media LAWS
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 2/2017

FABRIZIO DI GERONIMO*

Cyber threats and human rights:
the special relationship with privacy and the role of the principle of proportionality

SUMMARY: 1. Introduction. – 2. The impact of cyber threats on human rights. – 3. The impact of cybersecurity measures on human rights. – 4. The threefold relationship between privacy, cyber threats and cybersecurity measures. – 5. The importance of the principle of proportionality. A focus: the risk of a stabilized emergency. – 6. The principle of proportionality: how and when. – 7. A practical application of the principle of proportionality in a case of cyber threats: the DPI again.

1. *Introduction*

The main legal trend concerning cyber threats is to study them from a variety of perspectives, including Internet law and the strategical and defensive point of view, that usually do not include the constitutional one. In particular, the many researches concerning cyber threats have rarely studied this new phenomenon as regard its interrelation with the protec-

* Graduated from Bocconi University (Combined Bachelor and Master of Science in Law, 2016), *summa cum laude;* fellow in Constitutional Law, Bocconi University.

Law and Media Working Paper Series
Codice ISSN: 2531-484X
EDITORE: Oreste Pollicino - COORDINATORE EDITORIALE: Marco Bassini
SEDE: Via Roentgen, 1 – 20136 Milano e-mail: submissions@medialaws.eu

tion of human rights as protected by national Constitutions and international conventions. It is even more uncommon to find any study considering the impact of both cyber threats and cyber security strategies (aiming at fighting cyber threats) on fundamental rights and liberties and the consequent particular relationship existing between these three elements.

The aim of this paper is to start a first analysis in this direction, highlighting how both cyber threats and cybersecurity measures hinder human rights protection. A solution, careful to the exigencies of protecting rights and liberties has to be found in the adoption of an appropriate set of legislative measures, all respectful of the principle of proportionality. This principle must, indeed, guide the work of every legislative body acting in this field, in order to avoid serious consequences as regard human right protection.

The analysis will proceed in this order. First of all, both cyber threats and cybersecurity measures will be examined from a general point of view, in order to understand that they both are able to hinder the respect of rights and liberties (par. 2 and 3). In particular, as regard the ability of cyber threats to endanger human rights protection, it is necessary to separate cyberterrorism and cyberwarfare from cybercrime and cyberespionage, because these two groups attack different values. The first one is more likely to damage the right to life and national security; the second one, on the contrary, has as its main target the right to privacy, the property right and the economic wealth. However, it must be clarified since the very beginning of this paper, that these categories are not to be considered definitive and absolute. In the world of cyber threats, because of the newness and complexity of the phenomenon, from a legal but also factual point of view, it is actually very difficult to find something clearly definable.

Moving to the second element (par. 3), cybersecurity policies, we will see that they are also able to endanger the protection of human rights, especially of privacy, thus creating in some legal scholars the fear of an hypothesis of future mass surveillance, justified by the need of fighting cyber threats. The real example shown in this paper is the deep packet in-

spection, a measure often proposed by academics, that would certainly be able to reduce cyber threats, but would at the same time reduce the level of data protection.

It is clear, therefore, that privacy plays a fundamental role in the relationship between cyber threats and cybersecurity policy and that can work as a litmus paper, able to show the intensity of the sacrifice of rights in the name of security (par. 4). Moreover, it is not possible to reach cybersecurity without bearing a sacrifice in terms of liberties (i.e. data protection), thus being necessary to reduce the ensured level of privacy because of new technologies and cyber threats. The critical and constitutional issue, is to what extend privacy can be reduced in order to fight cyber threats. In other words, an equilibrium must be found between the exigencies of securities and the respect of fundamental rights and liberties. It is, therefore, necessary to apply the principle of proportionality. Otherwise, the risks would be the inefficacy in fighting cyber threats or the excessive reduction of human rights, resulting in the birth of a new hypothesis of stabilized emergency (par. 5).

In conclusion, the analysis will move to the study of the principle of proportionality, trying to understand how it should be applied and in which stage in order to be effective in reducing the impact on human rights and still allowing the legislative policy to properly fight cyber threats (par. 6). The negative model of the fight to terrorism will be an effective example of all the mistakes that must be avoided during the creation of a policy aiming at fighting any threats to our democracies. Moreover, the tendency of the judiciary (especially the European one) will be of fundamental importance in order to understand how the principle of proportionality must be applied.

All these elements will then be studied from the perspective of cyber threats, hypothesizing how they should be considered during the crafting of a cybersecurity policy. Finally, to have a practical example, the deep packet inspection will be considered again, trying to apply to it the principle of proportionality to verify whether is possible for a cybersecurity measure not to hinder excessively human rights protection.

2. *The impact of cyber threats on human rights*

It is worth beginning from a proper clarification: both cyber threats and cybersecurity strategies (aiming at fighting cyber threats) have a deep impact on the protection of human rights.

Considering firstly the impact of cyber threats, they damage human rights protection in many ways and with different intensity, varying from cyber threat to cyber threat[1]. Indeed, cyberwarfare, cybercrimes, cyberterrorism and cyberespionage have very different interactions with human rights, also varying the types of values endangered by the existence of these threats. In particular, a classification known by scholars divides cyber threats in two groups based on the jeopardized value[2]. Cyberwarfare and cyberterrorism would be, in this respect, separated from cybercrimes and cyberespionage. The first two threats would mainly damage national security and all the connected values, such as the right to life; the remaining two, instead, are principally linked with the right to privacy and the economic wealth.

[1] An initial, due classification, identifies four different classes of cyber threats: cyberwarfare, cyberterrorism, cybercrime and cyberespionage. Each of these types of cyber threats has a different impact on the protection of human rights.
However, in the field of cyber threats there are barely universally accepted definition. This is due to the novelty of the phenomenon and the interaction of many relavant areas of law. For example, some authors consider *hacktivism* – that can be defined as "*[t]he act of carrying out malicious cyber activity to promote a political agenda, religious belief, or social ideology*" (*Hacktivism. A defender's playbook*, 2016, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-hacktivism.pdf) in order to reach those aims traditionally achieved with sit-in activities and strikes (D. DENNING, *The rise of hacktivism,* in *Georgetown Journal of International Affairs, http://journal.georgetown.edu/the-rise-of-hacktivism/*)– to be an autonomous category, while others include it in the idea of cyber crime or cyberterrorism.

[2] See for example S. MELE, *Cyberwarfare e danni ai cittadini*, in www.stefanomele.it, 2010 (ultimo accesso il: 23/09/2016), p. 5

As anticipated, cyberwarfare and cyberterrorism have[3] a strong impact on the right to life, being both of them able to cause hundreds of deaths with a single attack. In order to understand the seriousness of a cyber-attack, performed by either a State (cyberwarfare) or a terrorist organization (cyberterrorism), it is easy to imagine the consequences of an intrusion into the aerial traffic control devices, the alteration of the system devoted to the management of civilian transport infrastructures, the tampering of the electrical grid or of military defence systems.

Moreover, even softer attacks may cause huge problems and serious consequences for a State. The effects of such an attack are usually threefold: physical pain, disturbance of normal life and decrease of confidence in political institutions[4]. In addition, the spread of terror among the civilian population can be an added consequence of a cyber-attack. To consider a real example, in 2003, Italy was shocked by a national black out (actually not due by a cyber-attack, but the effects are mainly the same). It lasted for for just few hours, but this was enough to cause 4 victims and more than 60000 emergency calls.

Moving to cybercrimes, the values mainly damaged are the right to privacy and the property right. With this respect, the growth of cybercrimes has been exponential, causing in 2016 annual loss of 500 billion Euro[5], 600 million victims and 348 million identity violated per year[6], compared to the loss of 113 billion dollars and the 378 million victims of 2013. The economic issues are caused by loss of value of goods protected by intellectual and industrial property rights, by financial frauds, by reduction of productivity and by damage to rep-

[3] It would be better to say "may have", since there has not been yet any real case confirming that hypothesis and, for some authors, these are events unlikely to happen in the real world, being restrained to academic analyses.

[4] L. FRANCHINA, *Infrastrutture critiche*, http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/OSN/Documents/05_Franchina.pdf, slide 38

[5] http://www.lapresse.it/allarme-garante-privacy-cybercrime-pesa-500-miliardi-l-anno.html

[6] 2016 Norton Cybersecurity Report, http://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_p1_seeglobalrpt

utation[7]. Moreover, the spread of digital frauds hinders the development of e-commerce because of the fear of being cheated[8].

Concerning data protection, hackers are easily able to access private data and the risk is exacerbated by the recent tendency to create big databases containing many sensible information[9]. A relevant, practical, example is the worm Flame, who had a great diffusion in the last years. It is capable of acquiring audio and video information using the cameras of smartphones and personal computers, of registering Skype conversations, controlling bluetooth devices and taking screenshots.

More generally, and without focusing on a specific violated right, cyber threats are able to jeopardize the correct functioning of our Western democracies, endangering the entire range of value protected. A clear and recent example of that was the (alleged) interference of Russian hackers in American election. The accusation is that Russia manipulated, with the spread of a virus, US voting machines in, at least, three States (Wisconsin, Michigan and Pennsylvania) in favour of Trump. Moreover, Russian hackers are accused of cybernetic intrusions into Democratic National Committee's servers and consequent diffusion of thousands of private e-mail. Whether or nor these charges are true, they could be true[10], and this is enough to be be aware of the danger cyber threats constitute for our democracies.

Therefore, it is undeniable that cyber threats constitute a great risk for our modern societies and that, as concern our main purpose, they constitute a strong hindrance to the realiza-

[7] F. DUAH, *The growing global threat of cyber crime: implications for international relations*, University of Ghana, 2013, http://hdl.handle.net/123456789/5294, p. 41

[8] *Ivi*, p. 40

[9] Consider the new PNR Directive, but also the *Visa Information System (VIS)*

[10] See for example J.A. HALDERMAN, *Want to Know if the Election was Hacked? Look at the Ballots*, https://medium.com/@jhalderm/want-to-know-if-the-election-was-hacked-look-at-the-ballots-c61a6113b0ba#.gsr7bhnq8, where the author confirmed that such an hypothesis could be true, and could happen in a near future simply because "*voting machines are computers, and they have reprogrammable software, so if attackers can modify that software by infecting the machines with malware, they can cause the machines to give any answer whatsoever.*"

tion of "cyberspace as an area of freedom and fundamental rights"[11], as it is required by the European Union Cybersecurity Strategy. In addition, cyber threats are also able to hinder the protection of offline rights.

It is therefore necessary to adopt some measures to re-establish the due level of protection of human rights and to let new technologies being an instrument of strengthening, and not weakening, of our democracies. However, from a constitutional law perspective, a problem lies in the fact that also (and to some extend even with a higher intensity) cybersecurity measures may undermine human rights protection.

3. *The impact of cybersecurity measures on human rights*

Browsing the many papers on cyber threats, it is easy to understand that almost all the proposed cybersecurity measures would have a certain implication for human rights[12]. The fear often highlighted by scholars is that of a new hypothesis of mass surveillance. On the contrary, a real analysis from the constitutional point of view, concerning the interaction between contrasting values, namely the exigency of security[13] versus the protection of other constitutional rights and liberties, is usually lacking.

---

[11] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, available at: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf, p. 15

[12] This is true for both those measures operating before and after the commision of an attack. We would focus on the last ones, that can properly be considered as cybersecurity measures, which can be defined as those measures aiming at avoiding the commision of a cyber threat. Differently, the measures operating after the commission of an attack should better be considered as enforcement measures, and are more linked with cybercrimes and (if defined as a crime by national criminal laws) cyberterrorism.

[13] As regard the value of security much could be said. What is necessary to state here is that – even if security has always had a fundamental role in constitutional speeches, since Hobbes and the Declaration of the Rights of Men and of the Citizens (see T. E. FROSINI, *Il diritto costituzionale alla sicurezza*, in

In particular, the right mainly damaged by cybersecurity measures is the right to privacy[14]. Indeed, as any other defensive strategy, also cybersecurity measures require a big amount of information in order to be effective. Moreover, the word "data" acquires in this context a special meaning, being data not only the information necessary to dispose an effective measure, but also the very same instrument through which the attack is pursued. Therefore, it is obvious that establishing an effective defense against cyber threats would require having access to a big amount of information and personal data. Among the many data necessary to obtain a successful control, it would be for example essential to collect and analyze,

---

www.forumcostituzionale.it, p. 1) – it has recently started to assume a new importance. In particular, the recent tendency is to consider the existence of a "right to security", as opposed to the previous "security of rights" (see C. BASSU, *Terrorismo e costituzionalismo. Percorsi comparati,* Torino, Giappichelli, 2010, p. 98). The right to security is, therefore, elevated to a real fundamental right that must be balanced with all the other rights and liberties recognized by Constitutions and international treaties (see also T.E. FROSINI, C. BASSU, *La libertà personale nell'emergenza costituzionale,* in A. Di Giovine, *Democrazie protette e protezione della democrazia*, Torino, 2005, p. 81).
The birth of this new kind of security has also practical consequences (in addition to the many draconian legislations, such as the US Patriot Act and the Data Retention Directive – see later on for a better analysis), all of which, as it is easily understandable, have a negative fashion. The main tangible manifestation of this new importance attributed to security is the closure of the borders (even in the Schengen area) and the construction of walls to reduce immigration and control the fear of the foreigner. Just to cite some of these, there are the big wall of Calais, the wall at the border between Hungary and Serbia, the displacement of more than two thousand soldiers between Austria and Italy and the barbed wire beween Macedonia and Greece.

[14] We are here considering the right mainly damaged (also because of the special relationship existing between privacy and cyber threats – see later on) but, not to be too superficial, it is necessary to clarify that cybersecurity measures are able to interfere also with the protection of other rights. Among these rights emerge the rights to online speech and the freedom of expression, limited, for example, by the Anti-Cyber Crime Law of Saudi Arabia that exploited it to imprison political dissenters. Freedom of expression was also endangered by the Philippine Cyber Crime Prevention Act that criminalized libel (N. GREEN, C. ROSSINI, *Cyber security and human rights,* at publicknowledge.org, https://www.gccs2015.com/sites/default/files/documents/Introduction%20Document%20for%20GCCS2015%20Webinar%20Series%20-%20Cybersecurity%20and%20Human%20Rights%20(1).pdf).
Also the CJEU, in a case concerning the protection of the intellectual property right, confirmed that privacy is not the only damaged right by cybersecurity measures. In *Sabam,* indeed, the Court recognized that "the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information" were excessively damaged by the measure under analysis (European Court of Justice, judgment 24 November 2011, C-70/10, *Scarlet Extended SA versus Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, par. 53).

at least, IP addresses, domain names and DNS records, all of which are included into the definition of personal data of the Data Protection Directive[15], therefore being protected by the same. It is not surprising, thus, that the same Directive 95/46/CE[16] provides an exception, excluding from its scope of application the processing of personal data for purposes of national security[17]. That was, indeed, necessary not to limit excessively the scope of action of national authorities, allowing them to establish some measures necessary for the immediate exigencies of national security and that would reduce the protection of privacy. However, this exception is not strong enough to allow all kind of measures against cyber threats, and probably cannot be considered as the only provision at the base of a complex policy aiming at fighting cyber threats. That would probably amount to an excessively broad interpretation and would corrupt the original purpose of the rule. In this regard, it would be necessary to find a new legal base for the subsequent bundle of measures essential to fight the analyzed phenomenon appropriately.

It is possible to consider the new Directive on security of network and information systems (NIS Directive)[18], together with the new General Data Protection Regulation[19], as a more

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
The broad definition of personal data is enshrined in article 2: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"
[16] Article 3: "This Directive shall not apply to the processing of personal data: … in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law"
[17] M. CUNNINGHAN, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, in *George Washington International Law Review*, Forthcoming, available at http://ssrn.com/abstract=2138307, p. 43
[18] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[19] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on

appropriate instrument. Indeed, the NIS Directive constitutes the first European attempt to approach in a comprehensive fashion the problem of cybersecurity, taking into account the seriousness of the problem from the technological and international point of view. In particular, for our purposes, the new obligations for both operator of essential services[20] and digital service providers[21] can certainly suggest a primary role for some technical measures against cyber threats. Indeed articles 14 and 16 require that operators of essential services and digital service providers "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems. … Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed."[22]

To understand how, in practice, an effective cybersecurity measure would endanger human rights protection, it is worth considering one of the measures that is more often proposed by scholars: the deep packet inspection (DPI). It is a technique that allows to analyze all the data that pass through an inspection point, situated between two end-points of the net. In this way it is possible to verify the existence of any threat, hidden in the sent data, and stop it before it reaches the final user.

The DPI is an evolution of previous techniques and, thanks to the most recent technological developments, allows to check not only the packet header (i.e. IP address), but also the body or payload of the packet, thus controlling the very contents of the transmitted data. A first problem from the point of view of privacy is, therefore, that the DPI, differently from previous techniques, analyzes the packets from the inside, not checking only the external el-

---

the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[20] See Directive 2016/1148, article 4(4) and article 5 (Identification of operators of essential services)

[21] See Directive 2016/1148, article 4(5) and 4(6)

[22] See the almost identical articles 14 and 16

ements[23]. Anonymity is certainly hindered but is probably correct to affirm that also privacy is damaged by such a filter on data packets[24].

The original function of DPI was network security, that is making sure that there was no undesired traffic on a certain net (local area network – LAN). However, it can be employed for much more goals and it is currently used at least for some of these[25]. Firstly, DPI is employed for traffic management, which consists in verifying all the data passing through the net in order to filter them and give a preference to some types of data (eg. preferring e-mail services over peer to peer), in order to organize the Internet service[26]. Through this system, it is also possible to create different types of subscriptions, depending on the required use of the web, establishing higher prices for some services (usually peer to peer). However, and this is a clear example of how controversial DPI is, this use of deep packet inspection is in contrast with another well-known value of the Internet: net neutrality.

Another use of DPI concerns the management of commercial banners, that can be customized for each user of the Internet thanks to the analysis of transmitted data and of previous browsing. Moreover, DPI can be very useful for the protection of intellectual property rights when threatened by cybernetic threats (which actually constitutes a type of cybercrime). This

---

[23] For a deeper analysis concerning DPI, especially in relation to previous techniques: A. DALY, *The legality of deep packet inspection,* in *International Journal of Communications Law & Policy,* No. 14 (2011), pp. 2-3. Available at: http://ssrn.com/abstract=1628024; C. HANGEY, *Deep Packet Inspection and Your Online Privacy: Constitutional Concerns and the Shortcomings of Federal Statutory Protection*, 2008, pp. 1-2. Available at: http://ssrn.com/abstract=1907078; C. PARSON, *What's Driving Deep Packet Inspection in Canada? ISPs, Netscapes of Power, and Privacy Advocacy*, 2009, pp. 1-6. Available at http://ssrn.com/abstract=2530814; S. STALLA-BOURDILLON, E. PAPADAKI, T. CHOWN, *From Porn to Cybersecurity Passing by Copyright: How Mass Surveillance Technologies are Gaining Legitimacy… The Case of Deep Packet Inspection Technologies,* in *Computer Law and Security Review*, 30 (2014), pp. 1-7. Available at: http://ssrn.com/abstract=2528186

[24] For the difference between anonimity and privacy see A. DALY, *The legality of deep packet inspection,* in *International Journal of Communications Law & Policy,* No. 14 (2011), available at: http://ssrn.com/abstract=1628024, p. 3

[25] A. DALY, *The legality of deep packet inspection*, pp. 3-7

[26] B. SAETTA, *Cosa sarà l'Internet del futuro? Il rischio Grande Fratello è più reale che mai?*, in *Valigiablu.it*, http://www.valigiablu.it/cosa-sara-linternet-del-futuro-il-rischio-grande-fratello-e-piu-reale-che-mai/

is one of the most developed branch of DPI and it has also gave rise to some important decisions of the CJEU[27].

However, to our purposes, the most important use of DPI is with reference to cyber security, that is using this technique to filter the malicious packet data containing the signature of a cyber-attack, individuating in advance the threats in order to prevent it from reaching its target. This branch of DPI is not very developed from a legislative (and consequently, judicial) point of view, but it is often proposed by legal scholars as one of the most effective solutions to the problem of cyber threats and it is certainly already employed in some countries, such as Russia and China, that unfortunately cannot be considered as a prototype for democratic societies where the rule of law is respected.

What can certainly be stated, is that the different uses of DPI are now going through a process of diffusion. This is especially true with respect to the functions of regulating traffic and personalizing commercial banners, but thanks to the role of the scholars and the diffusion of cyber threats, it is not unlikely to imagine a future increase in the use of this technique also when it comes to national security. This evolution is also testified by the adoption, by the International Telecommunication Union, a UN body, of the standard ITU-T Y.2770, which "specifies the requirements for deep packet inspection (DPI) in next generation networks"[28].

4. *The threefold relationship between privacy, cyber threats and cybersecurity measures*

What has been said thus far should be sufficient to illustrate the particular relationship between data protection, cyber threats and cybersecurity.

[27] See for example the already quoted *Sabam* judgment and *Netlog (*European Court of Justice (Third Chamber), judgment 16 February 2012, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) versus Netlog NV*)
[28] http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11566

Firstly, there is a special relationship linking privacy with cyber threats. Indeed, not only cyber threats prejudice the protection of privacy (which is true also with regard to other rights) but they have a common origin. The development of both (at least interpreting privacy as data protection) derives from the diffusions of ICT that, on one side, put the right of privacy at the top of the hierarchy of fundamental rights and, on the other side, are the instruments through which cyber threats spread.

In addition, the link between privacy and cyber threats becomes even stronger because of the threefold relationship between privacy, cyber threats and cybersecurity measures. Indeed, they both hinder data protection so that either establishing acts against cyber threats or not, privacy would be endangered. In other words, it is not possible to increase cybersecurity (that is, defending ourselves from cyber-attacks) without bearing a sacrifice in terms of data protection. At the same time, not to adopt cybersecurity provisions, would mean allow our privacy to be damaged by cyber threats. Indeed, "without security … consumers' bank accounts, spending patterns, health records, political and religious associations are exposed"[29].

The trade-off that the legislator (at a national, but also international level) must deal with is between a stronger or weaker cybersecurity, taking into account that, in the first case, data protection would be undermined (immediately) by the adopted measure, even if this would be able to reduce the number of cyber intrusions, i.e. of external invasions of privacy. On the contrary, in the case of a weaker cybersecurity, there would not be an immediate and certain reduction of privacy, but data protection would be attacked by the external intrusions of cyber attackers. Moreover, also other types of values would be vulnerable to cyber threats that, as noted, do not affect only the right to privacy but also other values, among which national security[30].

[29] M. CUNNINGHAN, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, p. 38

[30] It is possible to classify cyber threats with regard to the value that is damaged. On one side there are cybercrimes and cyberespionage, mainly attacking privacy and the economic wealth; on the other side, there are cyberwarfare and cyberterrorism that constitute a risk especially for national security (and therefore, among others, for the right to life).

In conclusion, it is arguable that the same diffusion of modern information and communication technologies dictate the reduction of privacy protection, no matter whether a legislative measure has been adopted or not. *Per se*, new technologies raise the possibility to violate privacy, also developing new forms of data collection and even shaping new kinds of personal data, such as the information on geolocation and DNA information[31]. The same existence of cyber threats is a consequence of ICT and is another element able to reduce privacy.

Therefore, it seems that, because of the peculiar relationship linking ICT, privacy, cyber threats and the measures able to contrast them, in our modern society it is not possible to ensure the same level of privacy protection than before and that a reduction of data protection should be accepted. Indeed, considering two extreme hypothesis, both if a strong measure against cyber threats has been adopted and if no measure has been crafted, privacy would be reduced by, respectively, the measure itself or by the hackers, left free to act. The last chance to protect both national security and privacy is to spot the perfect equilibrium between these extreme positions in order to minimize the impact of cyber threats, and more generally of new technologies, on privacy.

From a legal and constitutional perspective, it is necessary to apply the principle of proportionality[32] in order to struck a balance between the need of security (i.e. the fight to cyber threats) and the protection of human rights, especially privacy (i.e. cybersecurity measures must not be too invasive).

The two alternative risks would be, otherwise, to adopt no effective measure (so that cyber threats are not contrasted), or to establish a draconian legislation that would excessively reduce the enjoyment of human rights.

---

[31] H. ASHIYA, *Right to privacy in cyberage* in Various Authors, *Right of privacy: constitutional issues and judicial responses in Usa and India, particularly in cyber age*, 2009, available at http://ssrn.com/abstract=1440665

[32] We will focus later on the principle of proportionality

5. *The importance of the principle of proportionality. A focus: the risk of a stabilized emergency*

It should be clear by now that both national security and human rights are endangered by the very existence of cyber threats. The key problem lies in the fact that also effective cybersecurity measures would hinder human rights protection. This circumstance requires applying the principle of proportionality in order to verify which is the best equilibrium, among cybersecurity measures and freedom on the Internet, that would entail the lowest burden on human rights protection. Therefore, a balance must be struck between security and liberties.

The consequences of not applying the principle of proportionality could be extremely serious. Two alternative scenarios are possible. Firstly, it could be adopted a measure disproportionate in favour of rights and liberties, thus ineffective against (or, at least, not sufficient to fight) cyber threats[33], so that they would continue to endanger human rights, that would be ensured and protected only in theory. Moreover, this scenario could evolve into a real catastrophe, whether an hypothesis of cyberwarfare or a cyberterrorist attack should became a reality[34].

[33] It is possible to consider as measures partially ineffective all the acts currently existing in the European and national context with the specific aim of contrasting cyber threats. All these measures, indeed, certainly useful in the fight against cyber threats, cannot be considered as a sufficient defense against these new threats to our democracies, because they do not act immediately and technically against cyber intrusions. In other words, all the cybersecurity strategies (as they are usually named) establish aims to be reached in the medium and long period, providing for principles of cooperation, for the technologicla improvement of relevant hardware and software and national critical infrastructures, duties of criminalizations. Moreover, they aim at incrementing IT knowledge throughout the popoulation because, it has been verified, the majority of cibernetic attacks pass through private devices and are usually successful because of the inexperience of private users (see, among others, G.R. LUCAS, *Privacy, Anonymity, and Cyber Security*, in *Amsterdam law forum*, Vol 5:2, 2013, p. 107 and Cybersecurity Strategy of the European Union, p. 8). In conclusion, the measures currently in force would be a strong instrument in the future, when all the provided objectives would be reached. However, by now, they appear more as a program for the future than as a real cybersecurity measure. What is currently needed, indeed, is a measure that act on a technical level, using the same expertise exploited by cyber attackers.

[34] It is worth recalling that, so far, we have not yet experimented the worst hypotheses of cyber attacks, especially as regard cyberwarfare and cyberterrorism. In particular, acts of cyberwarfare, as already highlighted, are able to start a real war or at least to produce very serious consequences in terms of

On the contrary, the second possible scenario consists in the adoption of a strong legislative measure against cyber threats that, even if very effective, would endanger human rights at an unacceptable level as a precondition for its application. At the same time, it cannot be disregarded that with such a measure in force, the external impacts of human rights would be reduced. All these elements must be considered when it comes to applying the principle of proportionality.

To notice the negative effects of a strong policy against cyber threats, it is possible to imagine an aggressive application of the DPI. A law could craft the deep packet inspection providing that all the data transmitted over the net should be monitored, not only with regard to their external content (i.e. IP address) nor looking only at the signatures, but checking the very content of these communications. Moreover, it would be possible to establish the analysis of every packet data in order to verify the existence of some threat and to retain all the checked data creating a huge database, accessible by the competent authorities, that could also comprise intelligence agencies. It is obvious that a law of this type would amount to a case of mass surveillance, not so different (and probably even worse) than that experi-

---

human deaths and physical destruction. However, thus far, we have only experimented some weak (and still relevant!) example of cyberwarfare. The most notorious example is that of the worm Stuxnet that allowed the US and Israel to destroy Iranian nuclear power plant. Other important application of ICT to interfere with the ordinary living of another State are attributable to Russia, such as the shutdown of Ukraine's power grid (2015) (see https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, that is also very able in showing the difficulties in the attribution of a cyber attack) and interferences on Estonian governmental websites (2007) (See, for a big list of *cyber incidents*, Significant Cyber Incidents, *Center for strategic & international studies,* available at https://www.csis.org/programs/strategic-technologies-program/cybersecurity/significant-cyber-incidents).

The same is true also for cyberterrorism that can potentially produce enormous catastrophes, but has been, so far, very limited. Indeed, the net has been used by terrorist organizations especially for an organizational and propagandist application. In particular, Internet is exploited by terrorists for enrollement, training – on the web it is extremely easy to find real handbook on the contruction of bombs or on the preparation of a terroristic attack –, communication, research of funds, datamining and spread of terror through messagges and videos (see M. CONWAY, *Terrorism and the Internet: New Media-New Threat?*, available at https://www.researchgate.net/publication/29651834_Terrorism_and_the_Internet_New_Media--New_Threat; http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/)

enced with regard to the fight of terrorism. This scenario would end up with the creation of a so-called "stabilized-emergency" that would further hinder the protection of human rights and the survival of our Western constitutional democracies.

To explain this expression and understand the dangerousness of such a scenario it must be stated that the original idea of the state of emergency is the declaration of a special legal regime in order to fight an extraordinary event that threaten the very existence of a State. When the state of emergency is in force, special powers are attributed (usually to the executive branches), because the ordinary acts are considered ineffective against the specific threat. However, the intensity of these powers jeopardize the survival of the rule of law, endangering, above all, the separation of powers and the protection of human rights. The special powers attributed, indeed, are capable of reduce the guaranteed level of human rights in order to act more effectively against the threat. However, and this is one of the main feature of the state of emergency, the strength of these powers finds a limit in some guarantees disposed during the state of emergency, especially the temporariness of the powers. On the contrary, a "stabilized-emergency" is an abusive evolution of this model, characterised by the absence of any guarantee and, above all, by the absence of temporariness. This is caused by the introduction of special powers and the derogation of human rights protection rules through ordinary legislative acts, that certainly cannot be considered as provisional measures. Therefore, it is by using ordinary acts with an extraordinary content that the abusive and illegitimate derogation of human rights finds place in our legal systems, endangering their very survival from the inside.

This risk, that finds his main expression in the fight against terrorism[35], must be avoided at any cost, and here again the principle of proportionality must be considered as the proper

[35] The main example of normalized emergency is happening with regard to the terrorist threat. Indeed, since 2001, the international terrorism has been fought through the adoption of legislative measures very severe from the point of view of human rights protection. In particular, many powers have been conferred to governmental authorities in order to contrast and prevent terrorist acts that, on the other side, are limit constitutional guarantees, and above all privacy and personal liberty. The two

solution. In particular, there are, at least, two ways that will probably results in a normalized emergency "declared" to fight cyber threats. The first hypothesis would be realized whether a legislator decides to act against cyber threats but not applying the principle of proportionality, thus enacting a draconian legislation. This measure would probably be able to fight cyber threats but the cost in terms of human rights would be excessive. What is suggested here is to act in an anticipatory way, but without disregarding citizens' rights and the principle of proportionality. In other words, to act against cyber threats seems now a real need. However, the legislator must not act guided by preventive and irrational panic[36] but using a rational approach.

On the contrary, the second hypothesis follows from the decision not to adopt new legislative measures against cyber threats. That could clear the way to a dramatic cyber-attack that would cause many human deaths and/or relevant physical destructions. This scenario (that, in reality, is considered strongly unreasonable and unrealistic by some authors[37]) would spread panic through the population and the government would probably react with the introduction of strong cybersecurity acts. In the aftermath of this cybernetic 9/11, there would not be the proper reflection and discussion and the impact on human rights would be enormous because of the diffused feeling of fear and the need of security. The legal consequences would therefore be incredibly similar to those followed to the New York and Washington attacks[38]. To avoid these consequences it is necessary to act before a such violent cyber-attack happens, adopting a cybersecurity policy in accordance with the principle of proportionality.

---

stronger examples of this kind of legislative practice are the US Patriot Act and the European Data Retention Directive.

[36] V.K. SINGHAL, *Cyberterrorism: An Overview*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427059, p. 11

[37] *Ivi*, p. 7, where the author considers the "Digital Pearl Harbor" nothing but an irrealistic scenario

[38] In the same direction see also G.R. LUCAS, *Privacy, Anonymity, and Cyber Security*

6. *The principle of proportionality: how and when*

Moving to the analysis of the principle of proportionality, it is now necessary to understand how it works and when it must be applied.

The good news for scholars studying cyber threats from the perspective of their interrelation with human rights, is that they can count on the broad number of legislative acts, judicial decisions and opinions of scholars on the relationship between terrorism and human rights. Indeed, even if many differences exist, terrorism and cyber threats can be considered similar for certain elements. In particular, they both can be studied as phenomena that threaten the lifestyle ensured by Western democracies. Therefore, the fight of Islamic terrorism can be exploited as a (bad) model and, considering all the differences, to understand how cyber threats must be regulated and how the principle of proportionality must be applied.

As said above, terrorism has been fought mainly with legislative acts able to derogate to human rights protection to a strong degree. For example, in crafting the US Patriot Act[39] and the Data Retention Directive[40], the American and European legislators did not consider at all the principle of proportionality, only aiming at reaching security and relieving citizens. The adopted acts were definitely abusive and disproportionate, restricting the protection of human rights beyond any reasonable possibility.

On the contrary, the judiciary (both at national and international level) started very soon to consider and apply the principle of proportionality in order to show the excessive burden

[39] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 - USA-PATRIOT Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. 272, 288-90 (2001)

[40] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

on human rights of almost all the measures adopted to fight terrorism[41]. However, the work of the courts has often had very limited practical effects[42]. Therefore, as it would be showed later on, it is necessary to consider the principle of proportionality already during the crafting of the policy, at the legislative level.

To analyze cyber threats today, an historical period in which cyber threats do exist, but have not shown yet their complete negative impact on our societies[43], offers important opportunities. Firstly, it is possible to exploit the example of terrorism in order to avoid committing the same mistakes. Secondly, it is possible to act in advance, ahead of the verification of catastrophic cyber-attacks, trying to impede these events to happen and, at the same time, avoiding to legislate in a period of general fear (such it would be – and was in the case of terrorism – after a national tragedy).

Therefore, a first teaching of the disastrous example of the fight of terrorism, is the necessity to respect the principle of proportionality since the legislative stage, and not only at the judicial one, in order to avoid the very creation of an abusive measure. Indeed, even if someone could argue that there would always be the chance for the judiciary to improve the wrong equilibrium established at a legislative level, the truth is quite different. As demonstrated by many decisions of the CJEU (the same situation is observable in the United States with reference to the practice of the Supreme Court[44]), they often end up as having few practical effects, only reaffirming the correct balancing at a theoretical level.

---

[41] Apart from the European judgments, that would partially be considered in this paper, it is possible to understand the tendency of the judiciary studying some Supreme Court's judgments. See, among others, *Rasul v. Bush*, 542 U.S. 466 (2004); *Rumsfeld v. Padilla*, 542 U.S. 426 (2004); *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004); *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006)

[42] See, for example, note 44

[43] Remember that cyber threats are still at the beginning of their development and we have not experimented yet the most dangerous hypotheses of cyber attacks, especially as regard cyberwarfare and cyberterrorism.

[44] See for example *United States v. Jones*, 565 US _ (2012). In particular, in *Jones*, the Supreme Court clarified (especially in the concurring opinion of justice Sotomayor) that, in the digital era, a Fourth Amendment search occurs whenever the government violates a subjective expectation of privacy, that occurs also when the collection of metadata is at stake

Being clear the stage when the principle of proportionality should be applied, it is now possible to move to the 2014 *Digital Rights Ireland* judgment[45], necessary to understand how this principle must be applied in practice.

With this decision, that continued a previous tendency started with the 2008 *Kadi* decision[46], the CJEU invalidated in toto the Data Retention Directive, that we have already seen as one of the most vivid example of normalized emergency, because of the excessive burden it posed on human rights[47]. In other words, since the Directive 2006/24/CE did not establish a correct equilibrium while balancing security and liberties, it was disproportionate and, thus, illegitimate.

The importance of this decisions lies in the fact that the Court did not annul the Directive simply because it was hindering the protection of human rights and liberties, but because the burden was excessive in relation with the advantage in terms of security. In other words, the Directive had to be invalidated because it was based on a wrong balancing of values, and not simply because it reduced human rights protection.

(See also *United States v. Jones*, in *Oyez*, https://www.oyez.org/cases/2011/10-1259). Therefore, the governmental program of mass surveillance had to be considered as covered by the Fourth Amendment, even if collecting only metadata. However, as regard the weak practical effects of the courts' decisions, during their attempts to reduce the burden on human rights of unreasonable legislative acts, the same FISC denied the influence of *Jones* over the metadata collection programs with an interpretation of the Fourth Amendment incredibly opportunistic (not to say illegitimate) (See *Memorandum, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted]*, No. BR 13-158, https://www.aclu.org/files/assets/2013.10.11_fisa_court_memorandum.pdf), thus basically eliminating every influence of the Supreme Court's decision over governmental programs.

For an European example of weak practical effects see later for the case of *Digital Rights Ireland*

[45] Court of Justice, judgment 8 April 2014, joined cases C-293/12 e C-594/12, *Digital Rights Irelands*

For an excellent analysis see also VEDASCHI A., LUBELLO V., *Data Retention and its Implications for the Fundamental Right to Privacy*, in *Tilburg Law Review*, 20 (2015) 14-34; FABBRINI F., *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, in *Harvard Human Rights Journal*, Vol. 28, 2015

[46] Court of Justice, judgment 3 September 2008, joined cases C-402/05 P e C-415/05 P, *Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council of the European Union and European Commission*

[47] In particular, the complaint was based on the alleged violation of articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union, which respectively protect the right to private and family life, the right to personal data and the right to freedom of expression and information.

The CJEU recognized the existence of an objective of general interest, since the Directive's aim was to fight international terrorism in order to maintain international peace and security[48], but that objective could be pursued only respecting the principle of proportionality. Therefore, the CJEU did not deny the seriousness of international terrorism, nor the necessity to fight it with strong measures that could also partially reduce human rights. However, proportionality had to be respected between security and liberties. In the case of the Data Retention Directive, proportionality had not been respected in crafting the measure, because it imposed an excessive burden on human rights, unnecessary to the aim of fighting terrorism. Thus, it had to be annulled.

It is worth noticing that the Court did not act only considering conceptual and theoretical constitutional principle (i.e. the principle of proportionality as a general principle that should be applied), but also considered European legal norms. In particular, article 52, par. 1 of the Charter of Fundamental Rights of the European Union[49] (Charter) states that "[s]ubject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union"[50]. Therefore, the principle of proportionality is required by the same Charter that constitutes, now, primary EU law, having the same legal value as the Treaties[51]. Thus, the Charter, and the enshrined principle of proportionality, must be respected also from a strictly legal point of view, in the European

[48] Digital Rights Ireland, par. 41-42
[49] Available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf
[50] The complete first paragraph, article 52 states that "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."
[51] The Charter became legally binding and obteined this legal force thanks to the Lisbon Treaty. In particular, art. 6(1) TEU states that "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties."

(and, consequently, national) legislations[52]. Indeed, as primary EU law, the Charter is a real "parameter for examining the validity of secondary EU legislation and national measures"[53].

However, and this can work also as an evidence of the weak practical effects of courts' decisions, the shiny reasoning of the European Court of Justice in *Digital Rights Ireland* risks to be outdated by the practice. Indeed, firstly, to the annulment of the European Directive did not follow automatically the invalidity and annulment of all the national implementing acts[54]. As a consequence, all the national legislations implementing the (now void) Directive are still in force in national legal systems. This created, together with a situation of legal invalidity, also negative practical effects, because the Internet Service Providers (ISPs) are not well aware of their obligations. Indeed, according to national laws they have to bear some high costs and burdens in order to retain some categories of personal data, an operation that risk to be illegitimate under European Law[55]. In addition, and what is even worse, new legislative acts have been enacted after the 2014 judgment, showing a complete disregard of the CJEU's decision and principles. Indeed, the new French law on wiretapping and data retention provides even stronger hindrances to the protection of privacy than the act issued to implement the Data Retention Directive. Moreover, even the European legislator has recently adopted a new act, the PNR Directive, able to damage data protection for all the European citizens, no matter a link with terrorism, in open contrast with Digital Rights Ireland's principles[56].

---

[52] To understand how the CJEU applies the principle of proportionality as enshrined in art. 52 of the Charter see for example par. 38ss. of *Digital Rights Ireland*

[53] http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.1.6.html

[54] See also L. MARIN, *The Fate of the Data Retention Directive: About Mass Surveillance and Fundamental Rights in the EU Legal Order* in T. Konstatinides, V. Mitsilegas, M. Bergstrom, *Research Handbook on European Criminal Law*, 2016 (forthcoming), p. 12 ss

[55] I. GENNA, *Data retention, effetti anche in Italia dopo il caso Olanda?* in *corrierecomunicazioni.it*, http://www.corrierecomunicazioni.it/ict-law/33157_data-retention-effetti-anche-in-italia-dopo-il-caso-olanda.htm (ultimo accesso il: 23/09/2016)

[56] Recall par. 58 of Digital Rights Ireland

This example is fundamental to our purposes because it shows how the principle of proportionality must work and it also confirm the thesis that it should be applied since the legislative stage, risking the reestablishment of proportionality at a judicial level to be ineffective. What is necessary, then, is to apply the lesson from the European Court of Justice also to cyber threats. As clarified from the very beginning of this paper, cyber threats constitute, even being at the beginning of their development, a clear threat to national security and to the enjoyment of constitutional rights and liberties. Therefore, the fight of cyber threats can certainly be considered as an objective of general interest. In other words, the fight to cyber threats deserves to be reached, even at cost of partially reducing the protection of human rights. However, the principle of proportionality, between the exigency of security and the protection of rights and liberties, must be respected.

In the case of an hypothetical measure against cyber threats, the two groups of compared values would be, on one side, those protected by the cybersecurity act (and, therefore, those endangered by cyber intrusions) and, on the other side, those damaged by the same measure. In particular, the values protected by such an act would be national security, the right to life, the right to privacy, the economic wealth and the intellectual and industrial property right. On the other hand, however, the proposed act would hinder, at least, the right to privacy, the freedom of enterprise and the freedom to receive and communicate information[57].

In this particular balancing, human rights, and especially the right to privacy, appear in both the side of the equation because of the particular relationship that has been showed between privacy, cyber threats and cybersecurity measures. Indeed, both cyber threats and the possible measures have a deep impact on human rights and, above all, on privacy and data protection. The consequence is that the correct equilibrium that would allow to legitimately fight cyber threats, would be found in that point where the burden on human rights is at its minimum.

[57] As clarified in *Sabam*

7. *A practical application of the principle of proportionality in a case of cyber threats: the DPI again*

We can conclude our analysis on the interrelation between human rights, cyber threats and cybersecurity measures and the subsequent necessity to apply the principle of proportionality, coming back to the deep packet inspection and imagining how it should be crafted in a manner that could be considered respectful of proportionality.

The DPI, thanks to its capacity to filter all the packets of data transmitted on the net, can be very effective in order to reach cybersecurity, stopping cyber threats before they reach the target. However, it would be, at the same time, extremely burdensome for human rights protection.

Nevertheless, it is possible to establish some legislative precautions that would allow the measure under analysis to be still effective, and yet less problematic from the point of view of human rights. The presupposition would be the same of Digital Rights Ireland: find an equilibrium between human rights and security, without preferring one to the other[58]. To reach this aim it would be necessary to automate the process of scanning and filtering of the contents transmitted in order to eliminate the human intervention in the process. That could easily be obtained by using an algorithm[59]. In addition, it would be necessary to eliminate any kind of retention of the checked data. It must be especially avoided the retention of data concerning the totality of citizens with no link with situations that could give birth to criminal investigations[60]. In addition, it would be possible to set up the algorithm so that it would analyze only the signatures of the packets, renouncing to a search based on keywords that would be more intrusive of citizens' private life. In this way both human intervention and the retention of data would be limited to the cases strictly necessary, namely when a ma-

[58] Indeed, it would be also mistakenly to totally prefer the protection of privacy over the defense from cyber threats. With regard to terrorism, this is the position of the so-called *purists*. See C. BASSU, *Terrorismo e costituzionalismo. Percorsi comparati*, p. 99

[59] S. MELE, *Privacy ed equilibri strategici nel cyberspazio*, p. 71

[60] This exigency has been already individuated by the CJEU. See *Digital Rights Ireland*, par. 58

licious signature is individuated by the algorithm. Even in these few cases precautions should be taken, and the retained data should be kept in an EU-located server, so that all the EU acts on data protection would apply[61]. Lastly, it would be necessary to verify the authority which intervention would minimize the burden on privacy[62] and to establish accountability and auditing procedures.

It is arguable that, respecting these precautions, the analyzed measure would certainly reduce privacy protection but not in an excessive way with respect to the aim of reaching cybersecurity. Indeed, even if privacy would be partially hindered by the adopted DPI, it would be, at the same time, more protected thanks to the reduction of cyber intrusions. This is, again, a consequence of the particular relationship existing between privacy, cyber threats and cybersecurity measures, from which also arise all the peculiarities of the application of the principle of proportionality in the matter of cyber threats.

[61] *Digital Rights Ireland*, par. 68
[62] The two possibilities are to assign the analysis directly to the ISPs or to a governmental authority