THE FIGHT AGAINST VIOLENT EXTREMISM AND RADICALISATION LEADING TO TERRORISM: TACKLING “THE ROOTS OF THE ROOTS OF INSECURITY”

AURELIE GARBAY
Ph.D. Student in Public Law
CDRE – Université de Pau et des Pays de l’Adour – France

Keywords: Democracy, terrorism, Rule of Law.

Considering violent extremism and radicalisation leads to focus on the earliest stage of insecurity, at the beginning of a process that may end with the perpetration of a terrorist act.

In the collective imagination, notably since 9/11 and the “war on terror”, radicalisation and violent extremism were mostly linked to Jihadism. The recent movements observed regarding EU citizens deciding to reach Syria tend to confirm this trend\(^1\). However, it must be considered as a multifaceted phenomenon, embracing various ideologies – separatism, racism, religion-based, from political left to right… – and affecting as groups as lone wolves – as shown by the Breivik case. It is also multi-located, without borders: individuals can be radicalised at home notably due to the Internet\(^2\), as well as abroad, and once turned to terrorism, can perpetrate their actions on their home territory as well as in a foreign State\(^3\).

For States and for multilateral systems – e.g. the European Union (EU)\(^4\) –, developing strategies dedicated to radicalisation appeared as a mean to tackle the root causes of terrorism,

\(^1\) Facing this problem and notably taking into account the increasing number of French citizens leaving for Syria, Bernard Cazeneuve, French Minister of Homeland security, launched in April 2014 an action plan against the Jihadist networks based on three pillars: countering terrorists’ movements to and from Syria, intensifying the fight against Jihadist networks notably by developing detection and surveillance activities of the Intelligence services, and finally helping families notably by opening a free hotline to report suspect behaviours. *Vid.* Cazeneuve B., Communication to the Council of Ministers “Le plan de lutte contre la radicalisation violente et les filières terroristes”, 23 April 2014.

\(^2\) *Vid.* Europol, EU terrorism situation and trend report TE-SAT, 2013, p. 18 and 37.


\(^4\) Since 2005 and a Commission communication concerning the factors contributing to violent radicalisation – European Commission, Communication from the Commission to the Parliament and the Council concerning terrorist recruitment: addressing the factors contributing to violent radicalisation, COM (2005) 313 final, 21 September 2005 –, the EU institutions launched several actions in order to enhance the understanding of radicalisation and fight against this phenomenon. Notably, in 2008, the EU financed evaluations – 6\(^{th}\) Framework Programme, “The EU Counter-radicalization strategy – Evaluating EU policies concerning causes of radicalization”, Workpackage 4, deliverable 7, May 2008 and “Radicalisation, recruitment and the EU Counter-radicalisation strategy”, deliverable 7, 17 November 2008 – which were used as the basis, along with the observations of the Terrorism Working group, to set up the Radicalisation Awareness Network in 2011.
the “roots of the roots of insecurity”. It is a matter of prevention in order to protect their integrity and their citizens. Nonetheless, for democratic systems, the fight against this phenomenon must address the issue of conciliating opposed objectives: the right to security on one side, individual rights and freedoms, on the other side. More precisely and from a “Kelsenian perspective”, for States parties to the European Convention on Human Rights (ECHR), the strategies they implement must not only comply with their constitutional framework on limitations of their citizens’ individual rights and freedoms, but also with the ECHR standards and their interpretation by the European Court of Human Rights (ECtHR). Thus, focusing on States parties to the ECHR allows operating an examination regarding the preservation of a fair balance between public order and individual rights and freedoms, and the potential modifications in their apprehension, with a referential accepted as an established standard regarding the protection of human rights. This question is also a challenge for multilateral systems for instance the EU, whose apparatus is bound by the European Charter of fundamental rights⁵.

To be qualified as democratic systems, in application of the Rule of Law, their apparatus must comply with this framework. However, the study of the fight against terrorism reveals that systems tend to maximize their repressive action towards the exceptional nature of this threat⁶, with two outcomes. On the one hand, democratic systems adapted their apparatus to meet its specificities, notably by reconsidering the balance in the conciliation between the needs for security and the exercise of fundamental rights and freedoms; this first outcome should be considered as an “adaptation” as the modifications were conducted while ensuring that the new equilibrium would be in agreement with the democratic framework, in accordance with the Rule of Law. On the other hand, systems developed instruments in breach with their constitutional or international constraints; such infringements to the Rule of

---

⁵ When its accession will be completed, the EU will also be bound to respect the ECHR and will be placed under the control of the ECtHR.

⁶ Described by R.D. Crenlsten as “the deliberate use of violence and threat of violence to evoke a state of fear (or terror) in a particular victim or audience” – Crenlsten R.D., “Terrorism as political communication: the relationship between the controller and the controlled”, in Wilkinson P., & Stewart A.M., (ed.), Contemporary research on Terrorism, Aberdeen University Press, Aberdeen, 1987, p. 6 – terrorism appears for democratic systems as an exceptional phenomenon, considering three elements. Firstly, because the State does not face a traditional threat, such as a declaration of war by another State, despise G.W. Bush’s rhetoric after the 9/11 attacks – for instance the use of the “war on terror” in his speech at the graduation ceremony on 2nd June 2002, at West Point.

Secondly, the fighters are, sometimes to often, its own citizens – for instance in the case of the Basque terrorism, or in the Breivik case.

Thirdly, although it is considered as an extraordinary threat, the above considerations call on the systems claiming themselves to be democratic to ensure their protection with “weapons” set up under ordinary circumstances, passed under ordinary proceedings, in order to face an ordinary threat.
Law, regardless of reason or forms, appear to be frequent leading to a severe alteration of the democratic framework, notably when they relate to principles constitutive of its very essence. As it aims at tackling terrorism at an early stage, the fight against radicalisation is to be analysed in this context, while taking into consideration a specific aspect: radicalisation deals with a moment when a crime has yet to be committed. It was thus necessary for systems to develop mechanisms taking into account this particularity (I), while facing the risk of prejudicial transgressions to the democratic framework (II).

I – RADICALISATION: A DISTINCTIVE PHENOMENON REQUIRING A SPECIFIC APPROACH

The concept of “violent radicalisation” appeared for the first time in the European terrorist vocabulary in 2005, in a Communication from the Commission to the Parliament and the Council\(^7\). It is defined as “the phenomenon of people embracing opinions, views and ideas which could lead to acts of terrorism as defined in Article 1 of the Framework Decision on Combating Terrorism”\(^8\). In itself, this definition reveals the fundamental specificity of radicalisation: it is not a positive act than can be observed and objectively apprehended, as could be the set up and use of an explosive device. Indeed, it is an internal process, dealing with individuals’ mind. Its apprehension by traditional legal mechanisms thus appears to be compromised (A). However, as inaction facing this phenomenon and its consequences seemed unacceptable, States and multilateral systems developed counter-radicalisation mechanisms based on intelligence gathering (B).

A – The inadequacy of a specific incrimination related to radicalisation

As introduced by the EU definition, radicalisation appears as a process narrowly linked with individuals’ thoughts; the opinions, views and ideas considered must be radical enough to constitute the premise of the perpetration of an act of violence. This assertion raises several concerns, explaining the inadequacy of an incrimination related to radicalisation: the inextricable link with individuals’ subjectivity on one side, the difficulty to determine what is radical on the other side.


\(^8\) Council of the EU, framework-decision 2002/475/JHA on combating terrorism, 13 June 2002.
Radicalisation must be understood together with the personal reception of a context or a message, the individuals’ subjectivity. More precisely, depending on personal perceptions, a same message may be apprehended as the mere expression of ideas or as an incitement to commit terrorist acts. The establishment of an incrimination related to such messages would require to objectively determine which contents should be considered as objectionable and thus, as criminal, as it is the case, for instance, for child pornography. However, such approach would collide with the inner subjectivity of the reception of the message. In this sense, it should be noted that what might in the first place be considered as a form of radicalisation may, after an in-depth examination, turn out to be the consequence of a misinterpretation or the result of the psychological weakness of an individual feeling rejected or discriminated, and who finds answers to her/his dismay in extremist ideas and those who represent them.

For instance, a same statement related to a correlation between the rise of immigrants in a country and the rise of unemployment could have different interpretations depending on, for example, its recipient’s political ideas, social situation – employment status – or living condition – real or perceived insecurity in the neighbourhood. The reception of the same message could thus vary from a given fact that the individual would hear or read without follow-up, to a call to take actions against foreigners. It should also be added that, although a high number of “negative” criteria would be met, there is no guarantee that the recipient would eventually commit a terrorist act.

Regarding the expression of radical idea, Article 10-2 of the ECHR admits that the exercise of this freedom “may be subject to (...) restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity

---

9 In 2011, the EU institutions adopted the directive 2011/92/EU – European Parliament and Council, Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council framework decision 2004/68/JHA, 13 December 2011 –, which Article 2-c defines a wide range of contents considered as child-pornography; however, it should be noted that, unlike radical contents, child-pornography is under the “explicit content seal”, which means that the elements concerned can objectively be identified as criminal materials.


12 For instance, “in addition to anti-immigrant demonstrations, in 2013 some EU Member States experienced violence in the form of arson attacks on asylum seekers’ hostels or houses known to be inhabited by immigrants” – Europol, EU terrorism situation and trend report TE-SAT, 2014, p. 40.
or public safety, for the prevention of disorder or crime”. This provision consequently allows States adopting norms limiting freedom of expression when the exercise of this right would alter Public Order. Nonetheless, in order to comply with the principle “nulla poena, nullum crimen sine lege”, a law incriminating radicalisation would require to define with sufficient precision what “radical” means\textsuperscript{13}. This issue is a major difficulty regarding the incrimination of this phenomenon. It indeed relates to the idea that it would be possible to determine a threshold over which opinions, although not explicitly calling to violence, should be considered as criminal, or, considering the political spectrum, a spectrum of views that could be considered to be “the good/acceptable political opinions”. This approach creates risks of enhanced real and perceived stigmatisation and discrimination, as well as harms to pluralism.

The “explicit content criterion” appears to be decisive, although, as previously analysed, it does not seem applicable to the question of radicalisation. Although in the current state of law in Europe, the establishment of an incrimination dedicated to radicalisation seems inadequate, recent moves towards the criminalisation of “indirect incitement to terrorism” could be understood as a way to offset these difficulties. Indeed, the 2005 Council of Europe Convention on the prevention of terrorism calls its parties to establish as a criminal offence “the distribution, or otherwise making available, of a message to the public, with the intent to incite to the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed”\textsuperscript{14}. The explanatory report presents however precisions regarding how to address this offence. In particular, these provisions differ from the criminalisation of the expression of radical opinions in the sense that the indirect incitement to terrorism requires “a specific intent to incite to the commission of a terrorist offence”\textsuperscript{15}. This offence is not, thus, based on the subjective interpretation of the message by its recipients, but on its issuer’s intention and its actual content, “presenting a terrorist offence as necessary and justified” for instance\textsuperscript{16}. To be

\textsuperscript{13} Vid. ECtHR, 26 April 1979, Sunday Times v. The United Kingdom, case n° 6538/74, § 49: “a norm cannot be regarded as a “law” unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail”.

\textsuperscript{14} Council of Europe Convention on the prevention of terrorism, CETS n°196, 16 may 2005, Article 5-1. Similar provisions may be found in the Council of the EU framework decision 2008/919/JHA of 28 November 2008, amending framework-decision 2002/475/JHA.

\textsuperscript{15} Council of Europe Convention on the prevention of terrorism, CETS n°196, Explanatory report, § 99.

\textsuperscript{16} Vid. ECtHR, 2 October 2008, Leroy v. France, case n° 36109/03, on a drawing published in a weekly newspaper – Ekaizta, left-wing and abertzale (Basque nationalist) – and showing the destruction of the World Trade Centre towers with the caption “Nous en avions tous rêvé, le Hamas l’a fait” – “It was our dream, Hamas did it”.

5
constitutive of an offence, a second criterion must be met, “the significance and credible nature of the danger” of perpetration of a terrorist act. This definition, well detailed and approved by the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism as a best practice\textsuperscript{17}, reinforces the idea that an incrimination cannot be based on the presupposition of a subjective interpretation, varying from one individual to another.

Although its incrimination is unsuitable in the current state of law, tackling radicalisation remains of major interest for democratic systems seeking to develop strategies in order to protect themselves from terrorism.

\textbf{B – The inclination for intelligence gathering measures in countering radicalisation}

Radicalisation is not a recent phenomenon, and some States, notably with experience of home-terrorism, had set up strategies before the 9/11 attacks in order to counter this phenomenon. For instance, in France and in Spain, in order to fight against radicalisation by \textit{Euskadi Ta Askatasuna} – Basque Country and Freedom, \textit{ETA} – in prisons, the penitentiary administrations not only apply confinement to \textit{ETA} prisoners, but also “disperse” them, avoiding their gathering in a same prison or their detention near their home place\textsuperscript{18}. Thus, the lack of a specific incrimination does not prevent systems from fighting against radicalisation. Apart from this specific example, most actions are surveillance measures and lay in the hands of the intelligence services\textsuperscript{19}. The outcomes of these measures, which may vary from field to online surveillance, are considered to offer a better understanding regarding the suspicious individuals’ relationships with identified radical or criminal groups and, possibly, regarding connections allowing preventing the terrorist threat at an early stage.

\textsuperscript{17} United Nations, General Assembly, “Protection of human rights and fundamental freedoms while countering terrorism”, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, n° A/61/267, 16 August 2006, § 28: “The Special Rapporteur would like to refer to article 5 of the Convention on the Prevention of Terrorism of the Council of Europe as a best practice in combining the element of intent and the risk of the commission of a terrorist act”.


\textsuperscript{19} It should however be noted that the Northern Europe approach relies both on intelligence services and frontline workers – for instance, school and education agents, healthcare staff, community agents, etc. \textit{Vid.} Directorate General for internal policies, Policy Department C: Citizens’ rights and constitutional affairs, “Preventing and countering radicalisation in the EU”, study for the LIBE Committee, PE 509.911, 2014.
Among their traditional instruments, intelligence services use sound and recording systems, as well as computer data capture in public locations and individuals’ private premises. To be efficient, such measures must be conducted discreetly, without the consent of the concerned individual, and State officers may enter private premises in order to set up the required equipments. Such methods may consequently create harms to fundamental rights, notably right to privacy. However, the ECtHR ruled that the preservation of Public Order regarding exceptional threats such as terrorism justifies the restrictions to this right and thus, the use of these methods, as long as the related provisions regarding such interferences are clear and precise enough\(^{20}\).

EU member States may also use discreet surveillance mechanisms provided by Article 36 of the 2007/533/JHA framework decision\(^{21}\) and conduct discreet checks. These provisions allow judicial authorities to integrate alerts in the Schengen Information Systems – SIS –, on individuals and objects for the prevention of threat to public security “where there is clear indication that a person intends to commit or is committing a serious criminal offence”, or “where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit serious criminal offences in the future”. It should be noted under these provisions, it is not necessary that the concerned individual had committed an offence; the recording of a file is based on the assumption of a potential threat. These provisions are used in order to “track” the recorded individuals and may be of great use regarding the fight against radicalisation. Indeed, in case of police control of an individual under this surveillance regime, the officer is not supposed to arrest the person, but rather to conduct checks that must be seen by the person as a routine control, while the officer should make sure to gather relevant information – provided for in Article 37-1\(^{22}\). The purpose of this mechanism is to deepen the comprehension of a suspicious individual in order to have a clearer overview of the group(s) s/he belongs to, her/his routine trips or if s/he may meet up with other individuals identified as suspicious for instance. This mechanism


\(^{21}\) Council of the EU, decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II), 12 June 2007. These provisions were previously contained in Article 99 of the Convention implementing the Schengen Agreement.

\(^{22}\) Council of the EU, decision 2007/533/JHA, Article 37-1: “a) the fact that the person for whom, or the vehicle, boat, aircraft or container, for which an alert has been issued, has been located; b) the place, time or reason for the check; c) the route and destination of the journey; d) the persons accompanying the persons concerned or the occupants of the vehicle, boat or aircraft who can reasonably be expected to be associated to the persons concerned; e) the vehicle, boat, aircraft or container used; f) objects carried; g) the circumstances under which the person or the vehicle, boat, aircraft or container was located”. 

7
offers many possibilities regarding the surveillance of radical individuals. However, it raises questions regarding the preservation of their fundamental rights, not only related to privacy and data protection, but also regarding the phrasing of the provisions – e.g. the “overall assessment of a person” or the extensiveness of the State authorities’ interpretation of the “clear indication” –, notably considering the fact that there is neither harmonised interpretation of these provisions nor harmonised procedures in order to integrate such alert in the SIS. Moreover, this mechanism suffers a lack of judge or parliamentary monitoring, which may counterbalance the extensive police prerogatives in a more complete application of the principle of separation of powers than the EU-LISA Agency monitoring.

Although remaining of great use for intelligence services, these field surveillance methods had to be completed with new forms of online surveillance measures in order to integrate the rise of the Internet as a key platform of communication for terrorist groups, as well as for dissemination of radical ideas. In 2005, the EU strategy for combating radicalisation and recruitment to terrorism recommended an “effective monitoring of the Internet and travel to conflict zones”, calling States to take actions regarding this matter. However, as previously analysed, one of the major issues regarding radicalisation on the Internet is related to the fact that radical contents are not explicit. Consequently, pursuit and banning appear to be complex, as such actions would interfere in the preservation of freedom of expression. Nonetheless, States may turn this situation to their advantage, by monitoring suspicious websites and forums and their visitors. In cases of deeper suspicions, overlaps could be considered in order to check if travels were made or booked to sensitive destinations with specific data systems. Such methods were used by the French intelligence services in the Merah case, although it did not prevent Mohammed Merah from committing several terrorist attacks.

23 The second generation of the Schengen Information System is under the monitoring of the EU-LISA agency, which “shall ensure that procedures are in place to monitor the functioning of SIS II against objectives, relating to output, cost-effectiveness, security and quality of service” – Council of the EU, decision 2007/533/JHA, Article 66-1. Among its missions, the Agency shall present evaluation reports to the EU council, but also to the EU Parliament, ensuring a form of democratic control over the System, and is itself under the monitoring of the European Data Protection Supervisor – Council of the EU, decision 2007/533/JHA, Article 61 and EU Parliament and Council, Regulation (EU) n° 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 25 October 2011.

24 For a focus on selected UK cases, for instance of online radicalisation, Vid. RAND Europe, “Radicalisation in the digital era – the use of the Internet in 15 cases of terrorism and extremism”, 2013.

25 For instance, with the Advance Passenger Information System – APIS.

These intrusive methods surely offer a way to address the lack of a specific incrimination from a preservation of security perspective. Nonetheless, it must be reminded that the targeted individuals have not committed an illegal act yet, and may never do. Thus, the legal basis of surveillance instruments, the “presumption of a potential threat”, seems to announce an evolution in the understanding of major democratic principles.

II – FIGHTING AGAINST RADICALISATION: THE DEMOCRATIC FRAMEWORK AT STAKE

In 2008, the ECtHR enlightened the fact that fighting fire with fire would be counter productive as it would “give terrorists the perfect pretext for martyrdom and for accusing democracies of using double standards. Such a course of action would only serve to create fertile breeding grounds for further radicalisation and the recruitment of future terrorists”27. It is hence important that democratic standards remain, with appropriate monitoring in order to avoid such perilous evolution. Nonetheless, the development of proactive strategies and the will to take actions as early as possible led systems to extend the scope of police prerogatives (A), sometimes without simultaneously extending the related safeguards (B), which may result in undermining the democratic quality of the systems these measures were supposed to protect.

A – Redefining key democratic principles: a perilous tendency

Fighting against terrorism leads, as previously outlined, to restrictions and interferences in the preservation and exercise of fundamental rights and freedoms. These adjustments may be accepted under particular circumstances in order to protect Public Order, when they meet specific criteria notably defined by the ECtHR: be prescribed by law, pursue a legitimate aim and be necessary in a democratic society. However, some fundamental rights are established as inviolable rules as they are considered to be key principles structuring the democratic framework. Among them, the principle of presumption of innocence28, which is regarded as a

27 ECtHR, 28 February 2008, Saadi v. Italy, case n°37201/06, concurring opinion of Judge Myjer, joined by Judge Zagrebelsky.

28 On the notion of presumption of innocence, vid., inter alia, Koering-Joulin R. et al., La Présomption d’innocence en droit compare, symposium organised at the Cour de Cassation by the Centre français de droit
democratic standard\textsuperscript{29}, and is enshrined by Article 6-2 of the ECHR. The recognition of the right to be presumed innocent notably aims at avoiding stigmatisation of the individual not found guilty – yet – by Court\textsuperscript{30}. Its scope involves the penal proceedings, including, according to the Committee of Ministers of the Council of Europe\textsuperscript{31}, to the benefits of a person accused of terrorist activities. One of the specificities of the fight against radicalisation relates to the fact that it is led outside this scope, in a “\textit{para penal}” dimension\textsuperscript{32}, where the notion of presumption of innocence faces the notion of dangerousness.

Terrorism is an unpredictable threat and its consequences may be disastrous. States fight against this phenomenon by investigating on attacks and prosecuting its presumed authors, but they also seek to mitigate its effects by acting before the perpetration of a terrorist act. They thus work on its unpredictability and apply the precautionary principle. Derived from environment law\textsuperscript{33}, in a broader conception, it is considered as a principle for guiding public policies under which the lack of certainty on the reality of a risk should not prevent State authorities from taking reasonable preventive measures in order to avoid its materialisation\textsuperscript{34}. Applied to the fight against terrorism, States assume dangerousness and set up early detection and surveillance measures, such as the mechanisms previously analysed. This approach is one of the stated objectives of the EU counter radicalisation strategy, which intends to “\textit{disrupt the activities of the networks and individuals who draw people into terrorism}”\textsuperscript{35}.

\textsuperscript{29} Presumption of innocence, depending on sources, may be qualified as “democratic standard” – Besse M. \textit{et al.}, \textit{Délits de presse et Démocratie}, Fondation Varenne, 2012, p. 149 – but also as “principle” – Guinchard S. & Montagnier G., \textit{Lexique des termes juridiques}, Dalloz, 14\textsuperscript{th} édition, 2003, p. 450.

\textsuperscript{30} ECtHR, 18 April 2013, \textit{M.K. v. France}, case n° 19522/09, notably §36.

\textsuperscript{31} Council of Europe, Committee of Ministers, Guidelines on human rights and the fight against terrorism, 804\textsuperscript{th} meeting – 11 July 2002, IX – Legal proceedings, § 2.


\textsuperscript{34} Guinchard S., Montagner G., \textit{Lexique des termes juridiques}, Dalloz, 14\textsuperscript{th} ed., 2003, p. 445.

These measures aim at anticipating the threat, detecting it as early as possible – if manageable, before the adherence to radical and violent ideas\(^{36}\). To this end, the presumption is not of innocence but, rather, of dangerousness, which is particularly significant in the wording of the related norms. For instance, the provisions of Article 1 of the Agreement of 10 January 2008 evoke “individuals likely to support or to perpetrate terrorist acts”\(^{37}\); similarly, Article 36 of the Decision 2007/533/JHA allows integrating alerts in the SIS on the assumption that a “person will (...) commit serious criminal offences in the future”. Thus, State authorities rely on a presumption of dangerousness, a presumption of “possible future culpability” of an individual, although s/he has not committed the “culpa” yet.

These measures may create a form of rejection when the individuals realise that their personal data are used for surveillance purpose by State authorities\(^{38}\). They may also create a feeling of stigmatisation, notably when the individual was not found guilty but his data, collected for the investigation, are stored after the end of the criminal proceedings. The UK Government’s argument justifying such measure in the Marper case reflects this redeployment of the presumption from the notion of innocence to the notion of dangerousness. Indeed, the Kingdom authorities considered that storing these data “would assist in the future prevention and detection of crime in general by increasing the size of the database”\(^{39}\). This redeployment is particularly worrying regarding “the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are

\(^{36}\) The Danish pilot project – Thomsen M.H., “Deradicalisation – targeted intervention” - Brief summary of Danish pilot experience with deradicalisation and prevention of extremism, June 2012 – is a clear illustration of the implementation of the presumption of dangerousness. This project aims at developing “methods and tools to deal with radicalisation of young people and work against young people’s engagement in extremist environments that resort to violence or justify the use of violence” (Thomsen, p. 3). One of the essential questions in the conduct of this programme was how to target the young individuals “who could be assumed to be vulnerable to radicalisation” – image/appearance, behaviour, expression of opinions and relations – and thus, which criteria should be applied. Their target group was thus delimitated on the basis of “worrying signs and personal welfare problems” (Thomsen, p. 10).

\(^{37}\) Agreement of 10 January 2008 between the Government of the French Republic and the Government of the Kingdom of Spain on the cooperation in the fight against terrorism. This Agreement establishes joint – French-Spanish – permanent intelligence units dedicated to preventive actions against terrorism by detection, identification and localisation of individuals likely to support or to perpetrate terrorist acts. They were born from a “bottom-up effect”, in the framework of the fight against Basque terrorism, a cross border issue for these two States.

\(^{38}\) For instance, 10,000 persons demonstrated in Berlin on 12 September 2009 for a greater protection of their personal data, but also for the respect of their individual and fundamental rights, by “Big Brother”s eye – “Berlin: plus de 10000 personnes manifestent contre Big Brother”, Libération, 12 septembre 2009. More recently, the “PRISM scandal” led not only to an important Media coverage, but also to a reaction from the EU – EU Commission, Reding V., “PRISM scandal: The data protection rights of EU citizens are non-negotiable”, speech on 14 June 2013, ref. SPEECH/13/536.

\(^{39}\) ECtHR, 4 December 2008, S. and Marper v. The United Kingdom, cases n° 30562/04 and 30566/04, § 94.
entitled to the presumption of innocence, are treated in the same way as convicted persons”\textsuperscript{40}. It should also be noted that this case was not related to terrorism, but to attempted robbery and harassment; taking into account the intensity of the threat that terrorism represents for States, it would be legitimate to consider that, to counter terrorism, a same rationale would be followed in order to extend the ordinary rules and retain such data for a longer period of time.

The redeployment of the notion of presumption aims at fighting efficiently against terrorism, by striking the threat at its roots, in order to achieve an ultimate objective: preserving the democratic framework. This conception tends to be extended from discreet surveillance to legal prosecutions. The presumption of dangerousness is indeed particularly present in proactive measures, such as the French “association de malfaiteurs en relation avec une entreprise terroriste” – criminal association in connection with a terrorist enterprise, AMT – the former director of the French intelligence services qualified as “preventive legal neutralisation”\textsuperscript{41}. Established as a terrorist offence under the French penal Code\textsuperscript{42}, this sophisticated repressive legal regime allows arresting individuals in order to dismantle radical groups “before the perpetration or attempted commission of an attack”\textsuperscript{43}. Although this “dragnet” strategy includes the intent criteria – in the sense that the participants are considered to know that their contribution would help to the perpetration of a terrorist attack –, it is used at a stage when the individual has not committed the “culpa” yet, but rather one or more – suspicious, although undefined by the penal Code – material act(s). Interestingly, while this mechanism represents the majority of the French convictions for terrorism\textsuperscript{44}, a high number of the persons concerned, questioned in custody of even held in pre-trial detention, are dismissed during the investigations or found innocent by Court\textsuperscript{45}. Nonetheless, notably when placed in pre-trial detention, they face the same conditions as convicted persons, which is precisely the element the ECtHR argued against in the \textit{Marper} case.

\textsuperscript{40} ECtHR, \textit{S. and Marper v. The United Kingdom}, § 122.


\textsuperscript{42} Similar provisions are established in Article 576 of the Spanish \textit{Código Penal}, under the wording “colaboración con asociación terrorista”.


\textsuperscript{44} For figures, \textit{vid.} Bigo D., \& \textit{al.}, \textit{Au nom du 11 septembre... Les démocraties à l’épreuve de l’antiterrorisme}, Paris, La Découverte \textquoteleft\textquoteleft Cahiers libres”\textquoteright\textquoteright, 2008, p. 184.

This tendency may consequently indicate a drift, which may endanger the framework these measures were supposed to protect.

**B – Maintaining democratic systems in the democratic framework: a challenge to succeed**

The objective of a system setting up an apparatus in order to fight against terrorism, regardless the stage – from early detection to detention –, is to protect itself, to ensure its continuity, to safeguard its foundations. For a system claiming itself to be complying with the Rule of Law, it implies the respect of an essential principle: always acting within the constraints of the law. However, facing terrorism, States and multilateral systems tend to challenge the boundaries of security, at the expense of the respect of other norms they freely committed themselves to. The fight against radicalisation provides an eloquent example for this drift towards a more repressive approach, notably at the pre-attack stage. A fundamental question arises: is this approach of the fight against terrorism, initially intended to protect democratic systems from an extraordinary threat, leading to sink them?

A year after the 9/11 attacks, W. Schwimmer, Secretary General of the Council of Europe, expressed such concerns regarding a balanced approach between the preservation of security and the respect of Human rights. Indeed, “the temptation for governments and parliaments in countries suffering from terrorist action is to fight fire with fire, setting aside the legal safeguards that exist in a democratic state. But let us be clear about this: while the State has the right to employ to the full its arsenal of legal weapons to repress and prevent terrorist activities, it may not use indiscriminate measures which would only undermine the fundamental values they seek to protect. For a State to react in such a way would be to fall into the trap set by terrorism for democracy and the rule of law.” Following this logic, safeguards but also monitoring mechanisms should be set up in order to ensure that the measures used do not exceed the democratic constraints. To this end, the judge may play a

---


crucial role\textsuperscript{48}, and counterbalance interferences to fundamental rights and freedoms conducted on the basis of a presumption of dangerousness and uncertain elements\textsuperscript{49}.

However, regarding the fight against radicalisation, this actor seems to be left out of this “\textit{para} penal” dimension, which raises concerns related to the existence of a fair balance of powers, key element in order to strengthen the supremacy of the Rule of Law\textsuperscript{50}.

For instance, although the alerts registered in the SIS on the basis of Article 36 of the Decision 2007/533/JHA appear of great importance in order to proactively counter radicalisation and terrorism, their registration show a lack of monitoring by the judge. Indeed, there is neither \textit{ex ante} control of the suitability, nor of the “necessity in a democratic society” of the registration of an alert. These measures have not faced the Courts – yet –, neither the ECtHR nor the European Court of Justice – ECJ\textsuperscript{51}. However, regarding discreet surveillance measures, the ECtHR considers that, in the case of such interferences by the Executive, the Rule of Law implies a control by the Judiciary as “\textit{offering the best guarantees of independence, impartiality and a proper procedure}”, which may be substituted by an independent control from a Parliamentary board\textsuperscript{52}. The French-Spanish permanent intelligence teams established under the Agreement of 10 January 2008 might illustrate this second form of monitoring. The provisions of the Agreement of 10 January 2008 do not precise how the activities of these teams should be monitored. They actually use traditional intelligence gathering methods\textsuperscript{53}, provided for in the French and Spanish Law, subject to a dual form of control. On the one hand, both the French \textit{Code de Procédure pénale} and the Spanish \textit{Ley de enjuiciamiento Criminal} impose an \textit{ex ante} authorisation by the judge; on the other hand, both national regimes impose a parliamentary monitoring of the intelligence

\textsuperscript{48} Barak A., \textit{The judge in a Democracy}, Princeton University Press, 2008, p. 285: “We, the judges in modern democracy, are responsible for protecting democracy both from terrorism and from the means the State wants to use to fight terrorism”.


\textsuperscript{51} As they derive from EU law, from provisions of the Decision 2007/533/JHA, such measures, although implemented at the national scale, are subject to appeal before the ECJ.

\textsuperscript{52} ECtHR, \textit{Klass and others v. Germany}, § 56.

\textsuperscript{53} Telephone tapping, sound recording, electronic and non-electronic correspondences, including flows of objects, goods and products.
services. This second form of control is less direct and ensured by several parliamentary commissions, each specialised in a particular matter\(^\text{54}\).

External appreciation of their methods might also press systems to reconsider their normative apparatus regarding its compatibility with the democratic framework. It is notably the case with the ECtHR judgements, when the ruling declared that there has been a violation of the Convention. In the Gillan and Quinton case, the ECtHR considered that the powers to “stop and search”, provided for under “Section 44” of the Terrorism Act 2000\(^\text{55}\), was excessively wide as insufficienlty precise\(^\text{56}\) and overly based on arbitrariness\(^\text{57}\), and that “the safeguards provided by domestic law have not been demonstrated to constitute a real curb on the wide powers afforded to the executive so as to offer the individual adequate protection against arbitrary interference”\(^\text{58}\). This case is interesting in the sense that not only the Government had to remedy the damage, but the UK also revised its legislation. In 2012, the Protection of Freedoms Act repealed the stop and search powers and replaced them by a new mechanism, taking into account the criticisms from the ECtHR. “The new stop and search powers enable the police to protect the public but also make sure that there are strong safeguards to prevent a return to the previous excessive use of stop and search without suspicion”\(^\text{59}\).

The development of mechanisms to fight against radicalisation is necessary in order to protect the integrity of the democratic systems. This issue should be however “handled with care” as it threatens their very essence. Indeed, an uncontrolled drift may lead to abuses and, eventually, to a situation in which the failures – as attempts to the Rule of Law –, frequently occurring in the fight against terrorism, including in States parties to the ECHR, could affect

\(^{54}\) For instance, in France, the Commission set up under Article 154 of the Finance Law for 2002 is empowered to control the use of the “special funds” allocated to the intelligence services. In Spain, this same issue is monitored by the Comisión de control de los créditos destinados a gastos reservados, empowered by the Law 11/1995 of 11 of May 1995.

\(^{55}\) The Terrorism Act 2000 provided the legal basis for prosecuting terrorists and proscribing organisations. It notably empowered – under Section 44 – police officers to stop vehicles and pedestrians, and to search it/her/him; these measures were allowed “for the purpose of searching for articles of a kind which could be used in connection with terrorism” (Section 45 1-a) and these powers could “exercised whether or not the constable has grounds for suspecting the presence of articles of that kind” (Section 45 1-a).

\(^{56}\) ECtHR, 12 January 2010, Gillan and Quinton v. The United Kingdom, case n°4158/05, § 80.

\(^{57}\) ECtHR, Gillan and Quinton v. The United Kingdom, § 83: “based exclusively on the “hunch” or “professional intuition” of the officer concerned”.

\(^{58}\) ECtHR, Gillan and Quinton v. The United Kingdom, § 79.

other areas. Presented as justified by their – real or apparent – efficiency, such abuses would thus “infect” the system and the Rule of Law, undermined in counterterrorism, would be also altered to the benefit of the broader fight against criminality. This possibility is cause of concern as it is real, despite the existing safeguards such as recourse procedures against systems, for instance before the ECtHR or the ECJ. States, for example Spain, attest of this phenomenon, regarding violations of imprescriptibly rights. Spanish State officers indeed use torture, especially during custody for terrorism – as held under incommunicado, a secret detention regime –, in impunity; for a few years, this failure has been spreading in the immigration area.

The development by democratic systems of protective mechanisms facing terrorism must thus be conducted concomitantly with the development of safeguards in order to ensure the durability of their democratic essence. It is a major and fundamental challenge.

---

60 Four cases related to allegations of torture under incommunicado detention for terrorism where brought to the ECtHR. The Court concluded to the violation of Article 3 of the ECHR by the Kingdom of Spain for the absence of a real and effective investigation. ECtHR, 2nd November 2004, Martinez Sala et autres v. Spain, case no 58438/00; 28 September 2010, San Argimiro Isasa v. Spain, case no 2507/07; 8 March 2011, Beristain Ukar v. Spain, case no 40351/05; 16 October 2012, Otamendi Egigurren v. Spain, case no 47303/08. A few cases where discussed before UN committees, notably:
- Committee Against Torture, 17 May 2005, Kepa Urra Guridi v. Spain, CAT/C/34/D/212/2002 (2005), notably § 6.6: “the obligation to take effective measures to prevent torture has not been honoured because the pardons granted to the civil guards have the practical effect of allowing torture to go unpunished and encouraging its repetition”.

61 For instance, on 17 October 2011, the Audiencia Provincial – Regional Court – of Barcelona sentenced two police officers to imprisonment for torture towards a student from Trinidad and Tobago in September 2006 (sentenced no 81/09). The Council of Europe Committee for the Prevention of Torture (CPT) also reported on several occasions that its the delegations received a high number of allegations of ill-treatment by Spanish security forces. Vid. the last report: CPT, Report to the Spanish Government on the visit to Spain carried out from 31 May to 13 June 2011, CPT/Inf (2013) 6, § 81s.