23 > 24 February 2017 – Institut de formation judiciaire – Brussels

THE JUDICIAL RESPONSE TO TERRORISM IN THE LIGHT OF THE EU CHARTER OF FUNDAMENTAL RIGHTS

Terrorism and fundamental rights: the investigation and intelligence phase

THE CRIMINAL INVESTIGATION IN THE FIGHT AGAINST TERRORISM: INTELLIGENCE, JUDICIALISATION AND CIVIL LIBERTIES

By Antoine MÉGIE

Rapporteur for the European Project

With the financial support of
the European Union Justice programme

SUMMARY

Today Europe's judiciaries are faced with exponential growth in the number of terrorism investigations. Against this background, it seems necessary ***give some consideration to the missions and the judicial actors and the way in which they exercise their investigative powers***. The purpose of this second seminar is therefore to examine very directly these means by looking at the legal framework on the one hand, and their usages on the other. ***The experiences shared by members of European judiciaries constitute a wealth of essential know-how that can offer participants an opportunity for practical and thoughtful reflection on criminal investigations in terrorism cases at both national and European level***.

First of all, through the presentation of two models, the Belgian and French models, we will ***try to get a better understanding of the shifting boundaries between the intelligence phase and the criminal investigation phase. The collection of evidence, as we will see, is a crucial moment for the investigation in terms of effectiveness and compliance with the rule of law.*** Through a presentation of the work of the French and Belgian counter-terrorism units, we will also tackle recent ***developments in the criminal investigation and its new characteristics***.

Secondly, this report will focus on ***the question of intelligence as material to be shared and as evidence***. The dynamics of transnationalisation of terrorist phenomena are being accompanied by a transnationalisation of the measures taken to combat them. ***These exchanges take place between judicial actors in particular via the European agencies (Eurojust and Europol), but also with private actors (internet service providers). What place is there for the collection of forensic evidence in this relationship between freedom, security and technology, but also economic interests?*** Through their responses based on their experiences, European practitioners, including the representatives of internet access providers, have emphasised the interest in looking at these new legal relationships and their practical dimensions.

Finally, ***the point of view of ECHR case law will enable us to spell out, by way of a conclusion, the legal and practical limits that have been progressively defined within the judicial processing of terrorism cases***. Nevertheless, due precisely to the specificity of these regimes and their particular relationship with the notion of the rule of law, ***these limits are sometimes overstepped, illustrating the very singular relationship that state authorities maintain with terrorist violence***. Thus, in a more or less distant past or in the contemporary period, many States that still claim to adhere to the pre-eminence of the rule of law have justified and engaged in acts that are manifestly contrary to fundamental human rights (acts of torture, inhuman or degrading treatment) or devoid of any legal basis (for example "extraordinary rendition" and the use of secret prisons by the CIA and certain European services in the 2000s).

CONTENTS

EUROPEAN PROJECT AND PARTNERS

The balance between security and fundamental freedoms is an issue faced by the European authorities on a daily basis. This balance supposes that there is a surge in the judicial handling of terrorism placing the judiciary at the centre of this exercise in their role as guardians of individual freedoms.

The Member States of the European Union have become guarantors of fundamental rights by signing a joint charter.

Faced with the alarm generated by terrorist attacks carried out with the aim of spreading fear, judges and prosecutors must strive to reconcile the security issues raised by the violence of terrorist attacks and the protection of fundamental rights for all European citizens.

With financial support from the European Commission Justice Programme, the "Judicial response to terrorism in the light of the EU Charter of Fundamental Rights" project aims to reinforce practitioners' knowledge in the area of fundamental rights so that they can handle terrorism-related cases in accordance with the requirements of the Charter.

Dates of implementation: 1 July 2016 – 31 May 2018

Activities - Kit includes 4 seminars and 1 final conference:

- Seminar 1: Fight against violent radicalisation and protection of fundamental freedoms (*Strasbourg, Council of Europe – 8 and 9 December 2016*)
- Seminar 2: Terrorism and fundamental rights: the investigation and intelligence phases *(Brussels, Institut de formation judiciaire – 23 and 24 February 2017)*
- Seminar 3: Media coverage of terrorism cases *(Paris, Hôtel de Ville – 15 and 16 June 2017)*
- Seminar 4: Terrorism and fundamental rights: the trial and implementation of sentences *(Sofia, national Institute of Justice – 12 and 13 October 2017)*
- Closing conference: protecting fundamental rights in the judicial response to terrorism *(planned in Paris in March 2018)*

Partnership – the ENM is the coordinator of the following consortium:

- The judicial training institutes of Sweden, Bulgaria and Belgium;
- The Council of Europe;
- The European Judicial Training Network (EJTN);
- The Academy of European Law (ERA);
- Justice International Cooperation (JCI).

Target audience - The intention is to train approximately 270 members of the judiciary in 10 European countries. Furthermore, 40 participants from prison administrations, the police and journalism will also be taking part in the sessions.

Type and number of deliverables produced - 5 scientific reports available in French and English

Members	Duties
1 scientific advisor – **Cyril ROTH**, Auxiliary judge at the Court of Cassation, France	- Overall scientific design of the project - Identifies the contributors - Supervises the seminar leaders and rapporteurs - Takes part in the seminars - Validates the reports on the seminars
1 project director – judge at the ENM **Nathalie MALET**, judge, International Department, ENM Replaced by **Marie COMPERE**, judge, International Department, ENM	- Responsible for instructional engineering - Identifies and validates the contributors - Supervises the entire project team - Validates the reports on the seminars
1 ENM project coordinator, **Ségolène POYETON**, International Department, ENM	- Responsible for day-to-day management of the project - Coordinates the partners in the consortium - Point of contact with the European Commission for contract-related, administrative and financial issues
The scientific committee will be reinforced for each seminar by: - A seminar director - A rapporteur Seminar 1: **Vanessa PERREE**, *Substitut général* (deputy public prosecutor), Court of Appeal, Aix-en-Provence, France Seminar 2: **Anne KOSTOMAROFF**, *Avocat général* (assistant public prosecutor), Court of Appeal of Paris, France Seminar 3: **Nicolas BONNAL**, Judge, Court of Cassation, France Seminar 4: **Sabine FAIVRE**, First Vice-President, Tribunal de Grande Instance of Paris, France Rapporteur: **Antoine MEGIE**, Associate professor at the University of Rouen, director of the journal *Politique européenne* - Member of the editorial committee of the journal *Cultures et Conflits*, France	- Prepare the detailed programme for the seminar - Identify the contributors or contributor profiles to ask of the partners - Moderate the seminar - Draw up the report on the seminar

Scientific committee – The project will be led by a restricted team who are members of the scientific committee

SEMINAR PROGRAMME

23 February 2017

9.00 **Arrival and registration of participants**

9.30 **Opening speeches**
Axel KITTEL, Deputy Director of the Institut de Formation Judiciaire (IFJ), Belgium

9.45 **Presentation of the seminar programme**

Cyril ROTH, Auxiliary judge at the Court of Cassation, France
Anne KOSTOMAROFF, Director General of the AGRASC (agency for the recovery and administration of seized and confiscated assets), leader of the seminar, France

I. THE FIGHT AGAINST TERRORISM: THE LEGAL SYSTEM, THE STATE'S SAFEGUARD AGAINST ITSELF?

10.00 **"National security interrogations", the Ibrahim ruling, its sources and its consequences**
Paul MAHONEY, former judge at the European Court of Human Rights

10.45 *Discussion*

11.00 ***Coffee break***

11.15 **Illegal action by the intelligence and criminal investigation services: lessons learned from the Osama Hassan Nasr alias Abou Omar case**
Maurizio ROMANELLI, assistant national terrorism prosecutor, Italy

12.00 *Discussion*

12.15 ***Lunch break***

II. THE CRIMINAL INVESTIGATION IN THE FIGHT AGAINST TERRORISM: WHAT GUARANTEES OF FUNDAMENTAL FREEDOMS?

13.45 **Links between intelligence and judicial procedure in the fight against terrorism: towards a greater role for intelligence or towards earlier prosecution of intentionality? The French and Belgian experience of the investigation**
Camille HENNETIER, vice-public prosecutor, head of the counter-terrorism unit of the public prosecutor's department in Paris, France
Ann FRANSEN, public prosecutor, head of the counter-terrorism unit at the federal prosecutor's office, Belgium

15.00 ***Coffee break***

15.15 **The search for evidence and wider investigative powers: prioritising effectiveness?**
Camille HENNETIER, vice-public prosecutor, head of the counter-terrorism unit of the public prosecutor's department in Paris, France
Ann FRANSEN, public prosecutor, head of the counter-terrorism unit at the federal prosecutor's office, Belgium

16.30 *Discussion*

17.00 **End of Day 1**

24 February 2017

9.00 **Arrival and registration of participants**

III. THE FIGHT AGAINST TERRORISM: WHAT RISKS FOR PERSONAL DATA PROTECTION?

9.30 **The American digital service providers: how to strike a balance between supporting counter-terrorism investigations and protecting personal data?**
Nicole JONES, Senior Counsel, Law Enforcement and Security at Google
Béatrice OEUVRARD, Senior Attorney at Microsoft
Stéphane DUGUIN, Head of the *Internet Referral Unit* at Europol

10.45 *Discussion*

11.00 ***Coffee break***

11.15 **Judicial cooperation and criminal analysis at European level: the joint action of the Eurojust and Europol agencies**
Frédéric BAAB, national member of Eurojust, France
Sébastien MORAS, head of Liaison Office at Europol, France

12.15 *Discussion*

12.30 ***Lunch break***

IV. THE USE OF IMMIGRATION CHANNELS BY JIHADIST NETWORKS: WHAT RISKS FOR FUNDAMENTAL FREEDOMS?

14.00 **The routes into Europe used by jihadis: migrants, asylum rights and jihadist infiltration?**
Dimitri ZOULAS, police superintendent, internal security attaché at the French Embassy in Greece, France

15.00 *Discussion*

15.15 ***Coffee break***

15.30 **The link between terrorism and immigration: the risks for fundamental freedoms**
Elspeth GUILD, Professor of European Immigration Law at Radboud University Nijmegen (Netherlands), researcher at the Centre for European Policy Studies (CEPS) in Brussels, Netherlands

16.15 **Summing up and closure**

16.30 **End of Day 2**

INTRODUCTION

In the counter-terrorism field, European investigators and the judiciary are able to rely on special judicial procedures. At the heart of these powers and procedures, which fall mid-way between ordinary law and emergency law, the dangerous nature of the groups targeted and the need to anticipate their violent actions constitute the main issues justifying these changes in the judicial handling of terrorism cases. During the investigation, one of the major difficulties highlighted by members of the judiciary is the ability to establish proof of the activities and organisational structures of the accused making up the terrorist group.

The purpose of this second seminar is therefore to examine very directly the means at the disposal of the investigation by looking at the question of their legal framework, on the one hand, and their use by European judiciaries on the other. The experiences presented constitute a wealth of essential know-how that can offer participants an opportunity for practical and thoughtful reflection. As Anne Kostomaroff emphasised in her introduction "*(…) the purpose of the reflection based on judicial practices and European case law is to provide a clearer picture of this permanent tension between the need for law enforcement and the protection of freedoms. Is terrorism today fostering an anti-democratic mindset? Do we have any other choice than to take ever more repressive measures against individuals who threaten to make attempts on our lives?* "

Transnationalisation of investigative resources and proactive judicial action

Today there are several organisations that organise the production and application of judicial counter-terrorism regimes. The first dynamic with a marked momentum in this direction is the phenomenon of the transnational circulation of counter-terrorism standards. Without talking about transnational convergence, it is nevertheless clear that today a number of legal standards have been introduced at State and cooperation authority-level, especially in Europe. The second dynamic concerns the proactive judicial approach that has become the norm in investigative and arrest procedures in the terrorism field. Indeed, in a very large majority of Western judicial systems the qualification of the act of terrorism leads to individual responsibility being dissolved into a "terrorist undertaking", via the criminalisation of simple participation and/or intention.

This second movement leads to confusion between the principle of *actus reus* (meaning the forbidden way of behaving or acting) and *mens rea* (which describes the mental element, i.e. the intention and knowledge of the prohibited action). This legal definition tends to differentiate the principles of the offence from the conventional criminal justice system by giving as much importance to the material and the mental dimensions of the terrorist offence. The main idea is to be able to intervene, thanks to this procedural instrument, at an earlier stage and more effectively by bringing in the different members of groups for questioning. As counter-terrorism judges stress, this qualification of action makes it possible to arrest the entire structure including people who only provide logistical support for the more active members.

The assertion of a collective definition of "participation in a terrorist undertaking" is not without consequences on a legal level. Thus, regarding the degree of organisation of the structure and the number of people involved, the legal definitions remain fragile and are in most cases characterised by legal ambiguities that make it easier to qualify the events and *de facto* the charges. A second issue revolves around the way of considering intention (*mens rea*) via the question of the degree of intentionality enabling the judicial authorities to arrest and punish a person. On this precise point, the risk is of charging an individual whose only crime is that of ideologically supporting groups that claim to be fighting for a political cause. This is not

merely a doctrinal issue, as this dimension has concrete repercussions on the procedural practices in the judicial action, as certain members of the judiciary have pointed out.

In the preamble to its annual report in 2009, the International Association of Penal Law discussed, on the basis of different national reports,[1] the effects of the paradigms of the war on organised crime and terrorism on the evolution of national criminal justice systems: "*[...] the paradigms of the war on organised crime and on terrorism have led (1), to extensive reforms of the criminal justice system and criminal procedure as a result of governing through crime and security; (2) have introduced special procedural measures, profoundly affecting the objectives, nature and instruments of the criminal justice system and the applicability of human rights standards; (3) have extended the reactive system of punishment for crimes and rehabilitation of offenders with a pro-active system of prevention of crime and protection of public order and security; (4) have produced an intelligence-led law enforcement approach, by which intelligence authorities play an increasing role in the field of law enforcement; (5) have produced a digital-led law enforcement approach, by which search and surveillance powers have become very intrusive".*

Faced with these legal questions, it was felt that it is important to propose concrete and thoughtful visions by the actors involved in the current context of the fight against terrorism in Europe. In this European panorama, one issue has stood out as crucial in the different stages of the criminal investigation: the gathering of intelligence and its use in prosecutions.

The principle of a proactive judicial approach to counter-terrorism is completely in line with the paradigm that makes surveillance and technological intelligence gathering the cornerstone of the fight against terrorist phenomena and more widely against all forms of violence liable to pose a threat to national security. Under these conditions, the place of surveillance techniques in criminal procedures and their admissibility within a procedural framework represent another central issue. The possibilities for surveillance of telephone or digital communications have been multiplied to the point where their supervision has become extremely complex. The global and regional scale of digital networks and therefore of the data collected leads to a superposition of national, regional and international regulations that very often fall foul of practical and legal borders.

The investigation: judicialisation, intelligence sharing and fundamental rights

In the first part, through the presentation of the Belgian and French models, we will try to get a better understanding of the shifting lines between the intelligence phase and the criminal investigation phase. The collection of evidence, as we will see, raises the question of the risk to the investigation (in terms of effectiveness), but also the issue of compliance with the framework of the rule of law (in terms of individual freedoms). The developments in the criminal investigation and its new characteristics will also be examined in the light of recent events since 2015.

The second part will be devoted to the issue of intelligence as material that can be exchanged and shared. The dynamics of transnationalisation of terrorist phenomena are being accompanied by a transnationalisation of the measures taken to combat them. These exchanges take place in particular between judicial actors via the European agencies (Eurojust and Europol), but also with private actors (internet service providers), whose place and role still seem to be in need of definition. Are these multinationals in the process of setting themselves up as a rampart of mass surveillance? What place is there for the collection of forensic evidence in this relationship between freedom, security and technology but also economic interests?

[1] "Special procedural measures and respect of human rights. Resolution draft", International Review of Penal Law, 3/2009 (Vol. 80), p. 525-531.

In the third and final part, the point of view of European case law through the ECHR will enable us to spell out the legal and practical limits that have been progressively defined within the judicial counter-terrorism systems. Nevertheless, due precisely to the specificity of these regimes and their particular relationship with the notion of the rule of law, these limits are sometimes overstepped, illustrating the very singular relationship that state authorities maintain with terrorist violence. Thus, in a more or less distant past or in the contemporary period, many States that still claim to adhere to the pre-eminence of the rule of law have justified and engaged in acts that are manifestly contrary to fundamental human rights (acts of torture, inhuman or degrading treatment) or devoid of any legal basis (for example the GALs in Spain in the 1980s and the CIA's policy of "extraordinary rendition" in the 2000s).

PART 1: INVESTIGATIVE POWERS IN THE FIGHT AGAINST TERRORISM

Two national models have served as concrete examples to get a better understanding of the judicial issues that arise today within the framework and practices of the criminal counter-terrorist investigation. The current trend for joining and centralising cases and successive changes in the legislative frameworks have led to the introduction of new practices and relatively convergent judicial methods. After presenting the two systems with their institutional organisations and practices (1), we will focus on the issues that today seem central in practitioners' eyes. The aim in particular will be to get a better understanding of how the lines are shifting between the intelligence phase and the criminal investigation phase (2) and the consequences in terms of the evidential burden (3).

1. More resources and expansion of missions

Through the presentations of the two heads of the Belgian and French counter-terrorism divisions of the prosecution services, it was possible to confront the realities of judicial action in countries that have experienced significant levels of terrorist activity since 2010.

France

At the beginning of the 1980s, France experienced a major wave of terrorist attacks. In that context, the French political authorities' position in favour of a judicial approach to terrorism (abolition of the Security Court in 1981) would take a particular direction. The political authorities would seek to consolidate the legislative counter-terrorism arsenal following the main terrorist attacks, in particular those in 1986 for which responsibility was claimed by the Committee for Solidarity with Near Eastern Political Prisoners and the 1995 attacks attributed to the Algerian GIA. Precisely at the same time there were also persistent attacks by Corsican and Basque groups. This reinforcement of the counter-terrorism arsenal through a superposition of new laws should also be understood in part as a result of the political context at the time, characterised by cohabitation and alternating governments of different political colours. Thus, from the middle of the 1980s until the last terror attack in 2016, the French counter-terrorist legal system has undergone a constant series of changes, including:

- The **Law of 9 September 1986**, which introduced the principle of a special justice system for terrorist cases. This law abandoned the principle of pure ordinary law and introduced an element of specialisation with the counter-terrorism division in Paris. Exclusive jurisdiction over these cases was given to a specialist division of the prosecution service in Paris in order to avoid any competition between jurisdictions and the scattering of cases;

- The **Law of 22 July 1992,** for its part, brought the notion of the terrorist offence into the French criminal code. Common law offences (theft, murder, etc.) become terrorist offences if they are committed with the aim of disturbing public order through terror. From a legal qualification point of view, this involves the use of the notion of conspiracy to commit offences or crimes;

- The **Law of 9 March 2004** introduced new investigatory techniques in the fight against organised crime and terrorism. Special measures that constitute departures from ordinary law were now authorised, to facilitate information gathering in particular;

- Since 2010, the Syrian conflict and the phenomenon of "foreign fighters" and their comings and goings have led to the passing of three laws that have modified the legislative arsenal and increased the judiciary's investigatory powers, in particular those of state prosecutors (**Law of 13 November 2014; Law of 3 June 2016 and Law of 21 July 2016**). The general aim has been to strengthen law enforcement tools by introducing new offences such as "justification and incitement of terrorism", or the "ban on leaving the country", which for its part correlatively led to individuals who have gone or sought to go to Syria/Iraq being classified as offenders. Concerning the offence of consulting terrorist websites, this qualification has recently been sanctioned by the Constitutional Council (10 February 2017) which ruled that visiting websites that promote terrorism is not sufficient proof of adherence to the ideology. Finally, these developments in the French judicial arsenal show, implicitly, a desire to be able to increase the sentences that can be imposed on people involved with terrorist organisations (30-year prison sentences or a life sentence for leadership of terrorist groups since the Law of 21 July 2016).

The judicialisation process in the criminal investigation in France

By *Camille Hennetier*, vice-public prosecutor, head of the counter-terrorism unit of the public prosecutor's department in Paris

- The boundary between the administrative scope and the judicial scope: "*In the Law of 24 July 2015, intelligence is defined by the services that gather it, strictly delineated by the law and the aims enabling the use of certain intelligence gathering techniques by those services*". The six specialised services therefore have: "*as their missions in France and abroad, the search for, collection, exploitation and provision to the government of intelligence relating to geopolitical and strategic challenges and the threats and risks liable to affect the life of the Nation and [they] contribute to the knowledge and anticipation of those challenges as well as to the prevention and obstruction of those risks and threats*".
"*The prevention of terrorism is naturally one of those challenges, along with the major interests of foreign policy, economic interests and the prevention of organised crime. The separation of the administrative and judicial aspects is therefore clearly established, between prevention and repression. Intelligence therefore ceases when a criminal offence is discovered.* "

- Constitutional Council case law on this issue:
Decision of 23 July 2015: "*The gathering of intelligence may not have any other purpose than that of maintaining law and order and preventing crime; it may not be used to establish criminal offences, to gather evidence or to find the perpetrators.*"
Decision of 23 January 2006: investigations related to intelligence "*may not have any other purpose than that of maintaining law and order and preventing crime*" also pointing out "*the principle of the separation of powers and the primacy of the judiciary; (…) that there also remains the obligation incumbent upon any administrative authority, when it becomes aware of a crime or other offence, to inform the judicial authorities."*
The case law of the CNCTR (the national commission for the control of intelligence techniques) concretely implements this principle: "*a systematically negative opinion is given on the setting up of an intelligence technique whenever it concerns events already being pursued by the judicial authorities. In principle, the administrative and judicial frameworks are mutually exclusive and the judicial takes precedence over the administrative. The junction between the two seems to rest on a hermetic separation.*"

- The judicialisation process: "*The basis for judicialisation is found in Article 40:2 of the Code of Procedure, which obliges: "every constituted authority, every public officer or person who, in the performance of his duties, has gained knowledge of the existence of a felony or of a misdemeanour is obliged to notify forthwith the public prosecutor of the offence and to transmit to this prosecutor any relevant information, official reports or documents."*
In theory, it is therefore as soon as an offence is observed that intelligence should be judicialised, in accordance with the case law of the Constitutional Court. The same rules apply to counter-terrorism."

- The "judicialisation report": "*This is the report drawn up by the criminal investigation department of the police, based on the evidence gathered by the intelligence service, which is classified. This process is relatively easy when it is implemented by the DGSI (Directorate General for Internal Security), which is both an intelligence service and includes a criminal investigation subdivision. This judicialisation report "whitewashes the intelligence" and declassifies it. It can sometimes be elliptical, but nonetheless it must be detailed enough to justify launching an investigation. It sometimes a complicated exercise but it remains a fundamental one, for certain items of evidence must remain secret in order to guarantee the safety of human sources, the third service rule (forbidding any disclosure of information provided by a partner intelligence service) while others must be mentioned to constitute the criminal offence."*

- The limits of judicialisation: "*The evidence gathered in intelligence actions cannot be detailed in this report, which marks the starting point of the criminal investigation. We must do the investigation again, and so in most cases judicial intercepts will replace the administrative intercept and surveillance, etc. The judicialisation process is conducted in consultation with the prosecutor's office, concerning not only the timing but also its form and opportuneness. The items to be included in the report are assessed by the*

prosecutor and the investigating officer. The principle of judicialisation itself is only very rarely discussed, but the prosecutor's office could well consider that the evidence as it stands is insufficient to justify the launch of a preliminary investigation. The intelligence may not appear to be "ripe" enough, and this is sometimes the case. More than the actual principle and the methods of the judicialisation process, it is above all the moment of this judicialisation that can interfere with the well-established principle of the separation between the judicial and the administrative."

Belgium

The Belgian judicial system involved in counter-terrorism has undergone substantial legislative changes, in particular recently, with changes concerning investigatory powers or the methods of collecting information. The changes include, non-exhaustively:

- The **Law of 20 July 2015** which extended the list of situations in which phone tapping is permitted. New investigatory powers were also given to the Belgian judicial authorities;

- the **Law of 27 April 2016** introduced the possibility of carrying out police searches at night, thereby amending the Law of 7 June 1969. During the parliamentary work preparing this legislation, numerous reflections were raised regarding fundamental rights. The Belgian Council of State, drawing attention to the fact that Article 8 of the Human Rights Convention applies directly in Belgium, made it mandatory to justify night-time police searches. The Council of State also proposed that the Belgian legislature should introduce a number of conditions included in the French legislation, but the Belgian parliament refused (for example, special procedures for night-time searches). Finally, the amendment of the law on preventive detention now requires that reasons be given when remanding a person in custody;

- finally, the **Law of 25 December 2016** gives the King's Prosecutor new powers to carry out computer data searches. The King's Prosecutor is now able to carry out searches in computer systems, including systems related to the one under surveillance. Previously, only the investigating judge possessed such powers. This "extension of the search in a computer system" is authorised for the King's Prosecutor unless it is carried out secretly. In this case, only the investigating judge has the power to carry out such a search.

Finally, the King's Prosecutor now has the power to order *flagrante delicto* phone tapping in terrorism cases, for up to 72 hours. Previously, only the investigating judge had such powers. Nevertheless, in practice, the investigating judge will very quickly become involved as the latter is mobilised in the organisation of the search of the premises to gather evidence.

The judicialisation process in the criminal investigation in Belgium

By *Ann FRANSEN,* public prosecutor, head of the counter-terrorism unit at the Belgian federal prosecutor's office

- The legal framework: "*The judicial authorities work with Belgium's two intelligence services, the State Security Service on the one hand, and military intelligence on the other. The intelligence services may transmit general information to the judicial authorities. The intelligence services are under an obligation to inform the prosecutor's offices of crimes and misdemeanours. The cooperation between the intelligence services and the judicial and police authorities is explained in a circular (no. 9, 2012), which describes this exchange of information and technical assistance."* Two articles define the judicialisation procedures and the issues around cooperation between intelligence and the judiciary:
- Article 13/2 of the LSRS law: "*Prohibition on intelligence compromising a criminal investigation. The law states that if the intelligence services wish to apply exceptional or special measures (phone tapping, surveillance, etc.), they will be obliged to inform the BIM administrative commission, which will decide how the intelligence services can continue their investigations. The primacy of the criminal investigation is preserved; the exceptional procedure has been applied once."*
- Article 19/1 of the LSRS law: "*When the intelligence service applies an exceptional method and discovers strong evidence or a "suspicion", it must contact the BIM administrative commission, which will examine the strong evidence and then produce a declassified report containing that strong evidence. This report will be able to be used in the judicial proceedings. In this case primacy is given to the intelligence investigation."*

- The rules of evidence: "*In Belgium, the rules on the administration of evidence are free; there is no particular evidential value. Declassified reports are received in large quantities from the intelligence service. This is the basis of our investigation. Classified information and reports cannot be used in judicial proceedings. A great deal of classified information is never declassified. Investigating judges have access to these classified reports, but cannot use them."*

- Proactive searches and monitoring of "foreign fighters": "*Two major changes in this type of cooperation should be emphasised. The first concerns the possibility of carrying our proactive searches, preliminary inquiries based on reasonable suspicions. The problem has not arisen very often, as we did not have the capacity to carry out proactive searches. The Law of 9 December 2003 has led to a change. In terrorism cases, we work with the technical assistance of the intelligence service (which must provide all relevant information with the aim of contextualising it). At the same time, the Belgian intelligence services have also seen their methods of information-gathering extended under the different new laws.*
Such changes have had concrete effects, especially in cases relating to the Moroccan GIC in Belgium. A large number of cases started with a declassified note. In this investigation, we have had a procedural problem raised by the defence concerning information declassified by the State Security Service. The defence has alleged that these observations were contrary to Article 8 of the European Convention on Human Rights. This interference prohibited by Article 8 is covered by the Law (Article 13) on the intelligence services. The necessity is to be able to reconcile the requirements on protecting sources with respect for human rights and the rights of the defence. This information is devoid of probative value. In Belgium, we receive a lot of notes from the intelligence services, which are used in preliminary investigations.
The second change is connected to the terrorism situation since 2012 and the departures for Syria and Iraq. We discovered the departures of "foreign fighters" in real time in August 2012. Since 2012, we have been working with a list of all these "foreign fighters", divided into categories. This is a dynamic database containing updated information."

2. The challenges of the judicialisation of intelligence

The challenges of judicialisation in French criminal investigations

By *Camille Hennetier*, vice-public prosecutor, head of the counter-terrorism unit of the public prosecutor's department in Paris

- **The relationship between the intelligence and justice systems**: *"The tight separation between what is a matter for the intelligence services and what is a matter for the justice system is currently being challenged firstly by a process of earlier and earlier judicialisation and secondly by the search for a stronger framework of the exchanges between the judicial and administrative systems. This process of judicialisation occurring further and further upstream is leading to ever earlier judicialisation of intentionality. The right moment for judicialisation is therefore sometimes difficult to judge*".

- The time of judicialisation: "*It is the intelligence service that chooses the moment of judicialisation; the prosecution service has no control over it as intelligence activities are beyond its control. Generally, judicialisation primarily occurs when it seems necessary to use investigative methods within a judicial framework, with a view to gathering evidence. This is all the more important given that the information collected within an administrative framework remains unusable by the judicial authorities. Judicialisation can also occur secondarily when coercive measures need to be taken (bringing people in for questioning, search warrants, etc.), in cases where violent action is feared on the national territory or when departures to Syria/Iraq are imminent. (…) Furthermore, prolonging investigations within an administrative framework can have the opposite of the intended effect, namely the neutralisation of the individuals targeted, weakening the judicial procedure. It is important not to judicialise too soon, before the intelligence is "ripe", which would risk there being nothing to demonstrate judicially, with conventional investigatory techniques (for example, a simple, unsubstantiated prospect of violent action). It is clear that it is necessary to judicialise intelligence that has been ripened and checked and constitutes a solid basis for judicialisation: it is a subtle balancing act between intervening too soon and intervening too late."*

- The risk of losing evidence: *"Thus, for the prosecutor's office, there is a trade-off to be made as it is important not to judicialise too late, for apart from the danger of acts actually being committed, there is also a risk of losing evidence gathered within an administrative framework (for example wire taps). The latter will not be able to be used later as such, but potentially only mentioned in a report, leaving them with a much-reduced evidential value. A second risk concerns the effectiveness of the criminal response, which can be reduced when the facts are old. For example concerning returnees from Syria, someone who was dealt with by the intelligence services, in an administrative interview and who is judicialised later. It is difficult to argue that such a person is dangerous after he has been left free for several months after his return, without being judicialised. Such situations may well have occurred at the beginning of the conflict in Iraq/Syria conflict."*

Confusion between the missions of the judicial and intelligence systems?

According to some practitioners, there is evidence of ambiguity in the purpose of the missions of the judicial and administrative systems when it comes to terrorism. Thus, in France, theoretically it is the administrative authorities that are supposed to prevent the risk of occurrence of an offence, with the judicial system being responsible for arresting the perpetrators after the fact. However, in practice, the borderline between clues enabling the corroboration of a threat justifying the implementation of surveillance techniques concerning

an individual and those liable to characterise the preparation for a planned violent action can sometimes seem extremely hazy.

As pointed out already (cf. introduction), the qualification of conspiracy to commit acts of terrorism enables the judicial authorities to intervene very early before the commission of the act. As a result of this preventive mission, the judicial authorities and the intelligence services find themselves playing the same role: "*The change in the nature of the threat in France, the terrorist attacks, the multiplication in the number of individuals aspiring to commit such acts in France, has led to a desire to judicialise as early as possible, to neutralise individuals deemed potentially dangerous, due to pressure to arrive at zero risk. In concrete terms, concerning the situation in Iraq/Syria, this enables the judicialisation of mere intentions to travel to the conflict zone, in a context of radicalisation, while the joining of a terrorist group in the zone is not yet effective. Previously, judicialisation occurred once the joining of a terrorist group was established or assumed. Concerning plans to commit violent acts in France, it allows people to be arrested at the stage of intentionality, materialised by more or less operational exchanges, sometimes on the cusp of preparatory actions.* " (Camille Hennetier).

Redefining the relationship between the judicial and intelligence systems

According to Camille Hennetier: "*The current period is marked by a growing involvement of the judicial authorities in terrorism-related procedures, as they alone are able to judicially neutralise perpetrators. The cursor seems to be moving further and further back, as the risk is anticipated, but also as part of the "political" management of the current crisis, where the pressure placed on the specialised services leads them to want to judicialise as soon as the first warning signs appear. It is up to prosecutors, more than ever, to be vigilant in their legal analysis and in the trade-offs they make between respect for the rule of law and the freedoms of which they are the guarantors and the necessary taking into account of the threat. This is the challenge specific to counter-terrorism and the members of the judiciary who are tasked with reconciling the necessary anticipation of the commission of a terrorist act and the judicial neutralisation of dangerous individuals with a minimum requirement to test the evidence that cannot always be met in view of the urgency of some situations. (…) It is by the yardstick of this handful of reflections that we can measure the absolute necessity for a high quality of dialogue between the prosecutor's office and the intelligence services as part of the judicialisation process. Building a strategy together, analysing the imperatives involved is only possible with the utmost transparency in the sharing of the evidence gathered and the objectives pursued."*

Transfers from intelligence to the judicial system

The systematisation of the transmission of intelligence information to a judicial procedure comes up against several difficulties according to prosecutors:

- The existence of a culture of secrecy in the intelligence services;
- The need to protect sources (human and technical);
- The third service rule (information given by one service must never be revealed to a third service without the permission of the first)
- The transmission of information between the judicial authorities and the intelligence services.

It seems today that the day of intelligence is over. The judicial authorities are tending to take the lead in a logic of preventive judicial neutralisation: *"We are faced with a dilemma and are under an absolute obligation to be effective. In the first case, it is a question of not letting individuals go out to the conflict zone if they are likely to commit acts of violence there, to be trained in the handling of weapons and come back to France with the intention of committing*

terrorist attacks here. In the second case, not risking letting an act be committed: a balancing act between seeking to characterise actual preparatory actions, seeking stronger proof of intentionality and taking account of the risk. " *(*Camille Hennetier).

For some prosecutors, this judicialisation also constitutes a guarantee for individuals' rights, as Ann Fransen points out: "*For those planning to go abroad, it is better to be the subject of a criminal investigation rather than an intelligence operation, as it offers more guarantees. In an intelligence investigation, there is less control. The matter is handed over to the investigating judge very quickly."*

3. The rules of evidence

As Ann Fransen also points out**:** *"Evidence is needed. Sometimes there is circumstantial evidence or inferences, but you are unable to prove the intention to go further and join a terrorist group. You have to prove the original objectives. A person has to have contributed to a terrorist undertaking. Based on a piece of information, initially we investigate the circumstances. This means that we will issue a warrant, carry out searches, tap the family's phones. These techniques give good results, as terrorists call their families often. In Syria, the French-speaking Belgians are with the French. Terrorist fighters say things that provide information about other fighters. If we do not have any evidence, we cannot take matters to trial. (…) Recently, on 1 February 2017, a judgment of the court in Antwerp attracted attention. A "foreign fighter" was found guilty of a terrorist murder committed in Syria on the basis of three wire-tapped conversations with his girlfriend in Belgium. The convict said that he had managed to kill someone. The sentence handed down was 28 years in prison. Nevertheless, the tenuous nature of the evidence has been criticised."*

Are we moving towards an over-investment in the means of evidence gathering?

In the face of the legal and practical developments introduced by the use of surveillance methods, some legal experts are concluding that we are seeing a profound shift in the rules and use of evidence, a shift that goes beyond differences between national legal systems. Thus, in the conclusions of a collective comparative study on the rules of criminal evidence, Professor Guidicelli-Delage refers to three types of phenomena that are behind these developments:

- firstly, the strengthening of the regulation of the law of evidence thanks to the requirement for a fair trial and respect for substantive human rights (cf. Part 3);

- secondly, the under-investment in the law of evidence marked by the development of a dialogue between the parties in a trial;

- and finally, the over-investment in evidence which concerns mainly its collection due to the desire to set up new instruments to deal with criminal phenomena like organised crime and terrorism.

Concerning the first trend, the authors consider that under the influence of international law, we are seeing a constitutionalisation of the principles of the fair trial, which is rendering obligatory, in the regulation of evidence, compliance with certain substantive human rights, more precisely that of human dignity and the right to privacy. The second trend, for its part, is in line with the idea of simplifying and accelerating procedures. Such an orientation is closely bound up with the changes in the organisation and functioning of the judicial institutions on the grounds of increasing efficiency.

This under-investment in the law of evidence should also be understood as the result of the virtually generalised introduction of a restorative approach to justice reflected in a desire to heighten the value given to dialogue and negotiation between the parties. The use of procedures that allow the accused to plead guilty before the trial begins, which is entering the legislation of more and more countries, illustrates the same trend. Finally, regarding the last trend, which concerns our analysis more specifically, the over-investment in evidence results from a desire on the one hand to rely heavily on science and its supposed accuracy in terms of proof and on the other to gather as much evidence against the accused as possible in order to be able to sentence individuals belonging to complex organisations.

Under the effect of these lines of force, the balance between truth, effectiveness and legitimacy, which is the basis of the concept of proof, is undergoing a profound shift. Although the relationship between effectiveness and truth still remains relatively balanced, due to the opposing trends towards over and under-investment which produce contrasting results, the relationship between effectiveness and legitimacy, on the other hand, is subject to a deep imbalance, with effectiveness predominating over legitimacy. Thus according to Professor Guidicelli-Delage: *"All the principles of the fair trial that govern the rules of evidence – presumption of innocence, equality of arms, adversarial principle, principles of fairness, appropriateness and proportion – but also substantive human rights (dignity, respect for the human body, the right to privacy) are, to some degree, at one time or another, sacrificed for the sake of effectiveness.*[2]

[2] Geneviève Guidicelli-Delage (Dir), "Les transformations de l'administration de la preuve pénale: perspectives comparées. Allemagne, Belgique, Espagne, États-Unis, France, Italie, Portugal, Royaume-Uni", Mission de Recherche Droit et Justice, Paris, December 2003. http://www.gip-recherche-justice.fr/wp-content/uploads/2014/07/01-24-NS.pdf

PART 2: INTELLIGENCE SHARING IN INVESTIGATORY PROCEDURES

By way of introduction, the study conducted by Fabien Jobart and Niklas Schulze-Icking (2004) on the new instruments allowing the collection of evidence (genetic fingerprinting, wire-tapping, bugging, recording of interviews) offers an enlightening analysis of the consequences of intelligence practices in criminal investigations[3]. This analysis is all the more relevant given that in the three countries studied (Germany, France and Great Britain) the rules of criminal evidence are still governed quite differently, in spite of pressure to harmonise practice in Europe.

More specifically concerning phone tapping, which is at the heart of surveillance practices, two legislative orientations are found as regards the judicial value of these methods in criminal proceedings. In the case of France and Germany, the use of telephone intercepts is subject to a strong legal framework, especially in Germany, whereas under British law, phone tapping is decided exclusively by police officers, limited only by their "intuition and conscience". The decision as to whether such surveillance practices are opportune therefore remains only with them. This system, which can be qualified as liberal, is nevertheless counterbalanced by the fact that not all the information collected within this framework can be presented to a judge as evidence. The information-evidence link is therefore broken, leading to the accumulation of sometimes very personal information to the detriment of the legal and regulated construction of a body of proof. The legislative gap between France, Germany and Great Britain also extends to the legal distinction that is made between different methods of eavesdropping. Thus, if there is a strict separation in German procedure between "security intercepts" used in a preventive logic where there is a threat to state security, and judicial wire-tapping, this difference has been called into question in France since the 2004 law on organised crime and it has no significance in Great Britain.

By comparing these legal differences to the figures on the concrete use of these surveillance techniques, Fabien Jobart and Niklas Schulze-Icking found that in a liberal legal framework, the use of wire-tapping did not necessarily lead to an over-instrumentalisation of these techniques. Conversely, a tight legal framework does not necessarily mean low usage of telephone intercepts. Indeed, a higher use of these techniques can be found in the case of Germany, in spite of the application of extremely detailed conditions for the law enforcement authorities. According to the figures quoted, taken from a several German studies dating between 1987 and 1992, the likelihood of having your phone tapped (all types of tapping) was 13 times higher in Germany than in the United States, where the crime rate is considered to be much higher. This phenomenon has been accentuated since the beginning of the 2000s, with 0.5 phone taps per 100,000 inhabitants in the United States, compared to 15 in Germany. Phone tapping constitutes in this count the most commonly used practice in the fight against cross-border organised crime. Based on this result, the authors consider that these surveillance techniques are used above all as a way of consolidating a body of evidence rather than to solve a crime directly.

One last thing that comes out of this research and deserves to be highlighted is the question of the effectiveness and possible dangers that the use of these techniques implies for the fairness of the trial. On this point, the authors consider that the main risk connected to the use of these methods does not lie in generalisation of preliminary inquiries, as is shown by the low number of phone taps identified, due in particular to their financial cost and

[3] Jobard, Fabien, Schulze-Icking, Niklas, *L'administration de la preuve pénale sous l'influence des techniques et des technologies (France, Allemagne, Grande-Bretagne),* Etudes et Données pénales, CESDIP, 2004. http://www.cesdip.fr/IMG/pdf/EDP_no_96.pdf

consumption of human resources. In actual fact, the most dangerous effects are thought to arise out of relentless use and excessive focus on the surveillance of already identified groups. Such concentration then leads to an over-representation of cases linked to certain types of crime (drugs, prostitution rings, terrorism) rather than others (financial crime).[4]

It is against this general backdrop that information sharing procedures have today come to represent a central focus of the transnational counter-terrorism effort. Although these exchanges take place between judicial actors via the European agencies for example (Eurojust and Europol), private actors, first and foremost internet service providers, today have an essential role to play. Thus after presenting the European systems (Eurojust and Europol) and their current cooperation practices (1), we will look at some concrete examples of practical schemes and the legal frameworks that today organise the relations between the multinational internet giants and the national judicial services in charge of collecting evidence for investigations (2).

2.1 The European cooperation agencies

The collection of information and the sharing of intelligence represents a large part of the institutional and political stakes in the field of European security. A link has progressively been built between the exchanging of extranational information and the reinforcement of mutual legal assistance and police cooperation. These methods are presented as indispensable tools in the fight against transnational criminal phenomena. At European level, such a system was structured institutionally in the mid-1980s with the Schengen Convention and the establishment of a system for exchanging data between national authorities: the SIS (Schengen Information System).

Following the terrorist attacks of 11 September 2001, biometrics as an identification technology became a priority objective within Community bodies. The use of databases remains much more ambiguous, as was illustrated by the signing of the Prüm Convention in May 2005 by seven Member States (Belgium, Germany, Austria, Spain, France, Luxembourg and the Netherlands). Reinforcing the EU's commitments in terms of sharing databases, this treaty provides for the permanent and reciprocal sharing of national data such as DNA profiles, fingerprints and all other personal data. As the scheme is intended to be applied in the future to the other Member States, a great deal of criticism has been made of the possible abuses due to a lack of harmonisation in the rules of use and data protection. In 2012, the European Commission, at the initiative of the Commissioner for Information Society and Media, Viviane Reding, put forward a proposal for a general reform of personal data protection. Considering that today personal data, including fingerprints, are stored in a large number of computer systems, according to the Commission the definition of their private or public nature requires the introduction of harmonised and sufficiently protective rules.[5] In this sense, the Court of Justice's July 2014 ruling against Google reasserted the principle of the right to be forgotten and the protection of citizens.

[4] Jobard, Fabien, Schulze-Icking, Niklas, *L'administration de la preuve pénale sous l'influence des techniques et des technologies (France, Allemagne, Grande-Bretagne),* Etudes et Données pénales, CESDIP, 2004. http://www.cesdip.fr/IMG/pdf/EDP_no_96.pdf

[5] Xavier Crettiez and Pierre Piazza (Dir.), *Du papier à la biométrie : identifier les individus*, Paris, Les Presses de Sciences Po, 2006.

Eurojust

The main characteristic of this judicial agency resides in its intergovernmental dimension. This architecture means that the prosecutors who sit at Eurojust are "national" members, anchored in the legal systems of their countries of origin. According to this logic, the College, which is composed of all the national representatives, constitutes the main decision-making body. Its members have no direct control over the investigations and prosecutions of the national judicial authorities. Under these conditions, the European unit is seen above all as a "point of contact" serving the national authorities. Its relations with the jurisdictions therefore have a direct impact on the volume of cases handled by Eurojust and on this unit's ability to impose itself as an essential link in the chain of judicial cooperation. According to its own members, Eurojust can only be perpetuated and yield results if national prosecutors refer cases to it.

Its activities have increased constantly since it was created and in 2015 Eurojust handled 2,214 cases, including 41 terrorism cases, representing a considerable increase on 2014, when it dealt with just 14 terrorism cases. "Drug trafficking" and "crime against property or public goods including fraud" represent the largest percentage of the cases recorded. While Eurojust's main mission is to encourage multilateral cooperation between national authorities in charge of fighting "serious forms of crime", bilateral cases continue to represent the major part of its activities compared to multilateral actions. From 2005 onwards, in response to the new rules of procedure concerning the processing and protection of personal data, Eurojust introduced an automated Case Management System (CMS) in order to enable the secure exchange of judicial information between Eurojust members and national judicial authorities. In December 2007, Eurojust was connected to the Schengen Information System, thereby enabling the States who are members of the unit to access and extract information from the SIS.

Eurojust: "a development in cooperation practices"

By *Frédéric Baab*, French judge at Eurojust

- The turning point of 2015: "*There was a turning point in judicial cooperation on terrorism with the attacks committed in France and then in Belgium. Until then, judicial cooperation was mainly bilateral, whereas the interest of Eurojust is that it serves to support cooperation in cases that concern several Member States. For example, for Basque terrorism, we only needed to be in contact with a Spanish counterpart. Eurojust was therefore not necessarily needed in that kind of case.*
Before 2015, in all the criminal analysis work files opened by Europol and in particular the criminal analysis file for "foreign fighters" and "travellers", the Eurojust unit was considered in the same way as a simple third country. No privileged relationship had been defined between the two agencies. After the attacks in Paris in 2015 and due to political pressure on our European agencies in favour of greater cooperation, an association agreement signed by Europol and Eurojust was confirmed through the creation of two focal points."

- The Eurojust-Europol synergy: "*As a point of contact for criminal analysis work files, I had much closer access to these files. Cooperation was greatly reinforced at institutional and operational level. And so Eurojust is now systematically involved with Europol's analysts and its coordination meetings. In the beginning, there might have been considerable reticence on the part of the intelligence services. We had to win them over and show them that we could be useful. The information shared in these meetings is subject to absolute confidentiality*".

- Greater confidentiality of intelligence: "*The one thing in particular that has led to Eurojust being used to a large extent by national authorities today, is that confidentiality appears to be guaranteed. In the past, Eurojust had a reputation for being something of an "open house". In fact, we are subject to the same rules on confidentiality and we adhere to them scrupulously. We decide at the beginning of the meetings how the information will be shared so that it can be used in criminal proceedings."*

Europol

A compromise between different political viewpoints,[6] the 1995 Europol Convention defined the police cooperation unit as a dual structure: a department whose mission was to produce and analyse databases (staff hired directly by Europol); a department made up of liaison officers responsible for facilitating bilateral and/or multilateral cooperation between Member States (national police service liaison officers).

Since this unit was set up, there has been an exponential rise in the number of analysts while the staffs of the liaison offices have risen less rapidly, if we take into account the addition of ten extra EU Member States in 2004. In 2017, the unit had 200 liaison officers. Concerning its powers, Europol has undergone a number of far-reaching changes with the adoption in 2000, 2002 and 2003 of protocols modifying the 1995 Convention. For example, that of 2002 gave the unit the possibility, subject to there being sufficient evidence, of asking a State to initiate an investigation or to participate in joint investigation teams, bringing together representatives of different European police forces on the same cases. In January 2006, a debate was started on the future of Europol with the main aim of setting up a corporate governance system and developing the agency's operational capacities. After a period of intense diplomatic discussion between the Member States, on 1 January 2010 Europol became a European Union agency.

[6] Didier Bigo, *Polices en réseaux*, Presses de Sciences Po, Paris, 1996.

Europol: "a development in investigatory dynamics"

By *Sébastien Moras*, Head of the Liaison Office at Europol

- Recruitment of experts: *"The Europol agency has changed a great deal, starting with its composition and the professionals that work for it. Alongside the (200) liaison officers in charge of facilitating the sharing of information between Europol and the Member States, we have a growing number of experts (IT, linguists, etc.). On top of this, there are also foreign (non-EU) partners, such as Australians, Canadians, Moldovans and Albanians. For anyone who enjoys multilateral cooperation, Europol is a fantastic tool that provides fast answers to the requests made to it*."

- A positioning in terms of expertise: "*Thanks to these specialist staff, Europol has built up a genuine body of know-how in information management, in particular as a source of technical support, which also allows for the trust and confidentiality necessary to data management systems in particular". Information can be rapidly shared between European countries, and Europol manages the secure exchange networks. It is a real speciality of Europol, this know-how in information management.*
At the same time, Europol has also developed a high level of skills in criminal analysis. All the data from investigations is examined with a fine tooth-comb, using scientific tools essential to criminal investigations. For example there are more and more tools allowing people to cover their tracks and not leave any evidence behind. It is often more difficult for police forces to keep track on people. By professionalising criminal analysis, Europol facilitates their investigations."

- The Europol "**Hub**": "*The power of innovation in the field of criminal analysis has become a major component in Europol's toolbox. At Europol we have more tools and know-how than in any one country because the whole of Europe is represented. EUROPOL's Internet Referral Unit is being used more and more by European police forces. Europol has become a hub thanks to ever greater transmissions of data. The police force in a country can request information from Europol and pass it on to the national prosecutor.* " (cf. part 2.3).

This increase in the importance of the police unit is reflected mainly in its capacity for criminal analysis, in particular through database interoperability projects such as those of the Schengen Information System (SIS II), Europol and the European Visa Information System (VIS). In this context, the control of these technical systems as well as the legal and constitutional compliance of the institutional agreements and frameworks on which they are based, in particular with regard to respect for the protection of rights, constitute one of the main issues relating to the development of the police unit, a dimension that was emphasised, furthermore, in the Stockholm Programme (2010-2014).

The experience of 13 November 2015: the Fraternity Task Force

When the attacks of 13 November 2015 occurred in France, the French police were faced with an attack on a hitherto unseen scale. Europol set up an information bureau on the premises of the SDAT (the French counter-terrorism unit).
Europol came with the mission of exploiting the data and information provided by European partners. "*France has provided large quantities of information to Europol on this case and closer and closer links have appeared during the investigation with other countries. Practices have changed because there is a real need.* " (Sébastien Moras). These data, such as the trips made by the perpetrators of the attacks, are sent to Europol and analysed by the Fraternity Task Force. Eurojust is also involved in this Task Force.

There is evidence in several countries: *"A real European jigsaw puzzle is starting to be put together (Turkey, Greece via certain migration routes, Hungary, Germany, Belgium and France). The attacks were committed by Belgian, French and Iraqi citizens, which means that the investigation cannot be only French, or even bilateral, as that would not allow a rapid response to the situation. Europol has provided an enormous number of analyses that have allowed the investigators to ensure they have not missed anything as well as enabling them to make connections and trace back the thread. Europol was not only a support service, but took an active part in the investigation.* " (Sébastien Moras).

Following this experience, several countries, Denmark and Sweden in particular, asked if they could set up the same Task Force configuration: *"The aim is to perpetuate the experiment to avoid the creation of a multitude of channels for judicial cooperation on terrorism and therefore to facilitate good transmission of information at European level.* " (Sébastien Moras).

2.2 Exchanges of information between judicial authorities and private companies (internet service providers)

After presenting the legal frameworks organising the procedures for information sharing between private actors and judicial actors, we will highlight what appear to be the salient legal and practical issues, in particular in view of the experiences on the ground of prosecutors already confronted with this sort of cooperation. Against this background, the explanations provided by the representatives of Microsoft and Google offer a concrete panorama of the practices of access providers and their relations with the judicial authorities. On the terrain of access to users' data, confidentiality rules and personal data protection, numerous questions still remain unanswered.

US legislation

For the representatives of Microsoft and Google, "*American legislation constitutes a complex system, but as American corporations, we have an obligation to comply with US legislation when answering requests from abroad."* Several laws and precedents form the legal system on this issue. First of all, the **4th amendment of the American Constitution**, "*whose aim is to protect audiovisual companies and individuals from all unnecessary data entries and therefore protect their security*. *In 1967, the US Supreme Court looked at how to protect data outside private places in a case where the government had placed a recording device in a public telephone box. The Court considered that the principle of "reasonable expectation of*

privacy" was the legal foundation. The law then applied to all electronic communications with the obligation to obtain a very wide-ranging warrant."

In 1986, the US Congress passed the Electronic Communications Privacy Act. "*This was the first law whose objective was to recognise a new situation regarding the private nature of information in an electronic world. A new doctrine was established, whereby all companies exchanging information electronically had to follow new rules. If you have voluntarily shared information with a third party, the guarantee of confidentiality is broken."* This law on privacy and communications was then extended to all electronic communications, since originally, these first rules were mainly applied to telephone tapping: "*In 1986, when the Act was passed, the use of e-mail was not comparable to what it is today. Today connection solutions are much simpler and everyone leaves their e-mails in their inbox, which does not mean that they are waiving or abandoning their right to privacy."*

As regards the content and metadata in these communications, there are several categories of information:

"*Category 1: Basic information (name, address, etc.) which we are generally asked to provide, which includes IP addresses. We provide these data. This type of request is generally made by the police. Before the Act in question was passed non-judicial authorities could obtain a writ to ask us for all kinds of information. Today, these writs concern only certain data.*

Category 2: transactional information not linked to content or a user. For example, the subject of the e-mail. For this, an injunction from a court is needed, which must demonstrate the relevance of this information to an investigation.

Category 3: the content (body of the e-mail, attachments, etc.). In the United States, it is necessary to provide precisely the plausible and likely reasons justifying access to this information".

Concerning the deadline for accessing this information, **since 2008 the 180-day rule is no longer a constitutional rule in the United States**: *"a Supreme Court ruling has indicated that we need a court order to get access to e-mails. Consumers expect their electronic conversations to be protected as part of their right to privacy. There were no divergent opinions, so today the 180-day rule makes no sense."*

Finally, **the acceptance by a judge of the "plausible reasons" and "probable cause" are necessary for the three authorities authorised to do so to gain access to these data**. Different procedures apply to these three authorities. Thus, (1) the NSA issues a National Security Letter, which can also be drawn up by the FBI; (2) a Court Order; finally (3) under section 702 of the Foreign Intelligence Surveillance Act (FISA): "*All this requires the setting up of technical procedures because neither Microsoft nor Google have direct access to this information. These data can only be disclosed after a technical operation."*

European legislation

- **The Budapest Convention on Cybercrime** was one of the first important texts (2001). Thus, in spite of current technological developments, internet access providers are regularly subject to seizures under this law. According to this Convention, the authorities can request that series of data be disclosed to them concerning people on their territory or another. Although there are no limits in terms of data, different aspects must be specified, in particular whether the request concerns "content data" or "non-content data". Depending on the request, the procedure is different. The main difficulty with this convention resides in the fact that it has not been ratified by all the EU Member States.

- **The European Directive on the European Investigation Order (EIO)** which is due to come into force in May 2017. According to the representatives of Microsoft and Google "*what is interesting here is that we are going to move from a system of assistance to a system of*

mutual recognition. It will be easier to work together. This Directive provides for the introduction of a single form. This single form will facilitate things, in particular for us, as we are obliged to deal with all the requests made to us. At the current time, all the forms are different because they come from different countries, which makes the situation complicated to manage. On the other hand, it should be noted that this Directive has not been signed by Denmark and Ireland."

Requests from European authorities with regard to US standards

- The importance of the American legal framework: According to the representatives of the internet access providers, the European legal framework seems "*not very precise or clear. The status of our companies is defined in the ECPA (Electronic Communications Privacy Act). Not being the owner of the electronic data, our use of these data is governed by the ECPA, which defines three stages in the procedure. For content data, we need an American-type warrant, for other types of data there are no restrictions. For BSI data for example, there are no restrictions. When the requests are not American, we will analyse those requests online in accordance with US legislation and international conventions. In the case of a request not emanating from the United States, we must therefore determine that there is no violation of American legislation. We ensure that requests are also compliant with the legislation of the requesting country."*

- Position of American companies on hate speech
Google representative: "*When we receive a request compliant with US law concerning hate speech, we consider that the request is valid. The 1st amendment does not apply to hate speech. We refuse certain requests when the content is defined as "critical" and not "hate speech".*
Microsoft representative: "*We have already amended the terms and conditions, with a specific clause mentioning that advocacy of terrorism is clearly prohibited. As soon as we receive requests, we delist sites that advocate terrorism from our search engines. There must be an approach to these situations that is investigatory and applied on a case by case basis. If we are a service provider, we can help with the diagnosis of technical situations. The borderline lies in our providing assistance without taking the decision to remove certain types of content ourselves. (…) We think that citizens expect the data management procedures to be the same in the United States and that their data will be protected outside their country. European harmonisation would facilitate procedures in this sense. If there is a direct threat to human life, you can obtain a rapid response to a request. Exceptions are in fact possible in urgent situations."*

The challenges of cooperation: "urgent situations" and "massification of requests"

- Define "urgent situations"? The definition of urgency gives rises to some questions according to prosecutors, in particular in terms of binding requests on internet access providers. Thus, if the judicial authorities consider a situation in terms of urgency characterised by an attack on the "integrity of life", to what extent do access providers have the possibility of rejecting the request considering that the situation is not sufficiently characterised? As one French police officer points out: "*We are well aware of the difficulty of defining the notion of urgency, but when it comes to terrorism the notion of urgency is inherent. It is difficult to characterise the notion of urgency to the operators when the threat may seem very vague. For us, all the searches will fall within the scope of searches on individuals."* What common framework exists today for the appreciation of this notion? Who are the decision-makers? What types of cooperation exist?

- **Microsoft representative**: "*We have been confronted with this situation, in particular during the Charlie Hebdo attack. We have understood what an urgent situation means. When we were confronted with this attack, we received 30 requests in 30 minutes. In this type of situation, the notion of an emergency procedure is self-evident. There is the principle of subsidiarity, but in those moments everything merges together at a global level. I have discussed this with a police representative for the returns from Syria: is that an urgent situation? I think it has to be examined on a case by case basis. The return is not a threat to other people's lives, so there is no urgent situation.*
We have set up a group in France, because in an urgent situation, every minute counts. Translation is important. During the 13 November attacks, we used pre-translated documents where the police just had to tick boxes. (…) When we receive a request marked urgent, but we do not accept this qualification, we explain the refusal. We talk to the police to get a better understanding of the case they are confronted with; we avoid making unilateral decisions."

- **Google representative**: "*We have changed the way we deal with these requests to take account of the current situation. Today we are less strict at the time of asking for evidence. If you have enough information to show that a person is radicalised or ready to commit an act, we understand the urgency. We will not ask you for evidence, but we would like to understand how the account is linked to the investigation. (…) This is a decision taken in real time - we have a hotline with people who are responsible for handing urgent situations 24 hours a day. We also have a pre-prepared form. This form is divided into different categories that define the situation that you are in."*

Nevertheless, it seems that this type of procedure does not fully answer the question of a common definition of an urgent situation. Thus for certain judges and prosecutors as part of the cooperation process and procedures for accessing electronic evidence, the notion of urgency can go beyond what access providers consider it to be.

- Processing capacity and non-harmonisation of requests The question of mass requests made by the judicial authorities and the access providers' means of meeting them constitute a salient issue for practitioners. The question arises here of the problems of mass handling that unavoidably lead to choices being made in terms of priorities. Although the companies do not seem to have any volume problems at present, such a situation risks occurring in the future. Indeed as Stéphane Duguin (Head of EUROPOL's Internet Referral Unit) points out: "*We understand that Microsoft is used to this, but it is not the case of young firms with millions of users, which do exist, so what do they do? You have a judicial reporting system, but you handle requests manually. If your community increases in size, you risk being confronted with this problem of volume one day."*

Microsoft representative: "*In this landscape, Microsoft is a large company, but also a long-established one and we have been dealing with this type of request for years. For Microsoft, when I speak to the French authorities, I don't hear anybody mentioning this problem of volumes of requests, or the time issue, so I am surprised by your question. (…) We do not have any harmonised regulations, although that is the key here to integrating service providers. The problem is not really the volume of requests, but the*

major difficulty lies in the non-harmonisation of the request we receive."

Google representative: "*In Belgium, there are two people who handle virtually all the requests sent to Google - this work is managed very well. For France it is more complex as the system is decentralised: what happened for the Bataclan attack was that we received the same requests from six different people. (…) What is interesting is that we have a team that manages the requests; we also have a linguistic team. We have a problem with the way the requests are made to us, we even still receive some by fax! The way this works needs to be simplified. A tool such as a computer portal would enable us to know what law applies. The volume we can cope with, the problem is the way the requests come to us."*

Europol: "towards the availability of a European Hub"

By *Stéphane DUGUIN,* Head of Europol's Internet Referral Unit

- The work of the criminal investigation: "*We have a job of prevention and a job of investigation. As regards prevention, we look at everything that is put out on the internet, everything is assessed manually (which is bad news), there is no algorithm. Detection can be automated, but the decisions have to be taken by humans.*
For example, concerning the Nice attack, videos of the attack were published. We combat broadcasting and reproduction. This content is present on a series of platforms. We work on detecting it, we do mapping that helps us to detect these situations. Today, information on a criminal (banking, logistics) is situated in different countries, which complicates things. "

- Relations with private companies: "*Today criminals act on decentralised platforms that we cannot access. In 2015, all the messages were on Twitter, then that network began to fade away and Telegram took over, and all the terrorists moved to Telegram. They are very proud of the fact that no judicial authority can get hold of their data, in fact they boast about it. We cannot even put in requests. In the future, services will be decentralised so it often appears difficult to contact them. In fact this is one of the main problems encountered by our European colleagues. Colleagues contact us at Europol saying they have contacted the companies directly but their requests come to nothing because they are not made according to the law in the country of the company. This is why, in particular, we have set up the SIRIUS platform which presents the services that exist so that our colleagues are aware of them. One case can be highlighted in particular: Facebook. Today, when you make a request, Facebook sends an e-mail to the owner of the pages and informs them.* "

- Handling of "urgent situations': *"As far as urgent situations are concerned, we have a technical and operational analysis. We have a lot of relations with the different companies. The definition of the urgent situation is the first point to analyse. We have a forum on the internet that these different companies have joined."*

PART 3: THE CONNECTION TO FUNDAMENTAL RIGHTS

This third part devoted to ECHR case law offers the possibility of spelling out the legal and practical limits that have been progressively defined within the judicial counter-terrorism systems in the name of respecting human rights. Within what are sometimes very heterogeneous European counter-terrorism systems (cf. Summary report, January 2017), a line of convergence seems to need to be imposed: civil liberties and respect for them. Faced with a very tense political and social situation, judges and prosecutors must include the question of freedoms and their fragility in their actions. This indispensable matching of freedom and security leads very directly to the links between techniques (judicial and policing) and elements of fundamental rights.

Based on the different articles of the European Convention on Human Rights (cf. box), we will look first of all at how the ECHR has produced case law concerning not only respect for the right to a fair trial and respect for the right to security but also the prohibition of torture (1).

Nevertheless, due precisely to the specificity of the counter-terrorism systems and their particular relationship with the notion of the rule of law, these limits are sometimes overstepped, illustrating the very singular relationship that state authorities maintain with terrorist violence. In a more or less distant past or in the contemporary period, many States that still claim to adhere to the pre-eminence of the rule of law have justified and engaged in acts that are manifestly contrary to fundamental human rights (acts of torture, inhuman or degrading treatment) or devoid of any legal basis. Through a presentation of the investigation of members of the Italian judiciary, we present the specific case of the Extraordinary Rendition programme organised by the CIA on European soil in the 2000s.

3.1 ECHR case law

European Convention on Human Rights and Fundamental Freedoms

As Elpesth Guild points out: *"In Europe, the legislative and regulatory framework protects fundamental freedoms. Thus the migration ban decreed by the new American President to "defend the nation against the entry of foreign terrorists into the USA" could not have been adopted. Such measures which have such a huge impact on citizens in Europe can only be taken after very long procedures. Certain provisions of the European Convention on Human Rights would be too deeply affected."*

Article 3 – Prohibition of torture
No one shall be subjected to torture or to inhuman or degrading treatment or punishment.

Article 5 – Right to liberty and security
1) Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law:
- the lawful detention of a person after conviction by a competent court;
- the lawful arrest or detention of a person for non-compliance with the lawful order of a court or in order to secure the fulfilment of any obligation prescribed by law;
- the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so;
- the detention of a minor by lawful order for the purpose of educational supervision or his lawful detention for the purpose of bringing him before the competent legal authority;
- the lawful detention of persons for the prevention of the spreading of infectious diseases, of persons of unsound mind, alcoholics or drug addicts or vagrants;
-the lawful arrest or detention of a person to prevent his effecting an unauthorised entry into the country or of a person against whom action is being taken with a view to deportation or extradition.
2) Everyone who is arrested shall be informed promptly, in a language which he understands, of the reasons for his arrest and of any charge against him.
3) Everyone arrested or detained in accordance with the provisions of paragraph 1.c of this article shall be brought promptly before a judge or other officer authorised by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial. Release may be conditioned by guarantees to appear for trial.
4) Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful.
5) Everyone who has been the victim of arrest or detention in contravention of the provisions of this article shall have an enforceable right to compensation.

Article 6 – Right to a fair trial
1) In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.
2) Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
3) Everyone charged with a criminal offence has the following minimum rights:
- to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
- to have adequate time and facilities for the preparation of his defence;
- to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

- to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
- to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Article 8 – Right to respect for private and family life
1) Everyone has the right to respect for his private and family life, his home and his correspondence.
2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 14 – Prohibition of discrimination
The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

The principle of the fair trial (Art. 6): Ibrahim v. UK case

On 7 July 2005, four bombs exploded in London killing more than fifty people. Two weeks later more attacks were foiled in London. Mr Ibrahim was then arrested along with three other suspects. Under British law a person suspected of committing a crime or offence must be assisted by a lawyer from the first contact with the authorities. Although the United Kingdom has not issued any exemptions from this rule, the legislation nevertheless provides that it is possible to delay this normally immediate access to a lawyer if the police officer fears that the security of the public is still at risk and considers that access to a lawyer could give rise to a terrorist attack. In this case, the objective of such "security interviews" is to obtain information with the aim of protecting the public.
In this case, the first three plaintiffs were assisted by a solicitor within the first few hours following their arrest and they were informed that they were entitled to remain silent. The fourth person, Mr Ibrahim, initially agreed to be interviewed as a witness without the presence of a solicitor. Now, during these interviews he admitted certain acts, such as having received possible terrorists at his home. "*From the moment when he became a suspect (by admitting that he had received these people), he should have been offered the assistance of a solicitor. The fact is that the senior police officer insisted that the interview should continue without giving him access to the solicitor. Mr Ibrahim continued to talk. Following these initial investigations, the investigating officers discovered that this attack was in fact only a "false threat" that was intended to draw attention to the conflict in Iraq. " (Paul Mahoney).*
Following this interrogation, the four suspects decided to take the matter to the ECHR, citing the fact that they did not all have access to a lawyer and considering that their right to a fair trial had been violated. "*The ECHR then considered that there had been no violation for the first three plaintiffs, but that, on the other hand, Mr Ibrahim's right to a fair trial had not been respected. " (Paul Mahoney).*

Ibrahim v. UK ruling

By *Paul Mahoney*, former ECHR judge

- Respect for the right to a fair trial: "*The Ibrahim ruling against the UK raises the issue of the judicial reaction within the framework of a democratic society. In this case, the general philosophy was to maintain a fair approach as there is no question of challenging the rules. We must try to maintain these basic rules regarding the just and fair trial in all cases. Article 6 must not be applied in such a way as to set up disproportionate arrangements. Interests relating to the protection of the public may not prevent the rights of the defence being respected. In the Ibrahim ruling, the Court insisted on the fact that the accused was not given access to a lawyer (…). The trial must be based on two stages. There must be information showing that there is good reason not to grant access to a lawyer, and the evidence must then be gathered. The evidence obtained in the investigation phase must be presented at the trial and show that there were sufficient grounds not to give access to a lawyer. In all cases, this situation must be temporary. Our mission is to ensure that the restrictions are circumspect and associated with clearly established circumstances.*"

- Interpretation of the subsidiarity principle: *"The general principle is that the right to a fair trial must be examined on a case by case basis. Article 6 has not been interpreted as being there to harmonise the increasing rules of the national systems. One exception however: the law prohibiting the extortion of confessions by torture (Article 3).(…)*
We have stressed a flexible approach to the subsidiarity principle in relation to the fair trial principle. In terrorism cases, national judicial authorities must examine the aspects connected to fundamental rights. It is these authorities that ensure the appropriate application of those rights in their country. For subsidiarity to work, it must be visible and credible in the reasoning of the national courts. What is crucial is to know whether the final results allow good conciliation to be guaranteed."

- Qualification of "urgent situations" (1): *"We have mentioned the issue of the exceptionally dangerous situation that existed when Mr Ibrahim was questioned, since other terrorists were at large. On this point, several members considered that there were imperious reasons for the first three and thus for the fourth. These imperious reasons should have, in our opinion, enabled the interrogation to continue. After maintaining his statements, Mr Ibrahim decided to change them. It is for this reason that certain judges thought that he should have been found guilty. He admitted that he had received a terrorist in his home and had helped him to flee to Italy. On this basis, certain judges considered that it was necessary to take an overall view of things and that in this respect, he was not treated unfairly.*
Nevertheless, this opinion was shared by 6 judges against 11 and the majority therefore prevailed. We considered that the majority had concentrated excessively on the plaintiffs' rights in the procedure to the detriment of the public's right to life and physical safety."

- Qualification of "urgent situations" (2): *"In another affair that came before the ECHR, the police had to act very quickly as it believed the three suspects were planning a bomb attack in Manchester. The Prime Minister at the time tripped up as he was leaving Westminster and his briefcase fell open revealing secret documents that were picked up by the media. It was necessary to act very quickly to apprehend the suspects. A warrant was issued very quickly to authorise the police to act. Afterwards, the British authorities were condemned for the fact that the warrant was too wide-reaching and vague. However, given the urgency and rarity of the situation, the Court nevertheless considered that this way action was acceptable and that the authorisation to intervene was given by a judge and not an administrative department."*

Prohibition of torture (Art. 3)

Concerning the use of torture, Elspeth Guild points out that: "*the first time that the ECHR envisaged the prohibition of torture in the context of the fight against terrorism dates from the Chahal v. UK case (15 Nov. 1996). The authorities suspected the person of being a member of a Sikh separatist group and of having taken part in a terrorist attack on a plane flying to Canada. No case was brought or sentence pronounced against him. The question put to the Court was, if Mr Chahal were sent back to India, would he be a victim of torture or inhuman treatment? Clearly he could have been tortured in India. The British government said the level of proof was lower if torture was possible in another country. The Court overturned the Chahal ruling in 2008 due to the concerns arising after 2001. In the Saadi v. Italy case, the deportation of the accused, a Tunisian who feared being tortured in Tunisia, was rejected. Italy was asking that the level of proof be reduced because this was a terrorism case. The Court's ruling confirmed that the burden of proof is the same whether the case involves terrorism or not. No exception can be made to the prohibition on torture. Thus, the position is clear, terrorism is not an ace or a card that can be played to use torture."*

According to Paul Mahoney: "*The situation is actually clear, it is not permitted to use mistreatment as a means of obtaining information or to use intelligence obtained in this way. For example, a British case in which an extremist Islamist was on the point of being sent back to Jordan to be tried there: the plaintiff claimed that he would be tortured during the interrogation and that statements made by other accused persons who had been tortured could be used against him. This was a violation of Article 3. Although the Jordanian government said that there would be no torture, the ECHR granted this petition as we found that there was a genuine risk of this person not receiving a fair trial in Jordan. In the case in point, it was only a potential risk, but one so real that the Court would not accept that the States should use heavy-handed interrogation techniques*".

Under these conditions, it seems that the interpretation of the Convention is changing: *"In a case dating from 1978 in Ireland, the five interrogation techniques that had been used were considered as constituting inhuman treatment but not torture. It is highly likely that today these techniques would be considered as torture. We are therefore moving towards ever greater firmness. In a Belgian case, the Court qualified as degrading treatment the fact that four policemen had deliberately slapped a suspect.* " (Paul Mahoney).

3.2 The extraordinary rendition programme

Revealed at the end of 2006, the practice of secret flights by the CIA (Central Intelligence Agency) in Europe constitutes the most recent example of opposition between counter-terrorism strategies and respect for civil liberties. Part of the extraordinary rendition programme set up as early as September 2001 by the US administration, the aim of this scheme was to capture, transfer and detain individuals suspected of belonging to terrorist groups of participating in their activities, outside of any legal framework and therefore entirely in breach of international and regional conventions protecting civil liberties. This programme has the particularity of being applied on several continents, including Europe and of allowing certain suspects to be sent to countries considered until 2001 as Rogue States.

In a report submitted to the Council of Europe on 11 June 2007,[7] Senator Dick Marty directly accused Sweden, the United Kingdom, Italy, Germany and Turkey of "human rights violations" during these illegal transfers. Other European countries were also singled out for having participated actively or passively in the transfers and secret detentions: Spain, Cyprus, Ireland, Portugal, Greece, Poland and Romania. The latter two States were also

[7] Report available on the European programme site *Challenge: the Changing Landscape of European Liberty and Security* (www.libertysecurity.org/IMG/pdf_FMarty_20070608_NoEmbargo.pdf).

accused of having provided the Americans with secret prisons to detain suspects between 2003 and 2005. The authorities of several European countries therefore, according to this report, actively participated, with the CIA, in illegal activities, whilst other ignored them in full knowledge of the facts. Dick Marty's report concludes that the European countries sacrificed their essential principles on the respect for fundamental rights for the sake of the fight against terrorism.

Confronted with these accusations, the great majority of the governments concerned claimed not to be aware of these practices. However, as Senator Marty points out, the highest national authorities must necessarily have been informed of what was happening on their territory, in particular through the North Atlantic Treaty Organisation (NATO), since an agreement was adopted within this body in October 2001.

Neither the fact of belonging to a country, nor the national, regional and international legal protection rules are able to protect citizens against such arbitrary abductions and transfers. The numerous examples uncovered since 2001 have shown that the nationals of any State, even when that country is a close ally of the United States, could be abducted arbitrarily wherever they are. On the contrary, it seems, based on the cases that have come to light, that the States the individuals concerned come from are acting not in a logic of protecting their citizens but, quite the opposite, in a process of cooperation that risks putting them in a situation that is contradictory to their own internal laws. Several cases, including those concerning the CIA's secret prisons in Poland[8] and the El-Masri v. Macedonia case[9] have clearly identified these practices and the involvement of several European governments. It is incontestably the case of imam Abu Omar in Italy that today constitutes the central example of these illegal practices and the role of the judicial authorities.

The Abu Omar case

As Maurizio Romanelli, in charge of the judicial investigation, points out: "*This case, which dates back to February 2003, is still reverberating around the judicial world in Italy. An Egyptian citizen, Abu Omar, known to the intelligence services for his involvement in terrorist groups was in the street in Milan in broad daylight, at noon. He was approached by an Italian who introduced himself as a police officer so that Abu Omar would confirm his identity. A commando then appeared and took him away. He was put in a white van and driven off to an unknown destination. He was tied up and beaten, then taken to the Aviano Base (an US airbase in Northern Italy). He was then flow to another American airbase in Germany: Ramstein. Another flight then took him to Egypt: there Abu Omar was handed over to Egyptian secret service agents. He was held for 4 years and subjected to several forms of torture. The aims of this torture were twofold: to convince him to collaborate with the Egyptian secret service and then to obtain information on the terrorist network he belonged to".*

These facts are a consequence of the American programme, which, according to Maurizio Romanelli, constitutes: "*a grave offence in the sense of a crime against the individual's liberty with sequestration and several aggravating circumstances. Several principles are violated: firstly there is detention without trial, outside the control of the judicial authorities, and secondly there is torture."*

[8] Al Nashiri v. Poland (application no. 28761/11, 24 July 2014) and Husayn (Abu Zubaydah) v. Poland (no. 7511/13, 24 July 2014)

[9] *El-Masri v. the Former Yugoslav Republic of Macedonia* [GC], no. 39630/09, 13 December 2012, ECHR

The Italian judicial authorities faced with illegal practices

By *Maurizio Romanelli*, assistant national terrorism prosecutor

- The indictment procedure: "*The Italian judicial authority, faced with this crime, launched a criminal investigation that was carried out using all the investigatory instruments recognised by Italian law, in spite of the fact that we were dealing with foreign (the CIA) and the Italian intelligence services. The investigation was far-reaching and we reconstructed the entire affair. We found that numerous individual responsibilities were involved. After the preliminary hearing, it was decided to prosecute 33 plaintiffs, including 26 civil servants and international agents (notably those of the CIA) and Italian intelligence agents, plus 5 top civil servants who are thought to have taken part in the abduction, including the head of Italian military intelligence. These are all people who had a very significant role in the events. Other civil servants are accused of minor offences of complicity, as they were aware of the investigation being carried out by the Milan prosecutor's office and they tried to divert it. The Italian CID officer who carried out the fake identity check on Abu Omar has taken a very open attitude and collaborated to a great extent. His position has been made possible by judicial negotiations."*

- The legal issues: "*Given the type of people involved in the preliminary hearings and interviews, the adversarial process has been very wide-ranging. A complex series of legal questions have been raised, in particular concerning access to evidence.*
- First of all, it was necessary to define the legal concept of "rendition" according to Italian standards;
- Secondly, the possibility of justifying the act of abduction by the execution of an order. Indeed, the members of the US intelligence services had to carry out this abduction in execution of orders and therefore in the line of duty.
- Thirdly, the existence of diplomatic immunity for certain plaintiff who were part of foreign diplomatic corps on Italian soil.
- Fourthly and finally, the issue of state secrecy which was raised by the Italian plaintiffs and subsequently confirmed by the politicians (President of the Council of Ministers)."

- The judgments: "*The judgment in the first instance found 25 people guilty (23 US intelligence agents and 2 Italians for minor complicity offences). The 5 top civil servants and the most important Italian accused were released because of the invoking of state secrecy. 3 American civil servants were released as a result of their diplomatic immunity The second-instance judgment confirmed these verdicts.*
The Court of Cassation, however, quashed the acquittals of the Italian civil servants. Considering that state secrecy cannot be applied as it cannot cover the abduction and the offence committed. The judge therefore identified real evidence that did not confirm state secrecy. This being established, a new judgment found the 11 Italian civil servants guilty on the merits. The real evidence was considered as valid without state secrecy being able to be invoked."

- Opposition from the political authorities: "*At the top of the executive, the President of the Council suggested to the Constitutional Court, that there was a jurisdictional conflict. Thus, the political authorities claim that the Court of Cassation exceeded its powers when it opposed State secrecy. Such a conflict of power is an exceptional case in Italy. The Constitutional Court handed down a ruling in 2014 in which it accepted the conflict proposed by the government and ruled on the existence of state secrets in favour of the accused. The Italian civil servants were therefore permanently acquitted and the 3 Americans were finally convicted."*

- The autonomy of the justice system: "*This case was possible because in Italy the prosecution service is an autonomous body independent of all other powers. This was the sine qua non condition that enabled this investigation to take place. The Italian system allowed this criminal action to be undertaken independently of any interference from another power, the politicians. During the investigation, the prosecutors were accused by the judicial authorities of having violated state secrecy during the*

investigation. They were also prosecuted for endangering national security. The former Italian President brought proceedings against the members of the judiciary and took them to court. I think the police criminal investigators were also taken to court. The prosecutors stood firm, as did the prosecution service itself. They carried on their investigation. It has to be said that the results are exceptional."

Respect for fundamental rights as a criterion of effectiveness

According to Maurizio Romanelli: *"Illegal means of countering terrorism must be prosecuted by the judicial authorities in all our countries. The judiciary must not be in any doubt on this matter, no concessions or compromises must be made when we are talking about illegal practices. In Italy, domestic terrorism has been eradicated by legal means, in the courts not in the stadium. After the 2001 attacks and the US administration's choice of the war on terror, Italy restarted the debate on these issues clearly and effectively. For Silvio Berlusconi, it was not possible to eradicate terrorism with the penal code. According to a part of the political class at the time, the instruments of the law were not effective enough to eradicate terrorism. As if the rule were not sufficient, and as if judges and prosecutors were pointless and created problems because they require rules to be respected. But torture is banned and if effects are harmful."*

In the case of Italy, the Abu Omar case therefore caused some very negative effects, whether in the security services or within ongoing criminal investigations: *A fracture occurred as a result of this affair. Although the political powers did not want to replace the people involved, they were replaced even those in the highest positions. The people chosen had the capacity to recreate new relations between the intelligence services and the judicial authorities. Today those relations are good and based on trust, but it was difficult to achieve. (…) As we said, there was an ongoing criminal investigation concerning Abu Omar, his role and his terrorist network. In actual fact, criminal investigations do lead to results. In the end Abu Omar would have been arrested and convicted, without the intervention of the US intelligence services*".

SPECIAL FOCUS

European migration crises: is there a risk of terrorism?

By *Dimitri Zoulas*, police superintendent,
internal security attaché at the French Embassy in Greece

"A first point needs to be made clear: no European police force has established a link between the migratory phenomenon and terrorism. What I have observed in Greece, over the period from 2012 to 2017 is a situation where migratory routes are used by terrorists."

- The 2015 refugee crisis: "*The normal application of national laws was distorted in 2015, because of a year-long disappearance of borders and foreigners' rights. A state of great confusion was maintained in 2015 between migrations and refugee status whereas the two are completely different. Why did we go from 100,000 migrants a year to 1 million migrants in 2015? Why did the refugees only flee the war in 2015? In Greece, that year marked the arrival in government of the left-wing radical Tsipras. His party's proposals were the same as those of the No Borders organisations. Syriza abolished the borders and foreigners' rights in January 2015. The government closed down the administrative retention centres and opened the borders. From March onwards, we went from 4,000 to 80,000 migrants per month and then 210,000 in October. At the same time, during the summer, Germany decided on a welcoming policy: this opened up a breach that was logically interpreted by criminal organisations as a business opportunity. They massively recruited refugees; at 1,000 dollars per crossing they made a billion."*

- The Greek situation before 2015 and the importance of criminal organisations: "*Greece is the first point of entry for illegal immigration into Europe - we are not talking about asylum, but illegal immigration. Three million people enter the Schengen area from outside the EU via Greece. You have a particular policy in Turkey, which encourages the arrival of migrants in Greece; and one factor that is perpetually underestimated: criminal organisations. The identification of the members and repression of these organisations are completely inadequate. Police forces and judges only rarely examine the contents of the mobile phones of the migrant arrested to find out where he comes from and trace the rest of the network (especially in Greece). Migrant trafficking is people trafficking - it is organised crime. I would ask Europol: who is responsible for this trafficking? In 2015, when a million people came across, these organisations made a billion dollars. These are no small-scale people smugglers. When 8,000 people arrive in Lesbos, somebody is paying off the police. These mafia organisations have always existed. They co-exist with the structures of the Turkish state, but they also operate in other countries in Greece and Southern Italy. These criminal undertakings have legal frontages and have existed for a long time. The criminal organisations provide migrants with information on benefits, the asylum rules, real legal "briefings" (…). And yet to my knowledge, no knowingly organised links have been identified between criminal people-smuggling organisations and terrorist organisations. These migrant-trafficking criminal organisations are there to do business - they do not want to be involved with terrorist networks. The use of their networks by terrorists generally takes place without the criminal organisation being aware that the people are terrorists. The link does not exist, but the freer to operate and the stronger the migrant-trafficking criminal organisations are, the greater the risk of them taking people through to London. Fighting these criminal organisations means making it more difficult for terrorists to move about. Since all these events, we start to be interested in the flows of people. And we are not taking an interest in the equipment being moved (weapons, explosives). We check the lorry driver, not yet the contents of the lorry."*

- The terrorist risk: *"Before 2015, we were already dealing with Jihadist networks. In 2005, the Greek police arrested a man, who was carrying a false French passport, which was checked in the SIS and found positive. The Greeks arrested him and then expelled him to Morocco. The 190 people in his mobile phone contacts list enabled an investigation in France and the neutralisation in the Paris region of two Iraqi Islamist cells, one of which was planning an attack on the DST (national surveillance directorate). We were therefore already running this risk twelve years ago : these people take the same channels as*

illegal immigrants. If checks were made, we could detect suspicious persons (…) The materialisation of the terrorist risk in 2015: we knew that in January 2015 one of the main organisers of these attacks in Paris and Brussels was living in Athens. The Belgian investigation located him there. Abaaoud could have been arrested thanks to judicial cooperation and the information sent by Belgium to Greece. The Greeks found two apartments after the Verviers operation in January 2015. In one of them, one person claimed to be a Syrian refugee and had an asylum seeker's documents. The Greeks took his fingerprints and sent them via SIREN to all European countries. Belgium was not aware of this man, who was still not arrested. The fingerprints sent to France led to the identification of a French man, one of the main leaders of the Trappes network. Thus in January 2015, members of the Islamic State organisation (IS) were claiming to be Syrian refugees and living in Athens to run cells that were intending to strike in Belgium. IS had already taken advantage of the weak border controls. After 13 November, we discovered that on 3 October two suicide bombers had passed through a Greek island where they presented as Syrian refugees and they were allowed to go. We tried to find out who had been on the same island on the same day, and thanks to the investigations we found two more terrorists (who were caught in Austria). The major investigation on the Paris and Brussels attacks has shown that a large number of perpetrators had followed the same routes. This all reveals that the tools we rely on are not able to cope with a migratory crisis on this scale."

- The situation after the November 2015 attacks: "*Today, the migratory crisis is over; Europe has made an agreement with Turkey, and the flows have become manageable, with about a hundred people arriving each day. The flows have dried up because after the Paris attacks, the Balkan countries closed their borders. (…) But every three months the European Commission produces a report that notes the weak links in the external borders which enable controls to be reintroduced. (…) After 2015, the EU created "hotspots". These are centres where the European agencies (Frontex, Europol) have a presence. All the migrants arriving in Greece and Italy are grouped together to be registered. This control is still insufficient: each migrant is screened to check the information given (three minutes), then their fingerprints are taken. These fingerprints are for Eurodac, but after that no police databases are connected. The person's name is put through the system on the base of his declarations; often they have no papers. The name is put into the SIS database where there is no photo thus we are not able to check if we are aware of this person. Then into the Interpol SLTD database. This is what the checks in the hotspots consist of, no more, no less. (…) There is also a positive element with the relocation programmes. The EU has offered to take 160,000 people; France is taking 400 a month as candidates for refugee status. The list of these people is put through the French databases, and they are brought to a special building in Greece to be interviewed. The Germans are relocating 500 people from Greece without interviewing them first. Even that is dangerous, but I am not challenging it."*