersecurity defining rules, methods, procedures and specific measures to contain risks for cyber infrastructure. The US legislative choice to focus the provisions on safety information on a public - private partnership appears remarkable, where until the aftermath of the NSA scandal government organizations for security demanded - and obtained - by the service providers of connectivity information on activities performed by users, not only in the presence of concrete attacks as it would be legitimate, but also for mere prevention, or rather preventive surveillance. In the global context outlined above, it is evident that individual countries cannot undertake legislative measures which are not aligned with respect to the EU and US policies.

3. The intervention of the Italian legislation, in particolar: the Decree Law on Counterterrorism.

As anticipated, on the issue of critical infrastructures, the European Union has already started the process of policymaking aimed at living to the member countries a regulatory framework respectful of the balance of the different requirements for protection. Indeed, before the arrival to the proposed Directive NIS, the EU had adopted the term "critical infrastructure", equivalent to the term reported in the US executive order, within the Directive 2008/114 / EC of December 8th 2008, the scope of which, however, was limited to the strategic sectors of energy and transport, albeit with a slightly different meaning.

The legislative decree n. 61/2011, which incorporated the above directive, and, subsequently, the Law n. 33/2012, with specific reference to national airports, have defined the method for the identification of the European Critical Infrastructures (ECI) located throughout the country and they represent, therefore, the first step to outline a national regulatory framework in the field of cybersecurity. With the PM Decree of January 24th 2013: "in a unified and integrated context, the institutional architecture tasked with safeguarding national security in relation to critical infrastructure and tangible assets, with particular regard to cyber security and national security, indicating to this end, the tasks entrusted to each component and the mechanisms and procedures to be followed for the reduction of vulnerability, the risk prevention, the timely response to the attacks and the immediate restoration of the functionality of the systems in a crisis "(as art . 1, paragraph 1, of the aforementioned DPCM).

In this scenario, with two subsequent PM Decrees of January 27th 2014, the National Strategic Framework for the security of cyberspace and the national plan for the protection and cyber security have both been adopted. The first identifies the profiles and trends of the threats and vulnerabilities of systems and networks of national interest, it assigns specific roles and tasks to the various public and private entities involved and it identifies tools and procedures to pursue the growth of the ability of the country to prevent and respond to the challenges posed by cyberspace, whereas the National Plan indicates the priorities, specific objectives and guidelines to give practical effect to the Strategic Framework. These two DPCM represent the main instruments that the country has established to implement the strategies of defense against cyber attacks: actions more or less automated to destroy or damage the operation of the systems, or that are likely to compromise the authenticity, integrity and confidentiality of data stored.

The National Strategic Framework for the safety of cyberspace identifies six areas of action to enhance the cyber security of the country: the improvement of the technological capabilities to increase the capacity of monitoring and of preventive analysis; the strengthening of defense capabilities through the identification of a national authority in the field of ICT security that cooperates with its counterparts, the European Authorities, to share information; the encouragement of cooperation between authorities and businesses; the promotion and dissemination of culture of cybersecurity; the strengthening of contrast methods of illegal online content and the activation of a network of cooperation with third countries.

In the National Strategic Framework, great importance is given to public-private partnership (PPP) considered as a structural element within the architecture of the national authority to ensure cyber security. These forms of collaboration are focused, as indicated in the National Plan, on the system of info-sharing, in a plan to ensure the interoperability of data, sharing of communication standards and vulnerability assessment. In particular, private operators providing public communication networks or electronic communication services accessible to the public, are called to respond to a series of obligations including: the opening of its databases to allow access to controls by the competent authorities, the communication to the Cybernetics Security Nucleum (CSN) of any significant breach of integrity and security, the adoption of best practices for achieving cybersecurity and, more generally, the obligation to assist with the restoration of security in the event of infringement of the network.

Pending the full implementation of the National Plan for the protection and cyber security, the national lawmakers decided that it could rely on the voluntary involvement of individuals in order to prevent terrorism, as necessitated by the need to take note of recent events . Yesterday, the Council of Ministers approved - on proposal of the PM Matteo Renzi, Home Minister Angelino Alfano, Foreign Affairs Minister Paolo Gentiloni, Defence Minister Roberta Pinotti, and Justice Minister Andrea Orlando - a decree on urgent measures to combat terrorism. The adoption of this text is crucial because it is for the first time identified in the Anti-Mafia Direction the central coordination of all activities to fight terrorism throughout the country. It could not, in fact, be more delayed the identification of the competent authority responsible for coordinating all investigative activities and repression against a phenomenon which by its nature has not only local or regional character. The norm, in terms of criminal law, provides the introduction of a new type of offense intended to punish those who organize, finance and promote travel to commit terroristic acts (imprisonment from three to six years) and, in this perspective, the punishment of the subject

recruited as well as the subject who "self-trains" himself for terror techniques. It was also introduced the possibility of applying the measure of special surveillance of public security to potential foreign fighters as well as simultaneous withdrawal of the passport by the ‘Questore’ with the obligation to stay.

For present purposes of specific interest, the Decree updates the tools to combat the use of the Internet for the purpose of proselytizing and facilitation of terrorist groups, providing increases punishment for the crimes of apology and incitement to terrorism committed through computer instruments. The cooperation between judicial authorities and connectivity providers, hosting services and other services related to the Internet network is indicated by decree as the first tool for the prevention and countering of cyberterrorism. As part of the PPP, already identified in the National Strategic Framework, it is, in fact, established that the internet service providers cooperate with the Postal and Telecommunications Service of the State Police for the creation and continuous updating of a "black list" of Internet sites used for the activities referred to in Articles. 270-bis C.C. and purposes of art. 270-sexies of the Criminal Code, including those of "proselytizing", recruitment and training activities for the purposes of terrorism, also international terrorism. In this context there is also the amendment to Article 53, paragraph 1 of the Decree of June 30th 2003, n. 196 (Privacy Code), which provides that, in the new wording, the Police and other public security organs are excepted from certain provisions of this Code in carrying out processing of personal data for purposes of police expressly identified by law.

Finally, in relation to alleged offenses mentioned above, the legislative provisions contain, in analogy with the provisions of Directive 2000/31 / EC and legislative decree n. 70/2003, the direct obligation on providers of connectivity services, hosting or other services connected to the Internet to comply, within forty-eight hours, to the Judicial reasoned decree of order to remove specific Internet content if there are concrete indications that such acts were committed via computer. It is indisputable that the recent events have pushed the national lawmakers to take immediate action to avert the danger of drift "cyber anarchy" and a new militarization through the use of this space, with the possibility for Member States to host or sponsor criminal, terrorist or web-spy networks similar to what happened in these days with regard to the policy document, clearly influenced by propaganda, signed by Isis entitled "the Islamic State in 2015", which has used the site Wikilao to be disclosed on the network and recruit fighters to fill the fields of combat in the Syrian-Iraqi region. It must be observed, however, as the government has been able to delineate an emergency discipline which is not limited to a mere compression of rights, similar to what happened in France (v. Infra) and earlier in the United States of America, but, on the contrary, it proves able to balance the various interests at stake thanks to effective tools of involvement of private entities, always putting the final decisions to the Judicial Authority, which is, by its very nature, the guarantor for the respect of the rights .

These types of interventions are clearly the consequences of the use of exclusively legal instruments for the balancing of the competing interests, balancing that unfortunately sometimes compels a sacrifice or a squeeze of fundamental rights and freedoms of equal rank to which they will give protection.

4. The balance between individual rights and collective interests achieved through non-regulatory instruments.

The greatest risk in dealing with a subject as sensitive as the suppression of terrorist groups, is to adopt norms excessively repressive on the emotional wave of tragic events similar to those that occurred in France, as in the past happened in USA for the Patriot Act adopted after the attack to the Twin Towers in 2001.

In this sense, it can be observed how in France on February 5th it was adopted the Decree n. 5/2015 under which it can be inhibited access to a site via DNS blocking of certain sites without the intervention of a judge, but only with the intervention of an *ad hoc* committee in the case that the contents have child pornography or terrorist elements. Two are, *prima facie*, the critical issues in the aforementioned French decree: the first refers to the measurement technique that can be arranged and , by its nature, it would involve the blocking not only of the specific illegal content, but of the entire site that hosts; the second, with regard to the compression of constitutional freedoms, in terms of fair trial before the natural constituted judge, involves not only the protection of national security, but also for the protection of minors.

The task that the lawmaker, first, and the performers, in the application phase, then, are called upon to perform is to combine individual rights with collective interests: create large databases for the prevention of crimes, if the same are not sufficiently protected, may paradoxically increase the surface area of the terrorist attacks, facilitating access of criminal organizations to the names of individuals recruited for unlawful purposes. On the other hand, in operating the necessary balance, one cannot consider the normative principle developed by the courts; the reference is to the decision of the Court of Justice of the European Union in the field of data retention, which has invited the operators involved in investigative procedures to use tools of investigation proportionate to the protection of citizens freedom, without a right to prevail on the other. Indeed, the interest of a fair balance is not related only to the public question of the protection of individual and fundamental rights but also to the needs of a commercial view of the fact that from a violation of the right to privacy descends a responsibility on the holders of personal data.

Even stakeholders, with express reference to large service providers of information, must be, in fact, put in a position to know what exactly they are entitled and obliged to report to the judicial authorities and what, instead, have to keep private in respect of the inalienable rights of its members, this in order to protect even their freedom of economic initiative.

To sum up, therefore, the adoption of rules derogating from principal legislation to give real protection to the constitutional freedoms requires the need of a fair balance between the different interests involved. In particular, if, on the one hand, governments have the need to maintain public security, including through widespread control of preventive nature, on the other, it is prompted to the connectivity providers, especially the global suppliers, to guarantee the protection of the right to privacy of its users, by technical means, such as the encryption of data otherwise, conversely, it could expose too much the users.

The absence of legislation to regulate the relations between public authorities and private individuals within the PPP aimed at protecting public safety, makes the adoption of technical and

outreach initiatives even more complicated. These relations are free from rigid forms of bureaucracy and so able to be effective at the level of the same actions that contrast.

5. Conclusions.

According to these observations, the scenario proposed is therefore very complex: on the one hand the need, now more than ever urgent, to protect the collective interest of public safety, on the other hand the fact that the interference of the regulator could directly compress inviolable individual rights, or limit the rights of economic operators, service providers of the information society. The real challenge is, therefore, in achieving the fair balance that turns out to be not only essential but also very delicate, with regard to the status of the interests at stake: all of them of constitutional level, each protected by different sources national and supranational, which sometimes, in the wake of a particular historical and political context, have developed different solutions.

The complexity of the issues suggests, as already mentioned, also to consider alternative ways to that of regulatory instruments, in particular using the technical and communicative tools: for information purposes that, with the appropriate corrections, may be able to explain to the public opinion the intentions of the lawmakers. This should start with the creation and the implementation of inter-institutional networks that could be identified as speech patterns conducive to achieve a fair balance between all the interests involved, however, reducing the risk of exposure of connectivity providers and global service claims, protection of the right to privacy and protection of personal data made by users. The US experience, on the application of the Patriot Act, has also shown how the adoption of encryption techniques of data lead to a fair balance between protecting public safety and protection of the rights and freedoms constitutionally guaranteed: the encrypted data may, in fact, be collected and held by the competent governmental authorities which "use" such information only in the presence of a reasonable suspicion of a security threat coming from a particular individual.

Finally, other instruments may be useful technical information, such as counter-speeches which, appearing in superposition to the web page with critical content, pursue the goal of conveying positive messages, not necessarily refuting the contents viewed (which paradoxically may cause a strengthening of the beliefs of the user). Those listed above are only some of the non-regulatory instruments that could limit and combat in the same scenario of cyberspace the terrorist attacks on the web and to the web; and the national or supranational lawmakers cannot ignore the effective enforcement of dangerous phenomena as cyberterrorism without detriment to hard-won inviolable rights. It appears, moreover, easier to share globally a technical tool, such as the encryption of data, or political education of users of the web, ie. the counter-speech, rather than a legal text. This character must be a top priority because terrorist organizations do operate on a global scale and require equally global and unified responses. In this scenario, therefore, it emerges how the protection of cyberspace can be effectively and profitably entrusted with initiatives of self and co-regulation of economic operators who, as part of legislative policies shared by various countries, appear to be faster in giving a precise response to instances of conflict resolution.