Democracies' Fight against Radicalisation in the European Union: From Self-Protection to Self-Destruction

Original article

Democracies' Fight against Radicalisation in the European Union: From Self-Protection to Self-Destruction

Aurelie Garbay*

Abstract: One of the main perils democracies face when fighting terrorism remains in their response to it. This paradox relates to the fact that, in order to protect their integrity, they may use instruments that do not comply with the Rule of Law but actually undermine it. The specific case of the fight against radicalisation provides a concrete example of the possible difficulties democratic systems may face. This article shows that many democratic systems tend to maximise their repressive action and rely on the notion of presumption of dangerousness rather than that of innocence. To this end, the strategies and instruments used, and the principles they rely on, will be analysed in the light of the constraints democracies should respect. It concludes that the essential peril liberal democracies face comes from the lack of appropriate and effective democratic safeguards that would counterbalance the critical extension of the scope of police prerogatives.

Keywords: Democracy – terrorism – radicalisation – rule of law.

*Aurélie Garbay is a Ph.D. student and teaching assistant in Public Law at the University of Pau and Pays de l'Adour, France. Email: aurelie.garbay@univ-pau.fr

Introduction

Developing strategies to fight terrorism is an essential condition for democracies to survive. In this sense, countering terrorism at its very roots, by focusing on radicalisation, appears to democracies as an effective preventive approach in order to protect their integrity, their values and their citizens.

In the collective imagination, notably since 9/11 and the "war on terror", radicalisation and violent extremism were mostly understood as linked to Jihadism and the recent *Charlie Hebdo* events in Paris or the attacks in Copenhagen tend to confirm this trend. However, radicalisation must be considered as a multifaceted phenomenon. It embraces various ideologies—such as separatism, racism, religious, and political[1]—and behaves as groups or *lone wolves*—as shown by the Breivik case (Berntzen and Sandberg, 2014). It is also multi-located (House of Commons, 2012): individuals can be radicalised at home notably due to the Internet (Europol, 2013, 2014), in prison

(Briggs and Birdwell, 2009; Marret, 2009), or abroad, and, once they turn to terrorism, they can perpetrate their acts on home territory as well as in a foreign State (EU Commission, COM (2013) 941, 2014). The recent scientific studies dedicated to the question of radicalisation also highlight the fact that this phenomenon is not an “abnormal process”: any individual is likely to radicalise, and terrorism and violent extremism should be considered as a particular consequence, a specific manifestation of this process of idea shaping that would have gone “awry”, towards the support to violence (SAFIRE, 2013: 14).

Considering the great variety of facets of radicalisation, rather than a caseby-case or a single-ideology-focused analysis, this article will discuss how legal and police developments in counter-terrorist strategies can have an impact on liberal democracy. Firstly, the notion of radicalism and the legal framework set up to tackle terrorism and radicalism will be defined. Secondly, we will discuss the relationship between developing counter-terrorism strategies and safeguarding human rights. Indeed, while fighting radicalisation and terrorism, liberal democracies must address the issue of conciliating opposing objectives: the right to security on the one hand, and individual rights and freedoms on the other. They bind themselves to their protection by their constitutional enshrinement[1]. Hence, to be qualified a democratic system that applies the Rule of Law[3], the strategies they implement must comply with their constitutional framework (Kelsen, 1999) and with their international constraints (Kelsen, 1952). For instance, for States parties to the European Convention on Human Rights (ECHR), the arsenal set up must also comply with the ECHR standards and their interpretation by the European Court of Human Rights (ECtHR) (Sudre, 1990).

However, the study of the fight against terrorism, and more specifically against terrorist radicalisation, reveals that systems tend to maximise their repressive action towards the exceptional nature of this threat[4], with two outcomes. On the one hand, democratic systems have adapted their apparatus to meet its specificities, while ensuring that the new equilibrium respects the democratic framework, and the Rule of Law. On the other hand, systems develop instruments in breach of their constitutional or international constraints, which leads to a severe alteration of the democratic framework when the principles harmed are considered as constitutive of its very essence. Focusing on liberal democracy thus offers an opportunity to analyse how systems that should respect the Rule of Law are tempted to transgress it in the name of democracy.

Radicalisation: a distinctive phenomenon requiring a specific approach

The concept of “violent radicalisation” appeared for the first time in the official EU doctrine in 2005, 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” (EU Commission, COM(2005)313, 2005: 2). In itself, this definition reveals the fundamental specificity of radicalisation: it is not an 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 (TTSRL, 2008 a). Thus, its apprehension by traditional legal mechanisms, more precisely a specific incrimination, appears to be compromised. However, as inaction facing this phenomenon and its consequences seem unacceptable, States and multilateral systems have developed counter-radicalisation mechanisms, mostly based on intelligence gathering.

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 for 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 and the difficulty to determine what is radical on the other.

Radicalisation must be understood together with the personal reception of a context or a message, thus with individuals' subjectivity. More precisely, depending on personal perceptions, the 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 the contents that should be considered objectionable and thus, criminal, as is the case, for instance, of child pornography—which is under an "explicit content seal", as the elements concerned can objectively be identified as criminal materials (EU Parliament and Council (2011), directive 2011/92/EU[1]).

However, such an approach would collide with the inner subjectivity of the reception of the message. Indeed, some factors may contribute to enhancing the process of radicalisation, such as misinterpretations of writing or ideologies, or the psychological weakness of an individual who feels rejected or discriminated, and who finds answers in extremist ideas (EU Commission, COM(2005)313, 2005; European Commission's expert group on violent radicalisation, 2008; TTSRL 2008b). For instance, a 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 recipients' political ideas, social situation—e.g., employment status—or living condition—e.g., real or perceived insecurity in the neighbourhood (Rydgren, 2008). 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 action against foreigners, for instance global anti-immigrants demonstrations such as the events organised in the Czech Republic, or targeted attacks on foreigners or asylum seekers' accommodation (Europol, 2014). 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 (EU Parliament, 2014; SAFIRE, 2013).

Regarding the expression of radical ideas, 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 or public safety, for the prevention of disorder or crime". This provision consequently allows States to adopt norms limiting freedom of expression when the exercise of this right would be prejudicial to public order (ECtHR, *Handyside v. The United Kingdom*, 1976[1]). Nonetheless, in order to comply with the principle *nulla poena, nullum crimen sine lege*, a law incriminating radicalisation would require defining with sufficient precision what "radical" means (ECtHR, *Sunday Times v. The United Kingdom*, 1979[2]). This issue is a major difficulty regarding the incrimination of this phenomenon. Indeed, it relates to the possibility of determining whether opinions are criminal even when they do not explicitly praise or call for violence. The approach, in which the State is not neutral regarding its citizens' considerations (Rawls, 1971), creates risks of enhanced, real and perceived stigmatisation and discrimination (Sorell, 2009). Criminalising ideas that may pose a certain risk without explicitly calling for violence makes fighting radicalization very difficult (Kant in Ashton's translation, 1974: 58).

Although in the current state of law in the European Union, the establishment of an incrimination linked 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, Article 5-1 of the 2005 Council of Europe Convention on the prevention of terrorism[3] 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 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"[4][5]. The explanatory report of the Convention presents however details regarding how to address this offence. In particular, the 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" (Council of Europe Convention on the Prevention of Terrorism, Explanatory Report: 99). 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 (Council of Europe Convention on the Prevention of Terrorism, Explanatory Report: 98; ECtHR, *Leroy v. France*, 2008[1]). To be constitutive of an offence, a second criterion must be met: "the significance and credible nature of the danger" of perpetration of a terrorist act (Council of Europe Convention on the prevention of terrorism, explanatory report: 100). This definition, well detailed and approved as a best practice by the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2006: 28), 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 importance for democratic systems seeking to develop strategies to protect themselves from terrorism.

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 radicalisation by *Euskadi Ta Askatasuna* (ETA) in prisons, the penitentiary administrations not only applied confinement to ETA prisoners, but also "disperse[d]" them, avoiding their gathering in a same prison or their detention near their home place (UNGA-HRC, 2013). Thus, the lack of a specific incrimination does not prevent systems from fighting radicalisation.

Besides this specific example, most actions consist in surveillance measures (De Koster, 2005), and lay mainly in the hands of the intelligence services[2]. 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 that prevent the terrorist threat at an early stage. Among their traditional instruments, intelligence services use sound and recording systems, as well as computer data collected 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 equipment. Such methods may consequently damage fundamental rights, notably the right to privacy (Mitsilegas, 2015). However, this right is not established as absolute: under exceptional circumstances, such as terrorism, the preservation of public order justifies restrictions to the right to privacy and thus, the use of these methods, as long as the related provisions regarding such interferences are clear and precise enough (ECtHR, *Klass and others v. Germany*, 1978[1]; ECtHR, *Vetter v. France*, 2005[2]).

EU member States may also use discreet surveillance mechanisms provided for by Article 36 of the decision 2007/533/JHA, and conduct discreet checks[3]. These provisions allow the police and/or judicial authorities—depending on each national approach—to integrate alerts in the Schengen Information System (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 that 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 interest 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)[4]. 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. This mechanism offers many possibilities regarding the surveillance of radical individuals. However, it raises questions regarding the preservation of fundamental rights that firstly relate to privacy and data protection, and secondly, to the risk of an extensive interpretation of the provisions by law enforcement and military forces. As there are no guidelines on what should be understood as a sign of risk in the "overall assessment of a person", such alerts are integrated in the SIS depending on each State's interpretation of these provisions (Türk and Piazza, 2009). Moreover, this mechanism lacks judicial or parliamentary monitoring that, when set up, may counterbalance the extensive police prerogatives in a more complete application of the principle of separation of powers than the monitoring operated by the European Agency for the operational management of large-scale IT systems[1]. For instance, in several Member States, such as France or Spain, police authorities can directly issue these alerts without any warrant delivered by a judge. The implementation of adequate safeguards appears thus necessary in order to avoid "backlash effects", for instance appeals before the Courts that may rule against the State authorities' methods and invalidate the results of long investigations.

If they remain of great use for the intelligence services, new forms of online surveillance measures have to complement field surveillance methods 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 (Ashour, 2010; Europol, 2014). 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 (Council of the EU[2], 2005: 9). 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, pursuits and banning procedures appear to be complex as such actions would interfere with the preservation of freedom of expression. Nonetheless, States tend to turn this situation to their advantage by monitoring suspicious websites, and forums and their visitors. In cases of deeper suspicion, overlaps are processed in order to check if journeys were made or trips booked to sensitive destinations with specific data systems, for example with the Advance Passenger Information System (APIS). Such methods are for instance used by the French intelligence services to detect potential threats, although it has not prevented either Mohammed Merah from committing several terrorist attacks in 2012 (Borredon, 2012; Borredon and Cazi, 2012; Bordenave et al., 2013), nor Saïd and Chérif Kouachi and Ahmed Coulibaly from killing seventeen people in January 2015 (Delahousse, 2015). Such mechanisms also raise the question of the limited number of agents dedicated to the processing of online surveillance and the very high number of people under surveillance. It is thus impossible to watch all of them at once. For example, after the *Charlie Hebdo* attack, the French Homeland Security Ministry gave the figure of 3,000 people in France who were under surveillance measures. But, taking into account the failures of the French mechanisms (Follorou et al., 2015), one of the first announcements made after the events in Paris was a massive hire plan, including 1,100 agents to the intelligence services.

These intrusive methods surely offer a way to address the lack of existence of a specific crime. Nonetheless, it must be said that these measures only target individuals who have not yet committed an illegal act, and who may never do so. Thus, the legal basis of surveillance instruments, in other words, the “presumption of a potential threat”, seems to announce an evolution in the understanding of major democratic principles.

Fighting radicalisation: the democratic framework at stake

In 2008, the ECtHR stated that fighting fire with fire would be counter-productive because, according to Judge Myjer, 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” (ECtHR, *Saadi v. Italy*[1]*,* 2008: concurring opinion). 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 has led systems to extend the scope of police prerogatives, sometimes without simultaneously extending the related safeguards, which may result in undermining the democratic quality of the systems these measures were supposed to protect.

Redefining key democratic principles: a perilous tendency

Fighting terrorism, as previously outlined, leads to restrictions and interferences in the preservation and exercise of fundamental human 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 ECHR and the ECtHR. They need to be prescribed by law, pursue a legitimate aim and be necessary in a democratic society. Nonetheless, some fundamental rights are established as inviolable rules because they are considered the key principles structuring the democratic framework. Among them, the principle of presumption of innocence, which is regarded as a democratic standard (Besse et al., 2012) or as a democratic principle (Guinchard and

Montagnier, 2003), 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 yet found guilty by a court (ECtHR, *M.K. v. France*, 2013[1]). Its scope involves the penal proceedings, including for terrorist activities (Committee of Ministers of the Council of Europe, 2002). However, one of the specificities of the fight against radicalisation relates to the fact that this fight is led outside this scope, in a "para penal" dimension (GiudicelliDelage, 2010), where the notion of presumption of innocence faces the notion of dangerousness. Indeed, terrorism is an unpredictable threat and its consequences may be disastrous. States fight against this phenomenon by investigating 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 the notion of risk (Beck, 1992; Ericson and Haggerty, 1997), on its unpredictability, and apply the precautionary principle (Ericson, 2007). Derived from environmental law[2], the latter is to be considered as a principle for guiding public policies. Accordingly, although there is no certainty that a threat will materialise, State authorities should take reasonable preventive measures to ensure security (Guinchard and Montagnier, 2003). Applied to the fight against terrorism, States assume dangerousness and set up early detection and surveillance measures (such as the mechanisms analysed *supra*). These measures seek to anticipate the threat, detect it as early as possible—if manageable, before the adherence to radical and violent ideas[3]—as prescribed as an objective by the EU counter radicalisation strategy (EU Commission, COM(2010)386, 2010). 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 example, the provisions of Article 1 of the Agreement of 10 January

2008 evokes "individuals likely to support or to perpetrate terrorist acts"[4]; 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 an individual's "possible future culpability", although s/he has not yet committed the *culpa*.

These measures may create a form of rejection when an individual realises that her/his personal data is used for surveillance purpose by State authorities, as shown by the demonstration of 10,000 people in Berlin on 12 September 2009 who asked for greater protection of their personal data but also for the respect of their fundamental human rights (Euronews, 2009). They may also create a feeling of stigmatisation, notably when the individual is found not guilty but his data, collected for the purpose of investigation, is stored after the end of the criminal proceedings. The UK Government's argument justifying such a measure in the *Marper* case reflects this redeployment of the presumption, from the notion of innocence to the notion of dangerousness. Indeed, the United 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" (ECtHR, *S. and Marper v. The United Kingdom*[1], 2008: §94). 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 entitled to the presumption of innocence, are treated in the same way as convicted persons" (ECtHR, *S. and Marper v. The United Kingdom*, 2008: §122; Bellanova and De Hert, 2009). It should also be noted that this case was not related to terrorism, but to attempted robbery and harassment. Taking into account the intensity the threat terrorism represents for States, it would be legitimate to consider that, to counter terrorism, a similar rationale would prevail in order to extend the ordinary rules and retain such data for a longer period.

The redeployment of the notion of presumption aims at fighting terrorism efficiently, by striking the threat at its roots, in order to achieve an ultimate objective: preserve the democratic framework. This conception tends to be extended from discreet surveillance to legal prosecutions (Lowe, 2014). The presumption of dangerousness is indeed particularly present in proactive measures, such as the French "*association de malfaiteurs en relation avec une entreprise terroriste*"[2] that the former director of the French intelligence services qualified as "preventive legal neutralisation" (Bousquet de Florian, 2005).

Established as a terrorist offence under the French Penal Code, this sophisticated repressive legal regime allows the arrest of individuals in order to dismantle radical groups "before the perpetration or attempted commission of an attack" (French Senate, 2005). Although this "dragnet" strategy includes the intent criteria—in the sense that the participants are considered to know that their contribution would help the perpetration of a terrorist attack—, it is used at a stage when the individual has not yet committed the *culpa*, but rather one or more (suspicious, although undefined by the penal Code) material act(s). Interestingly, while this mechanism explains the majority of the French convictions for terrorism (Bigo *et al*., 2008), a high number of persons concerned—questioned in custody or even held in pre-trial detention—are dismissed during the investigations or found innocent by the Court (Bonelli, 2008). Nonetheless, notably when placed in pre-trial detention, they face the same conditions as convicted criminals, which is precisely the element the ECtHR argued against in the *Marper* case. This tendency may consequently indicate a drift that may endanger the framework these measures were supposed to protect (Ashworth and Zedner, 2014).

Maintaining democratic systems in the democratic framework: a real challenge

The objective of a fighting terrorism, regardless of the stage—from early detection to detention—, is to protect itself, to ensure its continuity and to safeguard its foundations. For a system that claims to comply with the Rule of Law, it implies the respect of an essential principle, that of always acting within the constraints of the Law (Delmas-Marty, 2010). However, facing terrorism, States and multilateral organisations tend to challenge the boundaries of security at the expense of respecting

other norms they are committed to. The fight against radicalisation provides an eloquent example for this drift towards a more repressive approach, notably at the pre-attack stage, raising the fundamental question of the risk that this approach produces: initially intended to protect democratic systems from an extraordinary threat, it may lead to sink them.

A year after the 9/11 attacks, W. Schwimmer, Secretary General of the Council of Europe, expressed such concerns about having a balanced approach between the preservation of security and the respect of Human rights. According to M. Schwimmer, “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 […] 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” (Council of Europe, 2002: Preface). Following this rationale, safeguards but also monitoring mechanisms should be set up in order to ensure that the measures used do not exceed the democratic constraints (Council of Europe, 2005). To this end, the judge may play a crucial role (Barak, 2008), and counterbalance interferences to fundamental rights and freedoms conducted on the basis of a presumption of dangerousness and uncertain elements (Donini, 2009). However, regarding the fight against radicalisation, the judiciary power seems to be left out of this *para* penal dimension, which raises concerns relating to the existence of a fair balance of powers, a key element in order to strengthen the supremacy of the Rule of Law (Venice Commission, CDL-AD (2007)016, 2007; Council of Europe, 2009). For instance, although the alerts registered in the SIS on the basis of Article 36 of the Decision 2007/533/JHA appear to be of great importance in order to proactively counter radicalisation and terrorism, their registration shows a lack of monitoring by the judge. Indeed, there is neither *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)[1]. But for 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 “offering the best guarantees of independence, impartiality and a proper procedure”, which, nonetheless, may suitably be substituted by an independent control from a Parliamentary board (ECtHR, *Klass and others v. Germany*, 1978: §56). The French-Spanish permanent intelligence teams (Vuelta Simon and MaurelOllivier, 2012), established under the Agreement of 10 January 2008[26], provide an illustration of possible forms of appropriate monitoring. If the provisions of the Agreement do not detail how the activities of these teams should be monitored, it should nevertheless be specified that they actually use traditional intelligence gathering methods, provided for in French and Spanish Law: telephone tapping, sound recording, electronic and non-electronic correspondences, including flows of objects, goods and products. These methods are subject to a dual form of control. On the one hand, both the French *Code de Procédure pénale* and the Spanish *Ley de enjuiciamiento Criminal* impose an *ex ante* authorisation by the judge[2]. On the other hand, both national regimes impose a parliamentary monitoring of the intelligence services. This second form of (less direct) control is ensured by several parliamentary committees, which are each specialised in a particular area. 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 May 1995.

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 (De Schutter, 1997). In the *Gillan and Quinton* case, the ECtHR considered that the powers to “stop and search”, provided for under Section 44 of the UK Terrorism Act 2000[1], was excessively wide, insufficiently precise, and overly based on arbitrariness, 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” (ECtHR, *Gillan and Quinton v. The United Kingdom*[2], 2010: 79). This case is of major interest in the sense that not only the UK Government had to remedy the damage, but it also had to revise its legislation. In 2012, the Protection of Freedoms Act repealed the stop and search powers and replaced them with a new mechanism, taking into account the criticisms of the ECtHR, and claiming that “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”

(Government of the UK, 2012).

Conclusions

If mechanisms to fight radicalisation are necessary in order to protect the integrity of democratic systems, they should, however, be “handled with care”. The 2000s and 2010s have witnessed the development of reflexions regarding the fight against terrorism and related phenomena, more particularly radicalisation, that seem to grant less and less importance to checks and balances (Wright and Kreissi, 2015). This is to the detriment of a conciliated approach in the protection of both security and individual rights and freedoms. Hence, uncontrolled drifts may lead to abuses and, eventually, to a situation in which attempts to the Rule of Law, frequently occurring in the fight against terrorism, including in States parties to the ECHR, could affect other areas. Presented as justified by their—real or apparent—efficiency, such abuses would thus “infect” the system. Eventually, the Rule of Law, already undermined in counterterrorism, would also be at stake by the deployment of similar counter criminality strategies in other areas.

This situation appears as even more worrying because some States that have traditionally been opposed to such approaches are now experiencing these symptomatic drifts. Indeed, in March 2015, the French Government initiated proceedings in order to pass a legal reform on surveillance

activities. Terrorism and the fight against related phenomena are a key motive, but the project also aims at “the prevention of organised crime and the prevention of collective forms of violence that may seriously prejudice public peace” (Projet de Loi n°2669, 2015). If adopted, the new regime would legalise practices currently used by the intelligence services, but that are at the moment prohibited because they do not offer sufficient safeguards[1]. However, the major problem with this reform relates to the fact that it fails to introduce proper safeguards, in particular the judiciary’s *ex ante* authorisation, thus controverting the Council of Europe’s recommendations regarding the principles of proportionality, suitability, and necessity (Council of Europe, 2005: a3). The French project is the clear illustration of a potential shift in the approach of the fight for the protection of public security, to the detriment of other constitutional— and international—constraints, among them, the protection of individual rights and freedoms notably ensured by a “mutual distrust” between State powers (Miranda, 2015). For democratic systems, they are not only a legal question but also a philosophical constraint (Fleury, 2009). There would be an absolute dichotomy in that they claim to be protecting democratic values on one side, and adopting a behaviour going against these same values on the other. Thus, although the efficiency argument reinforces the lure to transgress the Rule of Law, democratic systems must remember that they will ensure the durability of their democratic essence only on condition that security strategies are developed in accordance with cornerstone civil rights and liberties.

References

Ashour O (2010), Online de-radicalization? Countering violent extremist narratives:

message, Messenger and Media strategy. *Perspectives on Terrorism*, vol. 4-6: 15-19.

Ashworth A and Zedner L (2014), *Preventive Justice*, Oxford: Oxford University Press.

Bousquet de Florian P (2015), Le jihadiste français est plus fruste, plus jeune, plus radicalisé. *Réseau Voltaire Inernational*, June, 5. Retrived from:

http://www.voltairenet.org/article17151.html (accessed 4 March 2015).

Barak A (2008), *The judge in a Democracy*, Princeton: Princeton University Press.

Beck U (1992), *Risk society: towards a new modernity*, London: Sage Publications.

Bellanova R, De Hert P, Le cas S. et Marper et les données personnelles: l’horloge de la stigmatisation stoppée par un arrêt européen. *Cultures & Conflits* 76(4):101114.

Berntzen L E and Sandberg S (2014), The collective nature of lone wolf terrorism:

Anders Behring Breivik and the anti-Islamic social movement. *Terrorism and Political Violence* 26(5): 759-779

Besse M, Garcia M and Sanchez Perez L (2012), *Délits de presse et Démocratie*, Paris: Fondation Varenne.

Bigo D, Bonelli L and Deltombe T (2008), *Au nom du 11 septembre... Les démocraties à l'épreuve de l'antiterrorisme*, Paris: La Découverte "Cahiers libres".

Bonelli L (2008) Les caractéristiques de l'antiterrorisme français: "Parer les coups plutôt que de panser les plaies". *Le Monde*, September, 11. Retrieved from: http://www.lemonde.fr/societe/article /2008/09/11/les-caracteristiques-del-antiterrorisme-francais-parer-les-coups-plutot-que-panser-lesplaies_1093469_3224.html (accessed 4 March 2015)

Bordenave Y and Borredon L (2013), Un an après Merah, le nouvel âge de l'antiterrorisme. *Le Monde*, March, 16. Retrieved from:

http://abonnes.lemonde.fr/societe/article/2013/03/16/un-an-apres-merahle-nouvel-age-de-l-antiterrorisme_1849398_3224.html (accessed 4 March 2015)

Borredon L and Cazi E (2012) Merah: l'incroyable raté des services secrets. *Le Monde*, October, 19. Retrieved from: http://www.lemonde.fr/societe/article/2012/10/19/merah-l-incroyable-ratedes-services-secrets_1777963_3224.html (accessed 4 March 2015)

Borredon L (2012), De Toulouse à Sarcelles, les méthodes de la DCRI mises à mal.

Le Monde, October, 19r. Retrieved from:

http://www.lemonde.fr/societe/article/2012/10/19/de-toulouse-a-sarcellesles-methodes-de-la-dcri-mises-a-mal_1777972_3224.html (accessed 4 March 2015)

Bottoms A E and Brownsword R (1983), Dangerousness and rights. In Hinton J (ed.), *Dangerousness: Problems of assessment and prediction*, London: Allen and Unwin.

Briggs R and Birdwell J (2009), *Radicalisation among Muslims in the UK*, MICROCON Policy Working Paper 7, Brighton: MICROCON.

Cazeneuve B (2014), Communication to the Council of Ministers "Le plan de lutte contre la radicalisation violente et les filières terroristes", meeting of 23 April

2014. Retrieved from.http://www.gouvernement.fr/conseil-desministres/2014-04-23/le-plan-de-lutte-contre-la-radicalisation-violente-etles-fi (accessed on 27 May 2015).

Compagnie Européenne d'Intelligence et de Sécurité (2008), *Les facteurs de création ou de modification des processus de radicalisation violente, chez les jeunes en particulier.*

Study for the EU commission – Directorate-General for Justice, Freedom and Security. Retrieved from http://ec.europa.eu/dgs/home-affairs/elibrary/docs/pdf/ec_radicalisation_study_on_trigger_factors_fr.pdf (assessed on 27 May 2015).

Coolsaet R (2008) *Jihadi Terrorism and the Radicalisation Challenge in Europe*, 2nd ed., Surrey: Ashgate.

Coolsaet R (2010) EU counterterrorism strategy: value added or chimera? *International affairs* 86(4): 857-873.

Council of Europe (2002) Committee of Ministers, *Guidelines on human rights and the fight against terrorism*, 804th meeting. Retrieved from http://www.coe.int/t/dlapil/cahdi/Source/Docs2002/H_2002_4E.pdf (accessed on 27 May 2015).

Council of Europe (2005) Committee of Ministers, *Recommendation on "special investigation techniques" in relation to serious crimes including acts of terrorism*, Rec(2005)10. Retrieved from http://wcd.coe.int/ViewDoc.jsp?id=849269 (accessed on 27 May 2015).

Council of Europe (2009), *Armed forces and security services: what democratic controls*, Strasbourg: Council of Europe Publishing editions.

Crelinsten RD (1987), Terrorism as political communication: the relationship between the controller and the controlled. In Wilkinson P and Stewart A M (eds.) *Contemporary research on Terrorism*, Aberdeen: Aberdeen University Press.

De Koster P (2005) *Terrorism: special investigation techniques*, Strasbourg: Council of Europe publishing.

De Schutter O (1997) La cooperation entre la Cour européenne des Droits de l'Homme et le juge national. *Revue belge de droit international* 1: 21-68.

Delahousse M (2015) "Charlie Hebdo": la surveillance des frères Kouachi s'était arrêtée il y a six mois. *Le Monde*, January, 11. Retrived from:

http://tempsreel.nouvelobs.com/charlie-hebdo/20150110.OBS9696/charliehebdo-la-surveillance-des-freres-kouachi-s-etait-arretee-il-y-a-six-mois.html (accessed 4 March 2015)

Delmas-Marty M (2010) *Libertés et sûreté dans un monde dangereux*, Paris: Seuil.

Donini M (2009) Les droits fondamentaux et la juridiction pénale comme garantie contre ou comme justification pour l'usage du droit comme une arme? *Revue de Science Criminelle* 1: 31-42.

Ericson RV (2007) *Crime in an insecure world*, Cambridge: Polity Press Ericson RV and Haggerty K (1997) *Policing the risk society*, Oxford: Clarendon EU Commission (2005) Communication from the Commission to the European Parliament, COM (2005) 313 final. Retrieved from http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0313:FIN:EN:PD F (accessed on 27 May 2015).

EU Commission (2010) Communication to the Parliament and the Council, *The EU Counter-Terrorism Policy: main achievements and future challenges*, COM (2010) 386 final. Retrieved from http://ec.europa.eu/dgs/home-affairs/what-isnew/news/pdf/com_2010_386_en.pdf (accessed on 27 May 2015).

EU Commission (2014) Communication from the Commission to the European Parliament, The Council, the European economic and social committee and the committee of the regions, *Preventing radicalisation to terrorism and violent extremism: strengthening the EU's response*, COM (2013) 941 final. Retrieved from http://ec.europa.eu/dgs/home-affairs/elibrary/documents/policies/crisis-andterrorism/radicalisation/docs/communication_on_preventing_radicalisation_and_violence_promoting_extremism_201301_en.pdf (accessed on 27 May 2015).

European Commission's expert group on violent radicalisation (2008) *Radicalisation processes leading to acts of terrorism*. Retrieved from http://www.rikcoolsaet.be/files/art_ip_wz/Expert%20Group%20Report%20Violent%20Radicalisation%20FINAL.pdf (accessed on 27 May 2015).

EU Parliament (2014) Directorate General for internal policies, Policy Department C: Citizens' rights and constitutional affairs, *Preventing and countering youth radicalisation in the EU*, study for the LIBE Committee, PE 509.977. Retrieved from

http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509977/ IPOL-LIBE_ET%282014%29509977_EN.pdf (accessed on 27 May 2015).

Euronews (2009) Data protection march in Berlin. September, 13. Retrieved from http://www.euronews.com/2009/09/13/data-protection-march-in-berlin/ (accessed 4 March 2015).

Europol (2013) *EU terrorism situation and trend report TE-SAT*, The Hague: Europol.

Europol (2014) *EU terrorism situation and trend report TE-SAT*, The Hague: Europol.

Fleury C (2009) *Les pathologies de la démocratie*, Saint-Amand-Montrond: Livre de poche.

French Senate (2004) Reply from the Justice Ministry, published in the Official Journal of the Senate, 17 February 2005, to the written question n° 13584 from Senator Jean-Louis Masson, published in the Official Journal of the Senate.

Follorou J et al (2015), Les ratés à repetition du renseignement français. *Le Monde*, January, 12. Retrived from:

http://abonnes.lemonde.fr/societe/article/2015/01/12/les-rates-arepetition-du-renseignement-francais_4554311_3224.html (accessed 4 March 2015).

Garland D (2001), *The culture of control: crime and social order in contemporary society*, Oxford: Oxford University Press.

Giudicelli-Delage G (2010) Droit pénal de la dangerosité – droit pénal de l'ennemi. *Revue de Science Criminelle* 1: 69-80.

Government of the United Kingdom's (2015) "Protecting the UK against terrorism", Retrieved from: http://www.gov.uk/government/policies/protecting-the-ukagainst-terrorism (accessed on 4 March 2015)

Guinchard S and Montagnier G (2003) *Lexique des termes juridiques*, 14th ed., Paris: Dalloz.

Hudson B and Ugelvik S (2012), *Justice and security in the 21st century – Risks, rights and the rule of law*, Oxon: Routledge.

House of Commons (2012) Home Affairs Committee, *Roots of violent radicalisation*, 19th report of session 2010-2012, vol. 1.

Kant I – Ashton E B (translation 1974), *On the old saw – That may be right in theory but it won't work in practice*, Philadelphia: University of Philadelphia Press.

Kelsen H (1952), *Principles of International Law*, New York: Reinhart.

Kelsen H (1999), *Théorie pure du droit*, Paris: L.G.D.J.

Koering-Joulin R et al. (1998) *La Présomption d'innocence en droit compare*, symposium organised by the Centre français de droit comparé at the Cour de Cassation on 16 January 1998, Paris: Société de législation comparée.

Kuty F (2006),*Justice pénale et procès équitable – Exigence de délai raisonnable – Présomption d'innocence – Droits spécifiques du prévenu*, vol. 2, Paris: Larcier.

Lowe D (2014) Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty, *Terrorism and Political Violence*, printed online.

Marret J L (2009) *Prison de-radicalization and disengagement: the French case*, ICSR Project on de-radicalisation in jail, Fondation pour la Recherche Stratégique.

Miranda M (2015) Estado de la cuestión desde la perspectiva de la investigación judicial, in: Consejo General de la Abogacía Española, *30° aniversario de la Convención de Naciones Unidas contra la tortura – Retos y desafíos en España*, Madrid.

Mitsilegas V (2015) The transformation of privacy in an era of pre-emptive surveillance. *Tilburg Law Review* 20(1): 35-57.

Pisoiu D (2013) Coming to believe «Truths» about islamist radicalization in Europe.

Terrorism and Political Violence 25(2): 246-263 Projet de Loi n°2669 (2015) Relatif au renseignement, registered at the National Assembly on 19 March 2015.

Rydgren J (2008) Immigration sceptics, xenophobes or racists? Radical right-wing voting in six West European countries. *European Journal of Political Research* 47 (6): 737-765.

SAFIRE – Scientific Approach to Formulate Indicators and Responses to Radicalisation (2013) *From radicalisation analysis to deradicalisation: policy and field recommendations*, deliverable 6.1.

Sandel M J (2010) *Justice: what is the right thing to do?* London: Penguin.

Silke A (2014) *Prisons, terrorism and extremism – Critical issues in managemet, radicalisation and reform*, Oxon: Routledge.

Sorell T (2009) *Moral risks of preventive policing in counter-terrorism*, DETECTER – Detection Technologies, Terrorism, Ethics and Human Rights, deliverable 25.

Sudre F (1990) *La Convention européenne des droits de l'homme*, Paris: Presses Universitaires de France.

Thomsen MH (2012) *"Deradicalisation – targeted intervention" - Brief summary of Danish pilot experience with deradicalisation and prevention of extremism*, June.

Treschel S (2005) *Human Rights in Criminal Proceedings*, Oxford: Oxford University press.

TTSRL-Transnational Terrorism, Security, and the Rule of Law (2008 a), *The EU*

Counterradicalization strategy – Evaluating EU policies concerning causes of radicalization, Workpackage 4, objective 6.

TTSRL-Transnational Terrorism, Security, and the Rule of Law (2008 b), *Radicalisation, recruitment and the EU Counter-radicalisation strategy*, Workpackage 4, delivrable 7.

Türk A and Piazza P (2009) La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée. *Cultures & Conflits* 76(4): 115134.

United Nations General Assembly (2006) *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.

UNGA-HRC – United Nations General Assembly – Human Rights Council (2013), Written statement submitted by the Europe-Third World Centre / CETIM, *Violation of Basque political prisoners' human rights*, n°A/HRC/22/NGO/109. Retrieved from A/HCR/22/NGO/109 (accessed on 27 May 2015).

UNSC – United Nations Security Council (2013) Report of the Secretary General, *The rule of law and transitional justice in conflict and post-conflict societies*, n° S/2004/616.

Venice Commission (2007) *Report on the Democratic oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session*, CDL-AD (2007)016.

Von Behr I, Reding A, Edwards C, and Gribbon L (2013) *Radicalisation in the digital era – the use of the Internet in 15 cases of terrorism and extremism*, Santa Monica, RAND. Retrieved from

http://www.rand.org/pubs/research_reports/RR453.html (accessed on 27 may 2015).

Vuelta Simon S and Maurel-Ollivier A (2012) *La justice française contre ETA*, Paris: Presses Universitaires de France.

Wright D and Kreissi R (eds 2015), *Surveillance in Europe*, Oxon: Routledge.

Zedner L (2009) *Security.* Oxon: Routledge.