Quaderni di C.R.S.T.

Centro Ricerca Sicurezza e Terrorismo

Direttore Ranieri Razzante

Alessandro Lentini

Selected Issues in Counter-terrorism: special investigative techniques and the international judicial cooperation

Focus on the European Union

Pacini Giuridica

Realizzazione editoriale

Pacini Editore
Via A. Gherardesca
56121 Ospedaletto (Pisa)

Responsabile di redazione
Gloria Giacomelli

31.10.2018

Alessandro Lentini

Selected Issues in Counter-terrorism: special investigative techniques and the international judicial cooperation. Focus on the European Union.

This paper analyses the last trends of the Islamic terrorism, some of the special investigative techniques and the international cooperation, focusing on the situation in the European Union.

From the use of internet for terrorist purposes and the transnational nature of terrorism, new challenges and needs arise. States are changing their legislations and investigators are progressively adapting their methods to the terrorist exploitation of technology and the borderless nature of terrorism.

In this context, is essential to improve the international cooperation between judicial and law enforcement authorities.

This paper aims to show the existing criticisms in international, regional and national legislations and to propose alternatives to facilitate investigations on terrorism, in respect of fundamental rights.

Table of contents.

1. Terrorism and its evolution from 9/11

Even though the Islamic State is losing its territory[1], the jihadist terrorism is still one of the biggest threat to the international peace and security.

In fact, within the European Union, the number of suspects arrested for jihadist terrorism in 2017 was very high and the number of attacks was more than double of those carried out in 2016[2]. The deaths in the first 6 months of 2017 caused by jihadist attacks were 350[3].

Terrorism has changed since 2014 and this has been caused, mostly, by the activities and the impact of ISIL[4]. This change can be noted analysing the recruitment and training activities as well as the attack strategies.

In this times, terrorists are usually citizens of Western countries or people living in our cities since many years. This makes more difficult the control of extremist activities in our territories and allows terrorists to move freely from a country to another. They usually live in the suburbs[5], in degraded conditions and this facilitates their approach to radicalized environments. In particular, subjects can get radicalized in several ways. First, through their participation in radicalized environment, such as in mosques. Second, usually subjects get radicalized while they are in prison. In fact, a study conducted across Europe revealed that the 31 percent of terrorists began the radicalisation process while they are in jail[6]. Third, many subjects get radicalized on-line, using the propaganda made by ISIL, with magazines, handbooks, videos and short-movies. In fact , despite the degradation of IS organisational structures, the propaganda and networking via social media are still used by terrorists to spread their message for recruitment and radicalisation aims[7].

The training of terrorist and the attacks planning are also very different from the past. The attacks carried out by Al-Qaeda in the first 2000s were usually characterized by big money investments on training of terrorists and attack planning. For instance, the 9/11 terrorists were trained in hijacking and piloting; they checked directly the security measures in the airports and on planes, living and travelling into the borders of the United States[8] before to carry out the attack. It is easily understandable that all these activities had a cost, in terms of money and

[1] The US-led coalition against so-called Islamic State (IS) says 98% of territory once claimed by the jihadist group across Iraq and Syria has been recaptured.
"Islamic State and the crisis in Iraq and Syria in maps", BBC News (28th March 2018) <https://www.bbc.com/news/world-middle-east-27838034>, accessed 4th July 2018.
[2] The authorities arrested 705 suspects and the attacks have been 33.
Europol, European Union Terrorism Situation And Trend Report 2018 (TESAT) 22 https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 accessed 21th June 2018.
[3]Institute for Economics and Peace, Global Terrorism Index (2017) 59. <http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf> accessed 28th June 2018.
[4] *Ibid.*, 58.
[5] For instance, see the situation concerning the Banlieus in France.
[6] *Supra* note 3, 66.
[7] *Supra note 2*, 6.
[8] D. Johnston, '9/11 Congressional Report Faults F.B.I.-C.I.A. Lapses' New York Times (24th July 2003) https://www.nytimes.com/2003/07/24/us/9-11-congressional-report-faults-fbi-cia-lapses.html accessed 25th June 2018.

time as well[9]. Instead, in recent years, has decreased the sophistication in preparing and executing attacks[10].

Regarding the execution of attacks, we can recognize two phenomena. First, the attacks carried out by "returnees", the terrorists who came back (and are currently coming back) in Europe from Syria and Iraq, where they were trained and fought by and for the Islamic State. However, the latest trend revealed that the attacks are primarily carried out by terrorists who did not leave Western countries and who got radicalized and trained to the use of weapons and attack tactics on-line, through the material disseminated by ISIL[11].

From this difference in the planning and training activities, results a difference in the type of attacks. Despite the decrease of the sophistication of the attacks referred above, these are causing more deaths and casualties than any other attacks[12]. The attacks in the European Union resulted into indiscriminate killings, attacks on symbols of our culture or on authorities[13]. The last terrorist attacks were in fact carried out by shooting people with Kalashnikovs, suicide bombings and running over people with rented trucks[14].

This new trend has obviously some consequences. Firstly, it has reduced consistently the cost of a terrorist attack, in terms of money and time required for the preparation. At the same time, it has made the terrorist act accessible for everyone interested in. From this, it follows that terrorists cannot only be affiliates in one cell, but they can also be "solitary wolves" who did not have any contact with organized terrorist cells or ISIL being, instead, just inspired by them. Furthermore, it has made even more difficult to investigate in order to prevent a terrorist attack.

Consequently, the international community is facing new needs in the terrorism prevention and investigation: combating radicalization and the use of internet for terrorist aims, dealing with radicalized subjects who freely move from a country to another, the facility with terrorists can carry out this new kind of attacks, the phenomena of foreign fighters and returnees.

These circumstances brought States to adopt "emergency legislations"[15], focusing more on the necessity to prevent and prosecute terrorist acts rather than on the respect of human rights. Furthermore, there is a sort of "retrocession" of the criminalization line. In particular, it is possible to recognize the trend to criminalize preparatory conducts, such as planning to travel and join a terrorist organization[16]. The direct consequence is a sort of "osmosis" between criminal and intelligence investigations[17].

---

[9] The organization of the attacks costed between 400.000 and 500.000 US $. EN) 9/11 panel. 'Al Qaeda planned to hijack 10 planes' CNN News (Washington D.C., 17th June 2004) . http://edition.cnn.com/2004/ALLPOLITICS/06/16/911.commission/ accessed 15th June.

[10] *Supra* note 2, p. 5.

[11] *Ibid.*

[12] *Ibid.*

[13] *Ibid.*

[14] Respectively, the attacks in Paris (2015), the Manchester Arena Bombing (2017) and the Nice attack (2016).

[15] For instance, in France was imposed the State of Emergency in November 2015 and it finished in November 2017. S. Osborne, 'France declares end to state of emergency almost two years after Paris terror attacks' Independent (31 October 2017) <https://www.independent.co.uk/news/world/europe/france-state-of-emergency-end-terror-attacks-paris-isis-terrorism-alerts-warning-risk-reduced-a8029311.html> accessed 24th June 2018. However, the new French Counter-terrorism law includes into permanent legislation many of the emergency powers. A. Chrisafis, 'Macron's counter-terror bill risks France's human rights record, say UN experts', The Guardian (28th September 2017) <https://www.theguardian.com/world/2017/sep/28/macrons-counter-terror-bill-risks-frances-human-rights-record-says-un> accessed 24th June 2018.

[16] Daniela Curtotti, 'Criminal justice and intelligence in Italy: an increasing involvement, restricted by the law' (2018) 3 Processo penale e giustizia, 441.

[17] *Ibid*.

The international legislative framework is very fragmented: there are several UNSC Resolutions, Conventions related with transnational organized crime or terrorism and many European tools. However, there is still a sort of reluctance among States in cooperating in criminal matters and in sharing information about terrorism as well. In particular, there is low cooperation in sharing information not only between States, but also between law enforcement and intelligence agencies of the same Country. This is clear even considering the international legal tools, as will be further discussed.

Furthermore, there is also a lack of willingness to define common standards in the investigation. This makes even more difficult dealing with the existing tools of judicial cooperation.

In this paper, I will focus on the importance of some of the special investigative techniques, such as interception of communications and covert operations, trying to establish whether the current legal framework (if any) is respectful of human rights and in which measure. In the second part, I will analyse the current methods of international judicial cooperation in terrorism investigations and the cooperation between national law enforcement and intelligence agencies, within the European Union.

2. Special Investigative Techniques in counter-terrorism: interception of communications, surveillance and covert operations.

2.1. Communication interceptions.

The special investigative techniques are important in counter-terrorism because of the clandestine and complex nature of terrorism[18] and they are defined as those "applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aim[ed] at gathering information in such a way as not to alert the target persons" [19].

Within the special investigative measures, very useful in counter-terrorism are the interceptions of communications[20]. In fact, as referred above, many of the terrorist activities are carried out by means of communication.

Even though the use of special investigative techniques is encouraged by many provisions of international conventions[21], it is important to clarify that the definition of interception of communications is a domestic matter of the States. Nevertheless, it is possible to classify many types of interception of communications. The phone-tapping, which consists in intercepting a communication using the phone circuitry. The bugging, which refers to intercepting a communication taking place between two or more persons in a same place, usually making use of microphones or other audio and/or visual recording devices. The interception of

[18] 'The Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector' Global Counterterrorism Forum (February 7-8, 2012) 6.
[19] Recommendation CM/Rec(2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism OJ C148, Vol. 60, 2017.
[20] Tim Lister - Paul Cruickshank, 'Intercepted communications called critical in terror investigations' CNN (June 11, 2013) <https://edition.cnn.com/2013/06/11/us/nsa-data-gathering-impact/index.html> accessed 12th June 2018.
[21] United Nations Convention Against Transnational Organized Crime (Adopted 15th June 2000, entered into force 29 September 2003) 188 (UNTOC), art. 20.
United Nations Convention Against Corruption (Adopted 31th October 2003, entered into force 14th December 2005) 186 (UNCAC), art. 50.

communication online carried out, for instance, using malware and spyware on devices with access to internet.

Interception of communications demonstrated a big efficiency in combating terrorism and organized crime[22]. In fact, on one hand it allows to get information about one person or one group in a hidden way, leading to useful information in order to prevent or prosecute crimes as well; on the other hand, this method can be employed when it could be too risky using other methods, such as infiltrated agents or informants.

In these times, characterized by a huge use of internet, social media and chat by terrorists for many aims, interception of communications online play a big role in preventing terrorist activities as well as in prosecuting terrorists (or potential terrorists)[23]. However, terrorists often use encryption in order to communicate. Unlike Al-Qaida did[24], they usually communicate between apps already including encryption, avoiding the developing of encryption software, such as WhatsApp, Telegram, Facebook and so on[25]. These circumstances led law enforcement agencies to pretend collaboration by private providers, in order to gain possession of encrypted data[26].

Moreover, new methods are employed in order to intercept communications by mobile or laptop. In fact, law enforcement and intelligence agencies are often employing malware, such as *Trojan horse*. This is a type of virus which allows the "sender" to gain remote control of the device (phone, laptops, smartwatch etc.). Once the device is infected, the sender can remotely switch on the camera or the microphone, record, register keystrokes and so on[27].

It can be correctly stated that interception of communications is an invasive investigation method and because of this, it is necessary to take some precautions. There are several risks connected with a lacunose legislation, such as violating privacy of individuals, the freedom of expression or the principle of the fair trial. For this reason, States should adopt accurate legislations in this matter. Firstly, the interceptions shall be authorized and carried out by the competent authorities and under certain conditions; secondly, the treatment of the resulting data should respect the privacy of people intercepted; thirdly, the interceptions should be carried out in such a manner that allow the use of the information collected in courts, respecting

---

[23] Directive 2017/541/EU of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6.
The Directive defines various categories of terrorist acts and art. 21 sets that States "shall take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence […]. They shall also endeavour to obtain the removal of such content hosted outside their territory." Furthermore, when removal of the content is not feasible, States should take measures to block access to such content towards the internet users within their territory. The removal or block measures should be proportionate and necessary.

[24] Reuters Staff, 'Jihadi software promises secure Web contacts' Reuters (Dubai, January 18, 2008) <https://www.reuters.com/article/us-internet-islamists-software/jihadi-software-promises-secure-web-contacts-idUSL1885793320080118> accessed on June 14, 2018.
The article explains that Al-Qaida developed in 2007 an encryption tool called 'Mujahideen Secrets'.

[25] For a comprehensive picture of how terrorists use encryption, R. Graham, 'How Terrorists Use Encryption' (2016) 9 (6) CTCSentinel 20 <https://ctc.usma.edu/app/uploads/2016/06/CTC-SENTINEL_Vol9Iss614.pdf>

[26] 'Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU' Article 29 Data Protection Working Party' (April 11, 2018) <http://www.dataprotection.ro/servlet/ViewDocument?id=1476>

[27] J.J. 'Oerlemans, Investigating cybercrime' Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University (Leiden, 2017), 22.
<https://openaccess.leidenuniv.nl/bitstream/handle/1887/44879/Full_text_Investigating_Cybercrime.pdf?sequence=2> accessed 12th June 2018.

the right to a fair trial. In fact, "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence […][28]". According to the European Convention on Human Rights, "everyone has the right to respect for his private and family life, his home and his correspondence" and the public authority should abstain to interfere on this right unless, in accordance with the law, it "is necessary in a democratic society in the interest of national security, public safety […] for the prevention of disorder or crimes or for the protection of the rights and freedoms of others[29]". With regard to the interceptions by malware and taking into consideration that we spend most of the time with laptops and phones, even at home, the contrast with this right is even clearer[30].

However, the legislative trend is very different from these assumptions. For instance, the report of the United Nations Special Rapporteurs on the right to privacy states: "the terrorist attacks in Belgium, France, Germany and the United Kingdom created national and sometimes international moods, which gave priority to reactive and high-profile security responses over carefully nuanced approaches that would take into account security interests and the responsibility to protect their citizens' privacy"[31].

In 2015[32], the European Court of Human Rights has stated the "minimum safeguard" that States should adopt while legislating in this matter. The following requirements should be set out: "the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed"[33]. At the same time, laws should be flexible in order to deal with the rapid technological developments in communication[34]. However, despite the big use of this method of investigation and the issues "touched" by it, still there is not a legal tool aimed to define a clear common standard for interception of communications, neither at the international level nor at the European level.

Thus, depending on the State it is possible to recognize many definitions of interceptions as well as exist different legal frameworks regulating the necessary conditions and the methods in order to intercept communications.

However, from a general perspective, one distinction can be drawn between judicial and extra-judicial interceptions. The first ones are used in order to detect, investigate and prosecute a crime and are usually judicial acts; the second one are usually carried out for reasons of national security[35] and are usually administrative acts. This distinction is in a certain way the result of

---

[28] International Covenant on Civil and Political Rights (Adopted 19th December 1966, entered into force 23th March 1979) 171 (ICCPR) Article 17(1).

[29] European Convention on Human Rights as amended by Protocols Nos. 11 and 14 (Adopted 4th November 1950, entered into force 3th September 1953) Article 8.

[30] In Italy, the interceptions by malware have been allowed by the *d. lgs. 216/2017.*
Sara Bundtzen, 'Why you should know about Germany's new surveillance law' Open Democracy (30 October 2017) https://www.opendemocracy.net/digitaliberties/sara-bundtzen/why-you-should-know-about-germanys-new-surveillance-law accessed 20th June 2018. The article describes that also in Germany this method of interception has been permitted with the law adopted on 22 June 2016.

[31] 'United Nations Report of the Special Rapporteur on the right to privacy' (2018) A/HRC/37/62.

[32] *Zakharov vs. Russia* (2015) ECtHR, paragraph 231. <https://hudoc.echr.coe.int/eng#{"itemid":["001-159324"]}>

[33] The ECtHR also dealt with minimum safeguard appointed by the law in interception matters in *Szabó and Vissy V. Hungary* (2016) ECtHR. Available at <http://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf >

[34] *Supra* note 18, 6.

the shared taught for which terrorism (even the religious terrorism) is a matter of national security, important for the preservation of democratic States[36]. Depending also (but not only) on this distinction, interceptions can be carried out by the police or other law enforcement agencies; in other countries, this task is assigned to the intelligence agencies or, still, both of them. The pros and cons of interceptions carried out by law enforcement agencies or by the secret services will be further examined.

2.2. The interception of communications in Italy and the differences in other countries.

In order to clarify how many differences exist in the European legal framework, it can be useful to analyse the legislations of Italy and then briefly point out some analogies and differences existing in other countries.

Italy is dealing with organized crime and terrorism since a long time; for this reason, it had many chances to adequate its legislation to this threat and balance the security exigence with the respect of fundamental rights, as well as to develop strong skills in sharing information within the law enforcement and intelligence agencies. Also Spain has dealt with another type of terrorism since few years ago as well as Germany.

France, instead, has been hard hit by jihadist attacks in the last four years and it has upgraded its legislation in 2017. For many academics and NGO's, the new "Loi 1510-2017" is a "normalization" of the "*état d'urgence*"[37]. The U.K., adopted the criticized Investigative Powers Act adopted in 2016.

In the Italian Law, there are two regimes of interception of communications, distinguishing themselves on the moment in which are carried out. Both of them, constitute a derogation of the general rule stating that there are serious grounds (*gravi indizi)* that a crime has been committed and the interception is absolutely essential in order to keep on the investigation[38].

Regarding terrorism crimes, the authorization conditions set out above switch in "sufficient grounds to believe that a crime has been committed when the interception is necessary for investigative purposes[39]. This is the result of an extension of the special measures established to fight mafia and organized crime to terrorism crimes[40]. In any case, the interception has to be authorized by the judge for preliminary investigations (G.I.P.) and they can last up 40 days and can be renewed for up 20 days. In case of emergency, the interception can be ordered by the prosecutor and the judge will validate it *ex-post facto*, checking the existence of emergency reasons[41]. This type of interceptions is carried out by the Italian law enforcement agencies (State Police, Carabinieri and Guardia di Finanza).

The Italian system provides also another type of interception of communications not aimed to find evidence of a crime, but are finalized to prevent terrorism activities and direct the subsequent investigations. The preventive interceptions can be carried out by the law enforcement agencies as well as by the secret services (D.I.S., A.I.S.E, A.I.S.I). This special

---

[36] F Galli, Francesca Galli, (2016) 'The interception of communication in France and Italy – what relevance for the development of English law?' 20(5) IJHR https://www.tandfonline.com/doi/abs/10.1080/13642987.2016.1162412 accessed 18th June 2018 666, 669.

[37] OHCHR, 'France: UN expert says new terrorism laws may undermine fundamental rights and freedoms' (Paris/Geneva, 23 May 2018) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23130&LangID=E> accessed 8th June 2018.

[38] Italian Criminal Procedure Code, Art. 267.

[39] Italian Law 203 of 1991, Art. 13.

[40] The amendment is contained in Law 438 of 2001, Art. 3.

[41] *Supra* note 37, Art. 267 CPP.

technique of investigation was introduced onto the Italian legal system after the terrorism faced by law enforcement officers during the "Years of Lead".

The preventive interceptions are authorized by the public prosecutor of the district in which the person to be put under surveillance has the residence or operations should be executed. The Ministry of Interior detains the general competence to apply for this type of interceptions but, on his delegation, also the local commanders of the law enforcement agencies can apply in order to gain the authorization to carry out preventive interceptions. Furthermore, the Prime Minister or, on his delegation, the directors of the secret services can carry out preventive interceptions. However, in this case, the authorization is issued by the General Prosecutor's Office of the Court of Appeal of Rome[42], that also will check that there is no unnecessary duplication of activities between law enforcement forces and intelligence agencies. The duration of the interceptions is of 40 days, renewable for periods of 20 days. The communication intercepted by this method cannot be used in courts and are not considered as evidence. They can be used just in order to show that there are grounds to investigate.

In Spain, the interception of communications is regulated by the *Ley de Enjuiciamento Criminal*, amended by the *Ley Organica 13/2015.*

The judicial interceptions can be authorized and has to be motivated by the judge in order to investigate crimes punished with at least three years of prison, terrorism or organized crimes[43]. Furthermore, this method of investigation can be used when there are not other less intrusive means available and when the refuse to intercept communications could seriously prejudice the investigation[44]. The interception can be ordered by the judge or the competent authorities, the *Ministerio Fiscal* or the Judicial Police, can apply for it[45].

Unlike Italy, the interception can be carried out for an initial period of three months, renewable, for a maximum of eighteen months[46].

The interception of communications in Spain can be carried out in several ways, such as phone-tapping, online interceptions, malware interceptions, video and audio recording or the geographic localization[47].

Regarding the extra-judicial interception, the situation is very similar to the Italian case. Intelligence Services can use this method in order "to prevent, detect and provide for the neutralization of the activities that endanger, threaten or attack the security of the Spanish State and the stability of its institutions[48]".

Similar to Italy, Spanish intelligence needs the authorization of one specific Magistrate of the Supreme Court[49]. The evidence gathered by the intelligence cannot be used in Court[50].

---

[42] Italian Law n. 133. Of 2012, Art. 12.
[43] Spanish *Ley de Enjuiciamento Criminal*, amended by *Ley Organica* 13/2015, Article 579.
[44] *Ibid.*, Art. 588 bis a, 4 a-b.
[45] *Ibid.* Art. 588 bis b.
[46] *Ibid.* 588 3 g.
[47] I. FLORES PRADA, "Modernization" of the Spanish criminal justice in 2015. Partial reforms waiting the new code of criminal procedure" 2016 (5) Processo penale e giustizia, <http://www.processopenaleegiustizia.it/materiali/Contenuti/RIVISTE/Riviste%20pdf/2016/5_2016/27_Prada.pdf p.> 203, 212.
[48] Baker-Mackenzie, 'Surveillance Law Comparison Guide' (2017) <https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2017_surveillance_law.pdf?la=en> accessed on 2nd July 2018 246.
[49] Centro Nacional de Inteligencia 'Qué es el CNI' <https://www.cni.es/es/queescni/controles/controljudicial/> accessed 4th July 2018.
[50] *Supra* note 47, 259.

In the U.K., Secret Services do not need an authorization of the judicial power. The Secretary of State issues the authorization for reasons of national security, to prevent or detect serious crime, in relation to a mutual assistance request or for economic reasons concerning also national security and when it is necessary and proportionate to the aim[51]. A Judicial Commissioner has just to approve it, evaluating the subsistence of the requirements pointed out above[52]. The duration of a warrant changes according on its type[53]. However, the general duration is six months[54].

In Germany, there are three intelligence agencies that can carry out interception of communication. Furthermore, each Federal State can use this method of investigation through their own intelligence agencies[55]. Generally, German intelligence does not need a court order. In fact, this measure is ordered by the Federal Ministry of Interior and approved by a special commission. However, it can be approved *ex-post* if adopted in order to deal with imminent dangers or threat[56].

As can be noted, there exist some analogies but also deep differences between the European normative framework. These are the result of different legal culture, for sure, but also of the lack of an international or regional approach in regulating a delicate matter as the interception of communication. This can cause some difficulties when this investigative technique is used in the context of the international cooperation, as will be discussed in the next chapter.

2.3. Covert operations

The use of undercover agents is another special investigation technique, useful to investigate crimes that have been already committed as well as to collect information on a terrorist group before that a crime is committed. The use of undercover operations is encouraged by many legal tools that foresee the special investigative techniques[57].

Before the examination of the covert operations and despite the lack of a definition generally accepted, it is important to point out the difference between undercover agents and informants

The term "undercover agents" refers to a law enforcement officers or intelligence officers whose task is to collect information and evidence secretly, through the infiltration in a suspected terrorist organization. Instead, informants are persons (usually suspected criminals related to terrorists) who provide information to the authorities. In this paper I will analyse only the role of the undercover agent who are carrying out his activities online and not.

Regarding the methods of online undercover investigation, it should be distinguished between open source intelligence gathering operations and undercover law enforcement operations. The first category refers to general research of publicly information available on the internet[58]. This

---

[51] Investigatory Powers Act 2016 (19).
[52] *Ibid.*, 23.
[53] For an overview of the types of warrant, INTERCEPTION OF COMMUNICATIONS Pursuant to Schedule 7 to the Investigatory Powers Act 2016 - Draft Code of Practice (2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593748/IP_Act_-_Draft_Interception_code_of_practice_Feb2017_FINAL_WEB.pdf> accessed 5th July 2018 12.
[54] *Supra* note 50, 32.
[55] European Union Agency for Fundamental Rights, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update' (Imprimerie Centrale, Luxembourg 2017) 28.
[56] *Supra* note 47, 91-92.
[57] For instance, *Supra* note 21.
[58] UNODC, Foreign Terrorist Fighters Manual for Judicial Training Institutes South-Eastern Europe (2017) p. 30.

information can be gathered and collected manually or automatically, with the help of specific software. The second one refers to real undercover operations, carried out by specialized law enforcement or intelligence officers under an authorization of the competent authority.

Law enforcement officers can exploit the functions of internet and social network as terrorists exploit them. This can be better understood using one scenario. For instance, in order to investigate and prosecute terrorists making propaganda and activity of recruitment on social networks and other chat programs, investigators can just observe the suspect's behaviour, monitoring his activities and access to several information on his life, such as friends, personal information and so on[59]. Then, the undercover agents can enter in contact with them, creating fake profile on the specific social network. In this way, they can pretend to be interested in the propaganda and in the recruitment, obtaining information and evidence about those activities. Thus, depending on the aim of the undercover operation, the covert agent can introduce himself onto the terrorist cell or just gather the information he needs.

2.4. What are the issues of undercover operations?

As for the interception of communication, on one hand the undercover operations can be a key method in order to collect information and evidence about terrorist groups and activities; on the other hand, there are several issues to whom States should pay attention.

Some of these issues are commons between covert operations online and not while others depend on the specific type of operation.

Both categories of covert agents should receive a specific training on the undercover activities. For instance, covert agents should be trained to the correct use of social network and others online communication platforms, as well as to the methods of infiltration in a terrorist cell or organization. This training should include not only technical and professional skills, but also should consider legal issues[60].

In the case of online covert operations, covert agents should be trained also to the processing of information gathered and to "understand when and how to get a social networking account shut down and preserved for evidentiary purposes"[61].

Apart from that, important issues arise with respect to the right to a fair trial and the human rights. In fact, undercover operations should ensure the suspect has a fair trial and that the human rights of the agents are fully respected.

So, regarding the first point, covert agents should be trained also to the techniques to avoid the entrapment of the suspect(s). In particular, following a definition of entrapment[62], covert agents cannot act in such a way that induce or instigate a suspect to commit a crime that, otherwise, he would not have committed. In fact, this conduct would qualify as the conduct of the agent provocateur[63].

On this regard, an important sentence of the European Court of Human Rights define the line between the activity of the covert agent and agent provocateur. In *Ramanauskas v. Lithuania*, the Court held "police incitement occurs where the officers involved—whether members of the

[59] *Supra* note 27, 31- 32.
[60] *Supra* note 27, 49.
[61] *Ibid.* 50.
[62] Entrapment may be defined as "the act of government agents or officials that induces a person to commit a crime he or she is not previously disposed to commit". Legal Dictionary <https://legal-dictionary.thefreedictionary.com/entrapment> accessed 26th June 2018.
[63] Michael Kellett et al., Human Rights in Counter-Terrorism Investigations (Warsaw 2018, OSCE) 41.

security forces or persons acting on their instructions—do not confine themselves to investigating criminal activity in an essentially passive manner, but exert such an influence on the subject as to incite the commission of an offence that would otherwise not have been committed […][64]". According to the same sentence, " […] all evidence obtained as a result of police incitement must be excluded"[65].

Regarding the second point, especially in conventional undercover operations, the State must protect the human rights, of the agent(s) as well as those of the suspect(s). In fact, States should provide legal framework concerning also the activities in which the agent can participate and in what extent. For instance, covert agents cannot participate in the violation of fundamental human rights, like killing, torture and ill-treatment. In fact, for these acts there is an absolute prohibition.

However, also in this case, there is not a common international legal framework. The consequence is that the undercover operations are regulated in different manner depending on the State and this makes even more difficult the international cooperation between States countering terrorism.

3. THE INTERNATIONAL COOPERATION BETWEEN JUDICIAL AND LAW ENFORCEMENT AUTHORITIES.

3.1. The approach of United Nations and the universal legal framework regarding the cooperation in investigating terrorism.

In this globalized world, characterized by freedom of movement allowing people to move from a country to another and by the use of internet for countless, legal and illegal aims, terrorism has become an international threat. In fact, a terrorist attack can be prepared in one country and be carried out in another, can hit people of different nationalities in a same place, people can move to some country to get trained in the use of weapons and so on. From a European perspective, it is even clearer if we take into consideration the absence of borders within the European Union.

Furthermore, the broad use of internet for propaganda, training, radicalization, recruitment and so on brings the phenomena to an international level.

For this reason, international cooperation against terrorism is so important. However, the concrete efforts made up now appear insufficient and, perhaps, directed in the wrong direction. The lack of international cooperation has been indicated as the reason of the failure in preventing terrorist attacks[66].

The United Nations underlined at the very first moment the necessity to cooperate against international terrorism.

The Resolution 1373 adopted on 28th September 2001 by the Security Council decided that "Afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts,

---

[64], *Ramanauskas v. Lithuania* (2008) ECtHR para 56.
[65] *Ibid*., 60.
[66] K B Kanat, 'Lack of cooperation against global terror responsible for London attack' Daily Sabah (June 4, 2017) <https://www.dailysabah.com/columns/kilic-bugra-kanat/2017/06/05/lack-of-cooperation-against-global-terror-responsible-for-london-attack> accessed 1st July 2018.

including assistance in obtaining evidence in their possession necessary for the proceedings"[67]. The same Resolution invites States to intensify the exchange of operational information, cooperate through bilateral and multilateral agreements and ratify and fully implement the universal instruments against terrorism[68].

Regarding the implementation of cooperation in terrorism investigations, the Security Council issued others resolutions. The Resolutions 2178 invites States to implement the cooperation against terrorism and Foreign Fighters, through sharing of information in order "to identify foreign terrorists, the adoption of best practices and also through acting cooperatively, when taking national measures to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts"[69]. Furthermore, the Security Council recalls also the Resolution 1373 adopted 2001 and encourages Interpol to intensify its efforts against terrorism and foreign fighters, including the use of "Interpol Special Notices[70] to include foreign terrorist fighters"[71].

In order to deal with the new phenomena of the so-called "returnees", the Security Council has adopted the Resolution 2368 of 2017. This resolution invites States "[…] to improve international, regional, and sub-regional cooperation to address the issue of foreign terrorist fighters returning to their countries of origin, transiting through, traveling to or relocating to or from other Member States, including through increased sharing of information, in accordance with domestic and international law, for the purpose of identifying such movement of foreign terrorist fighters […]"[72].

Furthermore, also the United Nations Convention against Transnational Organized Crime establishes the duty to cooperate in investigation and proceedings. In particular, regarding special investigation techniques, art. 20 UNTOC encourages the conclusion of bilateral or multilateral agreements or arrangements[73]. Also, art. 27 UNTOC states an obligation to cooperate between law enforcement agencies, trough the establishment of communication channel between competent authorities, in order to facilitate the exchange of information about suspects and criminal activities[74].

However, in order to give concreteness to these premises, it is necessary that States upgrade their legislations.

Thus, the United Nations are making considerable efforts in order to sensitize States to improve cooperation among them, providing them legal basis to do so.

3.2. The international cooperation in investigations in the European Union.

---

[67] UNSC Res. 1373 (28th September 2001) para 2(f).
Furthermore, this Resolution also established the Counter – Terrorism Committee (CTC).
[68] *Ibid.*, 3.
[69] UNSC Res. 2178 (24th September 2014) para 11.
[70] For an overview of Interpol Special Notices see Interpol 'Special Notices' https://www.interpol.int/INTERPOL-expertise/Notices/Special-Notices accessed 7th July 2018.
[71] *Supra* note 68, para 13.
[72] UNSC Res. 2368 (20th July 2017) para 39. For other UNSC Resolutions, see <http://www.un.org/en/sc/documents/resolutions/> accessed 3rd July 2018.
[73] *Supra* note 21, para 2: 'For the purpose of investigating the offences covered by this Convention, States Parties are encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level. Such agreements or arrangements shall be concluded and implemented in full compliance with the principle of sovereign equality of States and shall be carried out strictly in accordance with the terms of those agreements or arrangements.'
[74] *Ibid.*, para 1.

The Single European Act, signed in 1986 by the twelve Member States, already stated that States "shall also co-operate in the combating of terrorism, crime, the traffic in drugs and illicit trading in work so fart and antiques"[75]. However, this was a generic statement of good purposes made by Member States. During the next years, especially after the events of the 9/11, the European Union came back on the topic, renewing the commitment to cooperate between States in the matter of the judiciary cooperation[76].

However, the cooperation between States cannot disregard a certain level of harmonization of criminal law in domestic systems. Let's say, to establish a working cooperation systems is not possible if one certain conduct constitutes a crime in one State while it is not recognized as a crime in another one.

This is why the legislative interventions made by the European Union were characterized by a certain reticence of States in concretely cooperating and sharing information. This is because criminal law is still considered as reflex of the state sovereignty and terrorism is seen as a matter of national security.

Even though there exist these limits, there have been important development in the judiciary cooperation between member States.

In this part of the paper, I will focus my attention on the analysis of the European tools aimed to implement the cooperation between States in sharing information and collecting evidence in the context of counter-terrorism investigations.

3.3. The European Order of Investigation.

The assumption of the European Investigation Order is the framework decision 2008/978/JHA adopted by the Council of Europe[77], stated the principle of mutual recognition in order to collect evidence to be used in criminal proceedings[78]. However, this was limited by the application of this instrument to existing evidence in the requested State[79].

From these circumstances arises the need for a new instrument able to facilitate the sharing of evidence (existing and not) between member states. This instrument is the European Investigation Order, adopted by the Directive 2014/41/UE.

According to article 1 of this Directive, this tool is a "judicial decision which has been issued or validated by a judicial authority of a Member State (the issuing State) to have one or several specific investigative measure(s) carried out in another Member State (the executing State) to obtain evidence in accordance with this Directive"[80]. The request can concerns also evidence that are already in possession of the executing State and it can be requested by a suspected or his lawyer.

---

[75] Single European Act, (1986) OJ L 169 1.
[76] Council Framework Decision of 13 June 2002 on combating terrorism (2002) OJ L 164 3 and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (2008) OJ L 330 21.
[77] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (2008) OJ L 350 72.
[78] Ion Rusu, European Investigation Order in Criminal Matters in the European Union: General Considerations. Some Critical Opinions (2016) 6 Juridical Trib. 56, 59.
[79]Directive 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters (2014) OJ L 130 1, para 4.
[80] *Ibid.,* art. 1.

The European Investigation Order (EIO) can be requested for any investigative measures, unless the Joint Investigation Teams, which are still regulated by art. 13 of the "Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union"[81].

The authority of the "issuing State" (issuing authority) has to respect some conditions. In fact, it can issues the EIO only if the same is necessary and proportionate for the purpose of the proceedings established in Article 4 and the investigative measures requested in the EIO "could have been ordered under the same conditions in a similar domestic case"[82]. On one hand, this kind of control is important because it brings to a "European level" the domestic rules regarding the admissibility of methods of investigation. For instance, if State X issues a EIO to Italy in order to obtain the interception of communication, the Italian authority would require a previous authorization by the judge (G.I.P.). Furthermore, this control makes easier the use of the evidence formed by the EIO in courts.

On the other hand, the respect of the necessity and proportionality requirements can be considered wholly respected by the issuing authority considering his domestic law but it cannot be the same for the executing authority, which has not any competence in evaluating it[83].

The request is directly transmitted from the authority of the issuing State to the authority of the executing State "by any means capable of producing a written record under conditions allowing the executing State to establish authenticity"[84].

The issuing authority can also request that some authorities of the issuing State participate and assist the executing authorities in carrying out the investigative actions requested. In this case, the authorities sent to the executing State are bound by the law of that State.

The executing authority should recognise an EIO without any further formality and execute it in the same way and under the same modalities as if the investigative measure requested had been ordered by an authority of the executing State[85]. However, "the executing authority shall comply with the formalities and procedures expressly indicated by the issuing authority unless otherwise provided in this Directive and provided that such formalities and procedures are not contrary to the fundamental principles of law of the executing State". It means that the principle *forum regit actum* applies to every EIO unless to those which contain the request for certain investigative measures, specifically regulated in Chapter IV of the Directive[86]. So, the procedural framework will be totally included in the EIO, that is available only for the executing and issuing authority. Because of this, it is really difficult that article 8 ECHR will be respected. This provision states that any interference with the right to respect for his private and family life, his home and his correspondence has to be in accordance with the law. It means that the law should be accessible[87].

In any case, the decision about the recognisance or the execution of the EIO should be adopted no later than 30 days after the receipt of the EIO[88].

---

[81] *Ibid.*, art. 3.
[82] *Ibid.*, art. 6.
[83] I. Armada, "The European Investigation Order And The Lack Of European Standards For Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?" (2015) 6(1) NJIL 9 15 <http://journals.sagepub.com/doi/abs/10.1177/203228441500600103> accessed 2nd July 2018.
[84] *Supra* note 78, art. 7.
[85] *Ibid.*, art. 9.
[86] *Ibid.*, from article 22 to art. 30.
[87] *Margareta and Roger Andersson v. Sweden* (1992) 14 EHRR para. 75.
[88] *Supra* note 78, art. 12(3).

Even though as can be noted the European Investigation Order constitutes a big step forward to a concrete judicial cooperation, the domestic systems are still and completely respected. In particular, the differences existing between legislations are taken into consideration and the same Directive relies to the manner in which Member States will implement this tool. In fact, the executing authority can recourse to an alternative investigative measure in three occasions. First, when the investigative measure indicated by the issuing State does not exist under the law of the executing State. Second, when the investigative measure requested by the issuing State cannot be applied in a similar case under the domestic law. Third, the executing authority can select a different investigative measure able to achieve the same result by less intrusive means than the investigative measure requested by the issuing authority[89]. This third possibility on one hand constitutes a limit to the mutual recognition approach of the Directive but on the other hand it is perfectly understandable. In fact, the executing authority surely can better evaluate whether a less intrusive measure exists in the domestic system[90]. In any case, these solutions are not possible if the EIO is issued for certain investigative measures, such as information or evidence which are already in the possession of the executing authority, information contained in databases held by police or judicial authorities and other types of evidence or information listed in art. 10[91].

The executing authority can refuse the execution of the EIO in the cases listed by art. 11. For instance, when there is an immunity or a privilege under the law of the executing State or when the execution of the EIO is a risk for the national security, jeopardize the security of the information source or it involves the use of classified intelligence information[92]. In particular,

---

[89] *Ibid*, art. 10.

[90] F Zimmermann et al., Mutual Recognition and its Implications for the Gathering of Evidence in Criminal proceedings: a Critical Analysis of the Initiative for a European Investigation Order (2011) 1(1) EUCLR 56, 69.

[91] *Supra* note 78, 10(2): "Without prejudice to Article 11, paragraph (1) does not apply to the following investigative measures, which always have to be available under the law of the executing State: (a)the obtaining of information or evidence which is already in the possession of the executing authority and the information or evidence could have been obtained, in accordance with the law of the executing State, in the framework of criminal proceedings or for the purposes of the EIO; (b) the obtaining of information contained in databases held by police or judicial authorities and directly accessible by the executing authority in the framework of criminal proceedings; (c) the hearing of a witness, expert, victim, suspected or accused person or third party in the territory of the executing State; (d) any non-coercive investigative measure as defined under the law of the executing State; (e) the identification of persons holding a subscription of a specified phone number or IP address."

[92] *Ibid.* 11(1): "Without prejudice to Article 1(4), recognition or execution of an EIO may be refused in the executing State where: (a) there is an immunity or a privilege under the law of the executing State which makes it impossible to execute the EIO or there are rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media, which make it impossible to execute the EIO; (b) in a specific case the execution of the EIO would harm essential national security interests, jeopardise the source of the information or involve the use of classified information relating to specific intelligence activities; (c) the EIO has been issued in proceedings referred to in Article 4(b) and (c) and the investigative measure would not be authorised under the law of the executing State in a similar domestic case; (d) the execution of the EIO would be contrary to the principle of ne bis in idem; (e) the EIO relates to a criminal offence which is alleged to have been committed outside the territory of the issuing State and wholly or partially on the territory of the executing State, and the conduct in connection with which the EIO is issued is not an offence in the executing State; (f) there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter; (g) the conduct for which the EIO has been issued does not constitute an offence under the law of the executing State, unless it concerns an offence listed within the categories of offences set out in Annex D, as indicated by the issuing authority in the EIO, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years; or (h) the use of the investigative measure indicated in the EIO is restricted under the law of the executing State to a list or category of offences or to offences punishable by a certain threshold, which does not include the offence covered by the EIO".

considering that terrorism is a matter of national security and that the general approach in Europe is to give even more powers to intelligence in counter-terrorism, this cause of rejection of an EIO could be used as a "loophole".

The executing authority can postpone the execution of the EIO if it could prejudice an on-going criminal investigation or prosecution or the objects, documents, or data concerned are already being used in other proceedings[93].

If does not intervene neither a refuse nor a postponement, the executing authority has to execute the investigation measure requested as soon as possible and, in any case, not later than ninety days by the decision on the recognisance or execution[94]. Considering that, as noted before, the judicial cooperation often meets the reluctance of States, the presence of precise terms within which to decide and execute the EIO is very important.

The Directive 2014/41/EU sets also specific rules regarding determined investigation measures[95]. I will analyse only the provisions concerning the special investigative techniques taken into consideration in the previous chapter: the undercover operations and interception of communications.

The authority of the issuing State can issue an EIO in order to request the executing State to give assistance in the investigations by officers acting under covert identity[96]. The issuing authority has to specify in the EIO the reasons why covert investigations could be relevant for the proceedings of that crime and the decision on the execution of this EIO will be taken by the executing authority, according to its domestic law[97].

The execution authority has the exclusive right to direct, act and control of the covert operations. However, the issuing State and the executing State have to agree on the duration and the detailed conditions of the covert investigation as well as on the legal status of the officers involved in the covert operations, according to their national laws and procedures[98].

Article 29 sets two further reason to refuse the execution of an EIO with respect to those listed in article 11. In particular, the executing authority may refuse the EIO if the covert investigations would be not allowed in a domestic case and if it has not been possible to agree on the arrangements for the covert investigations[99].

The Directive states that an EIO can be issued also in order to request the executing authority to intercept communications. It can happen that more than one Member State is able to give technical assistance in the operation: in this case, the EIO should be issued only to one of them.

The EIO concerning the interception of communications has to contain not only the reasons why this investigative measure is considered useful for the specific criminal proceedings but also the information in order to identify the subject of interception, the duration of the interception and sufficient technical data, in particular the target identifier, to ensure that the EIO can be executed[100].

Furthermore, paragraph 2 specify: "Paragraphs 1(g) and 1(h) do not apply to investigative measures referred to in Article 10(2)".

[93] *Ibid.*, art. 15(1).

[94] *Ibid.*, art. 12(4).

[95] *Ibid.*, from art. 22 to art. 30.

[96] *Ibid.*, art. 29.

[97] *Ibid.*, para 2.

[98] *Ibid.* para 4.

[99] *Ibid.*, art. 29(3).

[100] *Ibid.*, art. 30(2).

The issuing and executing authorities have to agree if the interceptions have to be carried out by "transmitting telecommunications immediately to the issuing State or intercepting, recording and subsequently transmitting the outcome of interception of telecommunications to the issuing State"[101].

Furthermore, as for the covert investigations, the executing authority can refuse to execute the EIO if the interception of communications would be not allowed in a similar domestic case.

Moreover, "the executing State may make its consent subject to any conditions which would be observed in a similar domestic case"[102].

At this point, it is possible to point out some final considerations on this tool.

Firstly, it should be considered that, as stated above, there are notable issues regarding the respect of human rights by this directive[103].

Secondly, also in the analysis of this directive, it can be noted the lack of a legal tool establishing minimum European standard for investigative measures it is an obstacle also for the judicial cooperation based on the mutual recognisance.

Thirdly, the effective contribution of the EIO is deeply mined by the differences existing between Member States' domestic systems.

3.4. Joint Investigation Teams.

The United Nations Convention against Transnational Organized Crime (UNTOC), adopted in 2000, still called on States to conclude multilateral agreements regarding the establishment of joint investigative bodies[104].

At the European level, the Joint Investigation Teams (JIT) was encouraged by the Tampere European Council[105] and was introduced in the European legal framework in the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, adopted on the 29th of May (Convention). However, in order to avoid the ratification process and due to the immobility of States[106], the Council of the European Union adopted the Framework Decision on Joint Investigation Teams (2002/465/JHA)[107]. The consequence is that the JIT has a double legal basis in the European Law and, especially in the past, it caused some problems between States that implemented the JITs according to the Convention or the Framework Decision[108].

---

[101] *Ibid.*, para 6.
[102] *Ibid.*, para 30.
[103] For other issues with respect to human rights, *supra* note 82.
[104] *Supra* note 21, art. 19.
[105] Tampere European Council, 15-16 October 1999, "Presidency conclusions", paragraph 43: "[…] The European Council calls for joint investigative teams as foreseen in the Treaty to be set up without delay, as a first step, to combat trafficking in drugs and human beings as well as terrorism. The rules to be set up in this respect should allow representatives of Europol to participate, as appropriate, in such teams in a support capacity." http://www.europarl.europa.eu/summits/tam_en.htm, accessed on 5th July, 2018.
[106] For instance, Italy ratified the Convention in 2017.
[107] Council Framework Decision of 13 June 2002 on joint investigation teams (2002/465/JHA) (2002) OJ L 162 1.
[108] See C Rijken, "Joint Investigation Teams: principles, practice, and problems Lessons learnt from the first efforts to establish a JIT" (2017) Utrecht Law Review 13(2), 99 – 118.

According to article 13 of the Convention[109], JIT can be defined as an international cooperation tool based on an agreement between competent authorities of two or more States, established for a limited duration and for a specific purpose, to carry out criminal investigations in one or more of the Member States. The authorities involved may be both judicial and law enforcement.

In particular, a JIT can be set up in two cases. First, when a Member State's criminal investigation requires difficult and demanding investigations having links with other Member States. Secondly, when some Member States are carrying out criminal investigations and the circumstances need a coordinated action in the Member States involved.

The leader of the JIT is a representative of the competent authority from the Member State in which the team operates and he acts within the limits established under his national law. However, the JIT, while is carrying out the investigations, has to respect the law of the Member State in which it operates.

The JIT shall carry out its operations in accordance with the law of the Member State in which it operates, taking into consideration the agreement between the competent authorities that settled up the JIT.

With regard to the members of team, those who are not from the State in which the JIT operates are called "seconded". They are entitled to attend when the investigations are carried out in the States involved, unless the leader of the JIT team, for particular reasons and in accordance with the law, decides otherwise. Moreover, seconded members of the joint investigation team may be entrusted by the leader of the JIT to take certain investigative measures in the State in which the JIT operates, if it is agreed between the competent authorities of Member States involved.

Furthermore, in the JIT can participate also other "external subjects". The competent authorities of the State of operations can ask for assistance of other Member States different by those settled up the team and, also, of third States. In addition, it can be agreed that different persons from the representatives of the Member States involved in the JIT can participate in the activities of the JIT. For instance, they could be officers of institutions established pursuant to the Treaty on European Union. In this context, in fact, Europol and Eurojust play an important role[110]. Lastly, all the members of the JIT are encouraged to share the information available in their country regarding the investigation being carried out by the JIT, within the limits established by their domestic laws.

With respect to the information lawfully collected during the JIT activities, they can be used for many purposes, including those for which the team has been set up. Depending on the prior consent of the Member State where the information became available, the information can also be used in order to detect, investigate or prosecute other criminal offences. The Member State interested can refuse to give its consent only when such use could harm criminal investigation ongoing in its territory or when the State could refuse mutual assistance.

Furthermore, the information can be used in order to prevent an immediate and serious threat to public security or for other purposes that are agreed between Member States participating in the team.

[109] Most of the provisions of the Convention have been copied into the European Union Framework Decision of 2002 on Joint Investigation Teams. This Decision just adds two provisions regarding civil and criminal liability of the officers involved in the JIT. See articles 2 and 3 of the Framework Decision cited above.

[110] E Bakker – J Powderly, "Joint Investigation Teams Added Value, Opportunities and Obstacles in the Struggle against Terrorism" (2011) ICCT International Centre for Counter-Terrorism - The Hague, pages 4 – 5.

Making a brief comparison between this tool and the EIO analysed in the previous section, it can be noted that the JIT is perhaps more flexible than the EIO, allowing real cooperation between judicial and law enforcement authorities coming from different States. In fact, while the JIT is characterized by full powers of officers on foreign soil and by a common investigative interest and goal, in the case of an EIO the investigative strategy is almost fully decided by the issuing authority[111]. Furthermore, the JIT activities can be carried out perhaps faster, because of the absence of formalities in communication and sharing information within the team[112].

However, also the Convention and the Framework Decision rely on how Member States implement (or have implemented) the JIT in their domestic system. Furthermore, the JIT is also based on the principle of mutual recognition (perhaps even more than the EIO) and on the trust between States. For this reason, this tool can suffer the lack of European common investigation standards.

3.5. The role of Europol and Eurojust.

Europol[113] deals with the improvement of the cooperation between law enforcement agencies in the European Union in order to prevent and combat serious crimes[114], mostly through the facilitation of the exchange of information[115]. It is not an executive police force with the autonomous authority to conduct its own investigations.

In particular, Europol can carry out several activities. Firstly, collect, store, process, analyse and exchange information, including criminal intelligence. Secondly, coordinate, organise and implement investigative and operational actions of Member States. Thirdly, it can participate in joint investigation teams, as well as propose it to Member States[116]. Lastly, Europol can also ask Member States to initiate, conduct or coordinate an investigation.

Each Member State designates a national unit, which is the liaison body between Europol and the Member State[117]. In January 2016 Europol created the European Counter Terrorism Centre (ECTC), an operations centre appointed in order to strengthen its response to terrorism[118].

Europol has the power to deploy its crime analysts to Member States in order to help them in investigations[119].

---

[111] R. Zaharieva, "The European Investigation Order and the Joint Investigation Team—which road to take: A practitioner's perspective" (2017) 18(3) ERA Forum, 397 407.
[112] Ibidem, p. 407.
[113] Europol is now governed by the Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) OJ L 135 53, which aligns the current framework of Europol (Council Decision 2009/371/JHA) with the requirements of the Treaty of Lisbon.
[114] The comprehensive list of crimes is pointed out in annex 1 to the Regulation.
[115] O. Bureš, 'Intelligence sharing and the fight against terrorism in the EU: lessons learned from Europol' (2016) 15(1) European View 57, 59 https://link.springer.com/article/10.1007/s12290-016-0393-7 accessed 4th July 2018.
[116] For the comprehensive tasks list, *supra* note 112, art. 4.
[117] *Ibid.*, art. 7.
[118] Europol, European Counter Terrorism Centre – ECTC <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc> accessed 6th July 2018.
[119] For instance, Europol analysts were deployed in France in 2015, after the attacks occured in Paris. More recently, four specialists were sent to Spain to support the Spanish authorities in investigations that brought to the arrest of 3 persons accused to recruit and finance terrorists. Europol, 'Successful counter-terrorism operation

The information regarding criminal activities and suspects are collected and exchanged on several databases and platforms, such as Europol Information System (EIS), Secure Information Exchange Network Application (SIENA) and Europol Platform for Experts (EPE).

Eurojust has been created in 2002 by the decision 2002/187/JHA, amended in 2003 and 2008[120] and it is constituted by 27 national members "seconded" to The Hague. Its role is to improve the coordination and cooperation between the competent authorities of the Member States, of investigations and prosecutions in their territory, particularly by facilitating the execution of or requests for, and decisions on, judicial cooperation. The list of crime for which Eurojust has competence is the same established for Europol.

Eurojust can act on initiative of one of its members or as a college. In any case, it can persecute its aims in several ways[121]. For instance, it can ask Member States to undertake an investigation, to coordinate between them, to set up JIT's, to take special investigative techniques, cooperate with the European Judicial Network and so on.

In order to carry out its activities, both Europol and Eurojust can access information available on several databases containing a huge number of information provided also by the private sector, regarding suspects and not. Some examples of these databases are the Schengen Information System, the Passenger Name Record[122]. Furthermore, also the States are progressively use more and more databases in order to monitor terrorist suspects. These circumstances bring to problems with respect human rights but, also, with respect to the prevention and investigating activities, as will be further discussed in the next chapter.

4. Conclusions.

The Islamic terrorism has evolved deeply and it keeps on changing. In particular, the frequent use of technologies for several purposes and the transnational nature of terrorism require more efforts by the international and regional organizations as well as by the States in their relationships. These efforts should be directed to adopt legislations balancing the respect of Human Rights and the need to guarantee national security. Contrarily, States seem to prioritize the national security rather than balancing the two values[123].

---

in Tenerife' <https://www.europol.europa.eu/newsroom/news/successful-counter-terrorism-operation-in-tenerife> accessed 6th July 2018.

[120] Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (2003) OJ L 245 44 as well as Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (2009) OJ 138 14.

[121] 2002/187/JHA, articles 6-7.

[122] For a general overview on the P.N.R, European Commission, 'Passenger Name Record (PNR)' <https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en> accessed 5th July 2018. For a general overview on the SIS, European Commission, 'Schengen Information System' <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en> accessed 5th July 2018.

[123] For instance, see *Supra* note 37.

Interception of communications are very useful in order to prevent or prosecute criminal acts. However, States have different requirements, conditions and limits in order to initiate and carry out interceptions as well as to the use of information gained by this investigative technique. This is a problem for two reasons. First, because there are different levels of respect of human rights. Secondly, because it makes more difficult the international cooperation[124]. In this sense, it could be useful adopting an international legal tool regarding the minimum standards that should be respected while legislating in this matter. Doing this for interception of communications regarding every crime is utopic, but it could be done with respect to terrorist offences. The same conclusion can be drawn with regard to covert operations.

The role of intelligence agencies is very important in democracies. However, the competences between law enforcement and intelligence agencies should be kept separate. In fact, on one hand the main task of intelligence agencies is to collect information regarding threats, under different rules with respect to those regulating the police activity. On the other hand, they usually don't reveal anything about their job[125]. So, it is difficult to ensure cooperation between law enforcement and intelligence agencies in the same national framework[126] and it is even more difficult to have international cooperation[127]. However, it seems that States are privileging the activities of intelligence agencies. In this context, it should be say also that to give a priority role to databases in investigations does not pay. Firstly, is very problematic with respect to human rights. Secondly, having a lot of information does not correspond to have more security. For instance, France claimed to have 15000 terrorist suspects in their database[128]: nevertheless, a huge amount of resources is required to monitor all of them.

International cooperation between judicial and law enforcement authorities and their specific training should be prioritized. Europol, Eurojust as well as the JITs and EIOs are the first steps in a cooperation system that has not a stable foundation. In particular, it should be given concreteness to the principle of mutual recognition in criminal matters. For instance, the EIO still suffers a lack of sharing of this principle. In order to ensure the mutual recognition and to reach a good standard in international cooperation, it is necessary to work on the integration of different legal systems.

Also the European Public Prosecutor's Office (EPPO)[129], which has competence with criminal offences affecting the financial interests of the European Union, constitutes a further

[124] See the example provided at page 15.
[125] A. Spataro, 'Politiche della Sicurezza e Diritti Fondamentali' in Questione Giustizia, Terrorismo Internazionale. Politiche della Sicurezza. Diritti Fondamentali. (2016) 167, 216. <http://questionegiustizia.it/speciale/2016-1.php> accessed 8th June 2018.
[126] Apart from the U.S. example cited in 'Introduction', see R. Kreissl, 'Terrorism, mass surveillance and civil rights'< https://www.cepol.europa.eu/sites/default/files/26-reinhard-kreissl.pdf> accessed 25th June 2018, 5-6.
[127] *Supra* note 124.
[128] M. Nikolaeva, 'France tracking 15,000 terror suspects, Prime Minister Manuel Valls warns' Independent' (11 September 2016) https://www.independent.co.uk/news/world/europe/france-15000-terror-suspects-prime-minister-manuel-valls-isis-warning-latest-a7237231.html accessed 1st July 2018.
[129] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (2017) OJ L 283 1.

step forward to an effective cooperation. Perhaps, its competence area could be extended to include terrorist offences[130].

Lastly, summing up the paper, States should not fight unilaterally against this type of terrorism and should not to surrender to the security need, omitting respect for those rights we are supposed to respect, defend and promote. This answer does not lead to any result and it would mean admitting having lost the war against terrorism.

[130] Spataro, *Supra* note 124, 220.

BIBLIOGRAPHY

LEGISLATION, UN AND EU DOCUMENTS.

- Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (2003) OJ L 245 44
- Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (2009) OJ 138 14.
- Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (2008) OJ L 350 72.
- Council Framework Decision of 13 June 2002 on combating terrorism (2002) OJ L 164 3 and Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (2008) OJ L 330 21
- Council Framework Decision of 13 June 2002 on joint investigation teams (2002/465/JHA) (2002) OJ L 162 1.
- Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (2017) OJ L 283 1.
- Directive 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters (2014) OJ L 130 1.
- Directive 2017/541/EU of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6.
- European Convention on Human Rights as amended by Protocols Nos. 11 and 14 (Adopted 4th November 1950, entered into force 3th September 1953).
- French LOI n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.
- International Covenant on Civil and Political Rights (Adopted 19th December 1966, entered into force 23th March 1979) 171 (ICCPR).
- Italian Criminal Procedure Code.
- Italian d. lgs. 216/2017.
- Italian Law 133 of 2012.
- Italian Law 203 of 1991.
- Italian Law 438 of 2001.
- Recommendation CM/Rec(2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism (2017) OJ C148.
- Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) OJ L 135 53.

- Single European Act, (1986) OJ L 169 1.
- Spanish Ley de Enjuiciamento Criminal
- Spanish Ley Organica 13/2015.
- U.K. Investigatory Powers Act 2016 (19).
- United Nations Convention Against Corruption (Adopted 31th October 2003, entered into force 14th December 2005) 186 (UNCAC).
- United Nations Convention Against Transnational Organized Crime (Adopted 15th June 2000, entered into force 29 September 2003) 188 (UNTOC).
- United Nations Report of the Special Rapporteur on the right to privacy' (2018) A/HRC/37/62.
- UNSC Res. 1373 (28th September 2001).
- UNSC Res. 2178 (24th September 2014).
- UNSC Res. 2368 (20th July 2017).

CASES.

- Margareta and Roger Andersson v. Sweden (1992) 14 EHRR.
- *Ramanauskas v. Lithuania* (2008) ECtHR.
- Szabó and Vissy V. Hungary (2016) ECtHR.
- Zakharov vs. Russia (2015) ECtHR.

ARTICLES, BOOKS, MISCELLANEOUS AND NEWSPAPER.

- 'Al Qaeda planned to hijack 10 planes' CNN News (Washington D.C., 17th June 2004) . http://edition.cnn.com/2004/ALLPOLITICS/06/16/911.commission/ accessed 15th June.
- 'Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU' Article 29 Data Protection Working Party' (April 11, 2018) <http://www.dataprotection.ro/servlet/ViewDocument?id=1476> accessed 29th June 2018.
- 'The Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector' Global Counterterrorism Forum (February 7-8, 2012).
- "Islamic State and the crisis in Iraq and Syria in maps", BBC News (28th March 2018) <https://www.bbc.com/news/world-middle-east-27838034>, accessed 4th July 2018.
- A. Chrisafis, 'Macron's counter-terror bill risks France's human rights record, say UN experts', The Guardian (28th September 2017) <https://www.theguardian.com/world/2017/sep/28/macrons-counter-terror-bill-risks-frances-human-rights-record-says-un> accessed 24th June 2018.
- A. Spataro, 'Politiche della Sicurezza e Diritti Fondamentali' in Questione Giustizia, Terrorismo Internazionale. Politiche della Sicurezza. Diritti Fondamentali. (2016) <http://questionegiustizia.it/speciale/2016-1.php> accessed 8th June 2018.

- Baker-Mackenzie, ‘Surveillance Law Comparison Guide’ (2017) <https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2017_surveillance_law.pdf?la=en> accessed on 2nd July 2018.
- Centro Nacional de Inteligencia ‘Qué es el CNI’ <https://www.cni.es/es/queescni/controles/controljudicial/> accessed 4th July 2018.
- D. Curtotti, ‘Criminal justice and intelligence in Italy: an increasing involvement, restricted by the law’ (2018) 3 Processo penale e giustizia.
- D. Johnston, ‘9/11 Congressional Report Faults F.B.I.-C.I.A. Lapses’ New York Times (24th July 2003) https://www.nytimes.com/2003/07/24/us/9-11-congressional-report-faults-fbi-cia-lapses.html accessed 25th June 2018.
- E Bakker – J Powderly, “Joint Investigation Teams Added Value, Opportunities and Obstacles in the Struggle against Terrorism” (2011) ICCT International Centre for Counter-Terrorism - The Hague.
- European Commission, ‘Passenger Name Record (PNR)’ <https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en> accessed 5th July 2018.
- European Commission, ‘Schengen Information System’ <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en> accessed 5th July 2018.
- European Union Agency for Fundamental Rights, ‘Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update’ (Imprimerie Centrale, Luxembourg 2017).
- Europol, European Counter Terrorism Centre – ECTC <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc> accessed 6th July 2018.
- Europol, European Union Terrorism Situation And Trend Report 2018 (TESAT) <https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018> accessed 21th June 2018.
- F. Galli, ‘The interception of communication in France and Italy – what relevance for the development of English law?’ (2016) 20(5) IJHR.
- F. Zimmermann et al., Mutual Recognition and its Implications for the Gathering of Evidence in Criminal proceedings: a Critical Analysis of the Initiative for a European Investigation Order (2011) 1(1) EUCLR.
- I. Armada, “The European Investigation Order And The Lack Of European Standards For Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?” (2015) 6(1) NJIL.
- I. FLORES PRADA, “Modernization” of the Spanish criminal justice in 2015. Partial reforms waiting the new code of criminal procedure” 2016 (5) Processo penale e giustizia, <http://www.processopenaleegiustizia.it/materiali/Contenuti/RIVISTE/Riviste%20pdf/2016/5_2016/27_Prada.pdf p.> .
- I. Rusu, European Investigation Order in Criminal Matters in the European Union: General Considerations. Some Critical Opinions (2016) 6 Juridical Trib.

- Institute for Economics and Peace, Global Terrorism Index (2017) 59. <http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf> accessed 28th June 2018.
- Interception of Communications Pursuant to Schedule 7 to the Investigatory Powers Act 2016 - Draft Code of Practice (2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593748/IP_Act_Draft_Interception_code_of_practice_Feb2017_FINAL_WEB.pdf> accessed 5th July 2018.
- Interpol, 'Special Notices' https://www.interpol.int/INTERPOL-expertise/Notices/Special-Notices accessed 7th July 2018.
- J.J. 'Oerlemans, Investigating cybercrime' Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University (Leiden, 2017). <https://openaccess.leidenuniv.nl/bitstream/handle/1887/44879/Full_text_Investigating_Cybercrime.pdf?sequence=2> accessed 12th June 2018.
- K B Kanat, 'Lack of cooperation against global terror responsible for London attack' Daily Sabah (June 4, 2017) <https://www.dailysabah.com/columns/kilic-bugra-kanat/2017/06/05/lack-of-cooperation-against-global-terror-responsible-for-london-attack> accessed 1st July 2018.
- Legal Dictionary <https://legal-dictionary.thefreedictionary.com/entrapment> accessed 26th June 2018.
- M Kellett et al., Human Rights in Counter-Terrorism Investigations (Warsaw 2018, OSCE).
- M. Nikolaeva, 'France tracking 15,000 terror suspects, Prime Minister Manuel Valls warns' Independent' (11 September 2016) https://www.independent.co.uk/news/world/europe/france-15000-terror-suspects-prime-minister-manuel-valls-isis-warning-latest-a7237231.html accessed 1st July 2018.
- O. Bureš, 'Intelligence sharing and the fight against terrorism in the EU: lessons learned from Europol' (2016) 15(1) European View.
- OHCHR, 'France: UN expert says new terrorism laws may undermine fundamental rights and freedoms' (Paris/Geneva, 23 May 2018) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23130&LangID=E> accessed 8th June 2018.
- R. Graham, 'How Terrorists Use Encryption' (2016) 9 (6) CTCSentinel <https://ctc.usma.edu/app/uploads/2016/06/CTC-SENTINEL_Vol9Iss614.pdf>
- R. Kreissl, 'Terrorism, mass surveillance and civil rights'< https://www.cepol.europa.eu/sites/default/files/26-reinhard-kreissl.pdf> accessed 25th June 2018.
- R. Zaharieva, "The European Investigation Order and the Joint Investigation Team—which road to take: A practitioner's perspective" (2017) 18(3) ERA Forum.
- Reuters Staff, 'Jihadi software promises secure Web contacts' Reuters (Dubai, January 18, 2008) <https://www.reuters.com/article/us-internet-islamists-software/jihadi-software-promises-secure-web-contacts-idUSL1885793320080118> accessed on June 14, 2018.
- S. Osborne, 'France declares end to state of emergency almost two years after Paris terror attacks' Independent (31 October 2017)

<https://www.independent.co.uk/news/world/europe/france-state-of-emergency-end-terror-attacks-paris-isis-terrorism-alerts-warning-risk-reduced-a8029311.html> accessed 24th June 2018.

- Sara Bundtzen, 'Why you should know about Germany's new surveillance law' Open Democracy (30 October 2017) <https://www.opendemocracy.net/digitaliberties/sara-bundtzen/why-you-should-know-about-germanys-new-surveillance-law> accessed 20th June 2018.
- See C Rijken, "Joint Investigation Teams: principles, practice, and problems Lessons learnt from the first efforts to establish a JIT" (2017) Utrecht Law Review 13(2).
- T. Lister – P. Cruickshank, 'Intercepted communications called critical in terror investigations' CNN (June 11, 2013) <https://edition.cnn.com/2013/06/11/us/nsa-data-gathering-impact/index.html> accessed 12th June 2018.
- Tampere European Council, 15-16 October 1999, "Presidency conclusions", <http://www.europarl.europa.eu/summits/tam_en.htm> accessed on 5th July, 2018.
- UNODC, Foreign Terrorist Fighters Manual for Judicial Training Institutes South-Eastern Europe (2017).

Quaderni di C.R.S.T.

Direttore: Ranieri Razzante

1. Dante Gatta, *Africa occidentale e Sahel: problematiche locali dalla valenza globale. Tra terrorismo, traffici illeciti e migrazioni*
2. Miriam Ferrara e Dante Gatta, *Lineamenti di counter-terrorism comparato*
3. Alessandro Lentini, *Selected Issues in Counter-terrorism: special investigative techniques and the international judicial cooperation Focus on the European Union*
4. Michele Turzi, *The effects of Private Military and Security Companies on local populations in Afghanistan*