CYBER-TERRORISM AND THE RIGHT TO PRIVACY IN THE THIRD PILLAR PERSPECTIVE

by

NADINA FOGGETTI*

Cyber-terrorism involved a serious of conducts such as a targeted attacks, politically motivated, conducted with the help of computer technology and/or within the information technology, with significant consequences at economic, political and social level.

Against this new threat the EU is called to give a answer with the instruments that it have to disposal in the Third Pillar.

In front of the proliferation of acts adopted in this sector, this is a luck of a specific legal instrument in the fight against cyber-terrorism.

The first questions that we will analyse concerning the definition of cyber-terrorism.

We will to analyse the possibility to apply of cyber-terrorism existing legal instruments. At the same time the fight against cyber-terrorism involves the need to collect systematically data and DNA data, also through Europol and Eurojust and to plug into databases. This data collection is essential in order to adopt the measure of execution of UN Resolutions for the prevention and repression of each typology of terrorist funding, as well as the freezing funds that are directly or indirectly addressed a to that end. This data is able to breach fundamental human rights.

There is the need to guarantee the right to privacy of persons and entity involved in data collected.

In the second part of the paper we will analyse the problem of the balancing between the need to combating international terrorism and cyber-terrorism and that to protect fundamental human rights, also by the study of the recent jurisprudence of the EC Court of First Instance. To that end we will analyse the legal instrument for individuals and entities in the EU law for the protection of their fundamental human rights.

* PhD – University of Bari, Department of International law and EU law, nadinafoggetti@gmail. com.

KEYWORDS
Cyber-terrorism, EU, privacy, data transfer, PNR agreement.

1. A DEFINITION'S ISSUE

In 1997 Mark Pollitt drew up a definition of cyber-terrorism, which tends to associate the word with a premeditated attack with political purposes, directed against information systems management that can determine serious consequences against targets that are not in state of war[1].

There are various definitions that, over time, have been attributed to cyber-terrorism. We could try to define cyber-terrorism as the use of information technology in order to obtain an advantage in a terrorist action or strategy.

This definition could cover both planned use of modern technologies and their possible use. But, if we believe that cyber-terrorism is an autonomous conduct, probably we cannot apply any international instrument currently in force. A lot of measures have been adopted in order to fight international terrorism at international and EU level. It is worth mentioning some of these standards such as the Framework Decision of 13 June 2002 on the fight against terrorism[2] and the proposal for a Council framework decision amending the Framework Decision 2002/475/JHA on the fight against terrorism.[3]

The European Convention for the Prevention of terrorism[4] was signed in Warsaw on May 15, 2005. Article 1 of the FD n. 475/2002 states that each Member State shall take the necessary measures to ensure that in their legal order the intentional acts which, given their nature or context, may seriously damage a country or an international organization where committed also with the aim of causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, are considered as a crime.

Indirectly, cyber-terrorism can be included under this definition.

However, the system is seen as an objective to which a terrorist act could be directed and not as a means by which terrorist cells can organize and launch the attack.

---

1 Pollit M.M. 1998, *Cyber-terrorism Fact or Fancy?, Proceedings of the 20th National Information Security Conference,* in Pollitt, M.M. (edit by),*"Cyber-terrorism: Fact or Fancy?," Computer Fraud and Security.*

2 *Council framework decision on combating terrorism, GU L 164, 22nd of June 2002,* p. 3.

3 *Proposal of a Framework decision that modify the Framework decision 2002/475/JAI on combating terrorism,* {SEC(2007) 1424} {SEC(2007) 1425} /* COM/2007/0650 def. - CNS 2007/0236 */

4 *European Council Convention for the prevention of terrorism*, signed in Warsaw on May 16, 2005, entry to force on June, 12007. www.coe.int

A reference to cyber-terrorism is in the proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism.

In this document, the institutions said that modern information and communication technologies play an important role in the development of the threat which is currently represented by terrorism: they may serve as a means of dissemination of propaganda aiming at mobilization and recruitment as well as instructions and online manuals intended for training or planning of attacks, addressed at current and potential supporters.

The Council, in particular, said that the Internet may serve as one of the principal boosters of the processes of radicalization and recruitment: it is used to inspire and mobilize local networks and individuals in Europe and also it serves as a source of information on terrorist means and methods, thus functioning as a 'virtual training camp'. The dissemination of terrorist propaganda and terrorist expertise through the Internet has therefore empowered terrorists, making the terrorist threat grow. Moreover, the importance of such dissemination can only be expected to increase, taking into consideration the fast growing number of users that will make the Internet an even more vital element of modern society than it is today. This proposal updates the Framework Decision on combating terrorism and aligns it with the Council of Europe Convention on the prevention of terrorism, through including public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism in its concept of terrorism. In the context of the Council of Europe, in fact, the only convention that might include cyber-terrorism is the European Convention on the prevention of Terrorism, signed in Warsaw on May 15, 2005 and recently entered into force.

Articles 5 and 6 of this Convention states that "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.

Even though Articles 5 and 6 do not mention cyber-terrorism, they state that each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist attack or recruitment terrorist cells, regardless of the means used, as criminal offences under its domestic law.

Since the provisions of the Convention are generic, they could make back the terrorist actions carried out through the Internet. But it is difficult

to put cyber terrorism in the definition of terrorism included in the Convention.

For the purposes of this Convention, "terrorist offence" means any of the offences within the scope of and as defined in one of the treaties listed in the Appendix.

Cyber-terrorism is not even mentioned in the Budapest Convention on Cyber crime drafted in the Council of Europe and also recently ratified by Italy. The problem that arises in this respect is the need to qualify on cyber-terrorism separately, by making a conceptual division between cyber crimes and terrorism. The whole offence will be punishable in this way on the basis of different standards. The existing measures may be applied to the recruitment, training and public provocation to commit a terrorist offence, made through the Internet. However they do not apply to terrorist acts undertaken and completed through the internet. For example, these measures do not apply if a terrorist group makes an illegal access to a computer system with the ultimate purpose of financing terrorists, or it makes a computer attack that endangers international security for terrorist purposes.

These facts cannot be classified in any of the acts mentioned. In the war against terrorism, human rights norms are often perceived as a constraint for an effective response to the danger. Many Governments, International organization at universal and regional level claim indeed that the very nature of the threat requires them to intervene even at expenses of basic democratic principles, such as respect for personal freedom and non-discrimination, or propriety. In this contest the right to privacy takes a dual significance[5]. It is a right, but it is also important because its enforcement helps to protect other fundamental rights.

2. EUROPEAN MEASURES AGAINST TERRORISM AND THE RIGHT TO PRIVACY

The EU and the States are implementing surveillance power. The EU has adopted a wide range of legislation in the field of counter-terrorism, such as Council Common Positions and the Council Regulation.[6]

A Common Position on combating terrorism, for example, which copies almost all provisions of Security Council resolution 1373 (2001).[7] A Common Position on the application of specific measures to combat terrorism

[5] Costamagna F. 2007, *Derogating from ECHR Obligations to Fight International Terrorism: Analysis of Some Controversial Issues*, La Comunità internazionale, pp. 111 – 150.

[6] *Council Regulation EC n. 2580/2001 on specific measures directed against certain persons and entities with a view to combating terrorism*, Official Journal of EC, L 344 , of 27 December 2001.

[7] *Council Common Position 2001/931/CFSP of 27 December 2001 on the application of specific measures to combat terrorism*, Official Journal of EU, *L 344*, of 27 December 2001.

and a Council Regulation on specific restrictive measure directed against certain persons and entities with a view to combating terrorism. In order to better counteract the financing of terrorism, the European Parliament and the European Council also amended Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (Directive 2001/97/EC). In addition to the Council Framework decision of 13 June 2002 on combating terrorism constitutes a central piece of counter-terrorism legislation in EU. In order to implement Paragraph 1 of United Nation Security Council Resolution 1373 (2001) at EU level, the existing institutions with legal personality, i.e. Europol and Eurojust have been strengthened. However, according to Article 30 of the TUE, Europol is meant to grow into the operation task of investigating terrorist offences; a participation of Europol in joint investigation teams has been envisaged in the Council Framework Decision of 13 June 2002 on joint investigating teams. The Schengen Information System (SIS) was seen as a compensation mechanisms for the removal of internal borders. The Schengen Information System has been replaced by a new system, the Schengen Information System II (SIS II), which shall allow new Member States to be integrated into the system.[8] It is interesting to note that according to the Monitoring group which assists the Sanction Committee against the Taliban and AL Qaeda pursuant to Security resolution 1390 (2002), States participating in the Schengen area are not able to prevent the entry into or the transit through their territories of members of these two groups. As highlighted in the Monitoring Group's second report of 22 August 2002 the SIS contained by then only around 40 of the 219 names of individuals who appear on the list of names annexed to resolution 1390 (2002).

In accordance with the decision SIS II, Europol and Eurojust have access to certain categories of records. These institutions have access to data entered in the SIS II under Articles. 26 and 38. By the same measures, the powers of control and access to Europol have been extended. The activity of exchange of information between Member States and Community institutions has been intensified following the adoption of the Hague program which allowed the introduction of the principle of availability of information[9]. Under this principle, in short, national and European institutions engaged in the processing of data in order to prevent and combat international terrorism, can expand the capacity of access to national databases without

---

[8] *Council Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation of the Schengen Information System (SIS II),* Official Journal of EC, L 328 of 13 December 2001, pp. 4–6

[9] Hosein G., L. M.., 2005, *Threatening the Open Society: Comparing Anti-Terror Policies in the US and Europe, International privacy*, pp. 45-67.

the permission of the court and beyond the limits of knowledge required by state law.

This has caused a huge traffic of information and data passing through the use of modern information technologies.

The use of IT systems to launch attacks has caused a huge traffic of data. The data resulting from the activities of cyber-terrorism is often combined with data neutral. These data shall in databases containing information about terrorists or suspected. Even the authorities have widely used this information to monitor terrorist activities and cyber-terrorism. In particular the object of control are the transnational travels of individuals.

In this context it is important to recall that on July 26 2007 the United States and the European Union have concluded the agreement on the transfer of passenger data contained in the Passenger Name Records (PNR).[10]

This agreement has followed another one previously concluded between the same parties that was submitted to the Court of Justice in order to assess its legitimacy in the light of the directive on the protection of personal data.[11]

The Court limits itself to assess the legal basis on which the decision to conclude the above mentioned agreement was issued. In this way it has failed to enter the substance of the matter relating to the protection of personal data in the third pillar, and more specifically in the fight against international terrorism. The court held that the transfer of personal data contained in the cards for passengers to Customs and Border Protection of the U.S. Department of Homeland Security was a treatment concerning public security and state activities in the field of criminal law.

The Court ruled that the decision on a related processing of personal data in accordance with Art. 3, No. 2 of Directive 95/46 did not fall within the scope of the directive. Therefore the Court concluded that it was necessary to cancel the decision. Following the decision cited, on July 23 2007 the Council signed the Agreement between the EU and the USA on the processing and transfer of passenger reservation Passenger Name Record (PNR) on the basis of Articles 24 and 38 TEU.

The conclusion of the PNR has excluded the application of the directive on the protection of personal data.

---

[10] *Council Decision n. 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)*, in Official Journal, L 204/16 of 4 August 2007.

[11] Judgement of the Court of 30 May 2006, C-317 e C-318/04, *European Parliament c. Council of the European Union*, http://curia.europa.eu/

Therefore it is not possible to apply the limits imposed by data retention directive especially by Art. 25. The just mentioned article provides that in order to allow the transfer of personal data outside the EU, the country receiving the data must ensure adequate protection of the received data.

Thus, if the legal basis were Art. 25, the institutions should have made an assessment about the adequacy of the level of protection granted by the USA to personal data.

In the United States of America there is no general law on the protection of personal data that also guarantees the right to judicial protection against potential abuse.

The US legislation concerning personal data consists of a series of agreements and sectoral codes of conduct. There is not an authority comparable to those established at national and EU level.[12]

We could conclude that the level of protection is not adequate to the requirements of Art. 25 of the Directive on data retention.

The change in the legal basis has enabled the institutions to lower the level of protection of personal data in order to prevent and combat international terrorism.

3. THE EU ANTITERRORISM MEASURE AND THE RIGHT TO PRIVACY IN THE EU AND ECHR PROSPECTIVE

A further issue that we must examine is whether the acts in question meet the fundamental principles of European law and European Convention on Human Rights. The protection of privacy under the law remains anchored however to the First pillar, while the fight against terrorism and crime takes place in the Second and Third pillar. For this reason it is difficult to balance the protection of privacy with the fight against international terrorism and to assess the impact of measures taken by institutions in order to reach this specific purpose.

In the just mentioned case law, the European Court of the Court held that the powers of the Community shall be exercised in accordance with international law. This provision applies even in the maintenance of international peace and security in the implementation of resolutions adopted by the Security Council under Chapter VII of Charter.[13]

The EU Court states that the Regulation is an EU act and then the Court is asked to assess their compatibility with fundamental rights.

---

[12] Simoncini M., L.M. 2007, *Legislazione antiterrorismo e tutela della privacy*, in *Rivista trimestrale di diritto pubblico*, p. 659 – 701.

[13] *Judgement of the Court of 20 May 2008, C-91/05, Commission vs Council*, in *www.europa.eu*

In this contest, the EU Court of Justice in a Case of September 3 , 2008, annuls the Council Regulation on May 27, 2002, No. 881, which imposes restrictive measures directed against certain persons and entities associated with Osama bin Laden, the Al-Qaeda and the Taliban, and repealing Regulation (EC) No 467/2001.[14]

But it orders that the effects of Regulation No. 881/2002 to be maintained, so far as they concern Mr Kadi and the Al Barakaat International Foundation, for a period that may not exceed three months running from the date of delivery of this judgement.[15]

However, the reasoning of the Court of Justice clearly shows the prevalence of the need to respond to the terrorist threat.

The Court, therefore, claims that the fight against terrorism prevails on fundamental rights.

In the second instance we must analyse if the PNR Agreement impair the European Convention on data retention and European Convention on Human rights.

To analyse the admissibility of the transfer of personal data in the light of the European Convention for the protection of data, we must consider the letter sent in July 2007 by DHS particularly the statement which outlined the terms and conditions for the data transfer .

The letter states that the data transferred to US authorities will be used solely for the prevention and suppression of international terrorism and related crimes and the prosecution of other serious crimes, including transnational organized crime. Art. 5 of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data states that personal data undergoing automatic processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes. The purpose of the fight against terrorism is determined. On the contrary, we cannot say that the aim is determined or determinable in relation with the crimes. The letter does not reveal, in fact, what are the serious crimes listed, which will be the criteria to be taken into consideration in order to identify these types of crimes.

We can therefore conclude that the agreement signed counteracts the Convention signed by EU Member States in relation to the obligation to ensure the definition and certainty of the purpose for which this is done.

The agreement also contrasts with Art. 6 of the Convention concerning personal data.

---

[14] *Judgement of the Court of 3 September 2008, C-402/05 P e C-415/05, Yassin Abdullah Kadi c. Council*, in *www.europa.eu.*

[15] *Council Regulation of 29 May 2002*, Official Journal of EU, L 139, 2002.

For this particular category of personal data, the Convention provides that they may not be processed automatically if national laws do not establish appropriate safeguards.

The same agreement also does not allow an adequate protection of the right to correct personal data subject to treatment and thus it is contrary to Art. 8 of the European Convention for the protection of personal data.

The PNR agreement and the letter DHS, in fact, guarantee only the application of the law in force in the U.S. on the matter, such as the Patriot Act. But it is applicable only to U.S. citizens.

Nor is it true that the mere reference made by the DHS letter of this legislation ensure the extension of its scope to individuals holding the data processed regardless of the nationality of the same.

Previous agreements on cross-border transfer of personal data between EU and U.S. ensured a higher protection.

The agreement is contrary to Art. 8 of the European Convention on Human Rights as interpreted by the Strasbourg court.

In particular, analysing the prevailing case law of the European Court, it can be concluded that the collection and transmission of personal information by public authorities breach Art. 8.

On the basis of the criteria identified by the Court in its jurisprudence, that a treatment could be determined, must pursue a legitimate aim of public interest, and it must be proportionate.[16]

The Court held that in order to assess the proportionality of the treatment itself, it is necessary to verify compliance with the law on access to their data by the interested parties. The discipline mentioned does not respect the principle of proportionality.

The obligations from both are incompatible with the Convention on the Protection of Personal Data and with the provisions of the Convention for the Protection of Human Rights.

4. THE PROTECTION OF INDIVIDUALS AGAINST ACTS AFFECTING THE RIGHT TO PRIVACY

In the fight against terrorism and in the internet era, it is necessary to protect the international and European security, but also the fundamental rights. In particular it is necessary the judicial protection of individuals against the abuses of the Authority also in the fights against terrorism. At EU level, citizens can appeal to the Court of First Instance and then to the Court of Justice of the European Union, but we have seen that recent case

[16] Cfr. Judgement of European Court of Human Rights, n. 9248/81, of 26th of March 1987, Leander Vs Sweden, www.coe.int

law is not in favour of the protection of fundamental rights when dealing with the fight against terrorism. We must then determine whether the conclusion of the PNR is attributable to the states. In order to solve this problem we must refer to the legal basis on which the agreement was concluded.

The legal basis is Articles 24 and 38 EU Treaty. An analysis of these provisions easily shows the crucial role played by Member States in concluding such agreements.

Art. 24 states that the Council may decide by a qualified majority whether the agreement is expected to implement a common position or a joint action. It should be noted that these acts must be approved unanimously. Art. 24 refers to Art. 23, par. 2 which states that "If a member of the Council declares that, for important reasons of national policy, intends to oppose the adoption of a decision taken by qualified majority, a vote. The Council, acting by a qualified majority, requests that the matter be referred to the European Council for decision by unanimity".

The role of the States is essential in this case. Data processing must respect the principle of proportionality.

In this particular context, the Court has noted, on several occasions, that in order to assess the proportionality of the same treatment, states must guarantee the right of access to data. The agreement provides only for transferring data from European airlines to US authorities.

The agreement conflicts with the European Convention on Human rights.

The states are liable for the breach of the European Convention on Human Rights in the fight against terrorism.

5. CONCLUDING REMARKS

Many countries introduced extraordinary laws and policies and emergency legislation. We see the introduction of new surveillance power of the State in answers to terrorism and cyber-terrorism. Privacy was also affected by the use of very technologically advanced instruments of control.[17]

The administration of emergency has ultimately become condicio sine qua non for the maintenance of international security.

In the USA and UK many of these laws have come to be questioned in parliaments, through the media, the courts, and in the public sphere. Some have been seriously amended or found unconstitutional while others have been enhanced.

The program for intercepting telephone calls and e-mail authorized by Bush 2001 and renewed in subsequent years, was ultimately blocked for vi-

[17] Terrasi, L.M. 2007, *Trasmissione dei dati eprsonali e tutela della riservtezza: l'accordo tra Unione euroepa e Stati uniti del 2007, Rivista di diritto internazionale*, pp.375-389.

olation of the First and the Fourth Amendment. In particular, the Court of Detroit noted that "It is not possible to pursue the goal of security by depriving citizens of constitutionally guaranteed rights".

The administrative emergency, ultimately, must ensure the protection of human rights. The real problem is the disappearance of the temporary nature of the emergency requirement.

The doctrine held that in order to guarantee an adequate balance between fundamental rights and combating terrorism, it is appropriate to take precautionary measures to combat the threat in question. The problem of collective security against the terrorist threat should move from the emergency plan in order to attain prevention administration in the first moment, and finally the precautionary administration.

What is more significant, in view of the measures taken to combat international terrorism, will be the loss of the temporary nature of the emergency requirement.

In short, the emergency and the rules designed to adjust from temporary have become permanent.

The doctrine held that, in order to achieve an appropriate balance between fundamental rights and the fight against terrorism, precautionary measures are needed to combat the threat in question.[18]

The problem of collective security against the terrorist threat should move from the emergency plan, that of prevention first and then the precautionary.[19]

The aim should be to find models of public administration to limit the risks linked to terrorism. In this way the regulation of an increasingly less certain risk would meet the policy to act gradually against the urgency of the threat.

If we could apply the precautionary principle in the fight against terrorism, with the procedural and substantive content of the principle, as developed by the Court of Justice relating to the environment and health, we might conclude that the administrative action in this area would be enriched with a connotation of a technical nature.

If the precautionary principle to become the administrative method of action in the fight against the terrorist threat, the assessment of the appropriateness and validity of the measures would be needed.

In this way, when facing a less certain risk of a terrorist attack, it is necessary to respond gradually. In this perspective we could get two positive

[18] Cfr. De Leonardis, R.I. 2005, *Il principio di precauzione nell'amministrazione del rischio,* Milano.
[19] Cfr. Simoncini, *Legislazione antiterrorismo e privacy,* cit. p. 985.

effects. First, it is possible to secure provisional measures and make progressive adjustments that are commensurate with the threat.

Where the risk is only "hypothetical", the individual recipient of the measure could require the annulment of the issued decision before the Court of First instance on the basis of the lack of conditions that justify the adoption of precautionary measures.[20]

However even when we do not reach the application of precautionary measures, the states must apply the principle of proportionality, in accordance with the interpretation given by the Court of Justice and the European Court on Human Rights. The Court maintained that the proportionality test has to be applied by taking into consideration a number of factors, such as the nature of the rights affected and the duration of the measures.

The Court made clear that the States are bound to the continuous reassessment of the effectiveness of the measures adopted and to repeal if they are found inadequate to meet the danger.

A further element that plays an increasingly important role in assessing the measures of proportionality is the existence of safeguards against the abuse of emergency powers. When the Executive interferes on fundamental values, such as personal freedom or privacy, the derogating measures is proportionate only when it provides a meaningful degree of judicial or independent control.

However, we doubt that the EU law, today, ensured an effective remedy for those affected and, hence, that the measures do not meet the proportionality requirement.

[20] Cfr. De Leonardis, R.I. 2005, *Il principio di precauzione nell'amministrazione del rischio, cit.*