COMMISSIONER FOR HUMAN RIGHTS

COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 5 June 2015 CommDH/PositionPaper(2015)1

COMMISSIONER FOR HUMAN RIGHTS

POSITIONS ON COUNTER-TERRORISM AND HUMAN RIGHTS PROTECTION*

* This is a collection of positions on human rights during counter-terrorism efforts from the Council of Europe Commissioner for Human Rights. It is a short summary of the Commissioner's positions, conclusions and recommendations concerning counterterrorism and human rights protection based primarily on his country-monitoring and thematic documents. See also the Commissioner's thematic webpage on counter-terrorism and human rights protection at:
http://www.coe.int/en/web/commissioner/thematic-work/counter-terrorism

Introduction

Terrorist activity has been a real and present threat, as well as a fundamental violation of human rights. However, state attempts to combat it must be human rights compliant and remain within the rule of law. Policies which respect established human rights norms, notably those flowing from the European Convention on Human Rights ("ECHR") and the case-law of the European Court of Human Right ("ECtHR"), preserve the values the terrorists are trying to destroy, weaken support for radicalisation among potential adherents and strengthen public confidence in the rule of law.

A culture of human rights promotes genuine and lasting security. Conversely, policies which run counter to European democratic values and human rights are not only contradictory to Council of Europe member states' international obligations, but are also counterproductive and contribute to the spread of extremism.

In the wake of the 2001 September 11th attacks, the US-led "war on terror" and many European states' counterterrorism efforts violated core principles of human rights and international law, including the following: protection against torture, the right to personal liberty and security, the right to a fair trial including the presumption of innocence, the right to respect for private and family life, the freedoms of expression and of movement, the right to an effective remedy and victims' rights to reparation following states' unlawful acts.

During this period, thousands of individuals, including many European citizens and many innocents, have been victimised. Serious human rights violations were committed in the context of anti-terrorist policies post- 9/11, including recourse to abduction, secret rendition, unlawful detention and interrogations, torture, and the widespread use of ethnic and religious profiling.

The use of illegal methods by democratic states has seriously harmed the international system for human rights protection, and has backfired as a strategy against terrorism.

Hardly anyone in Europe has been punished for their co-operation with the US in violating human rights. This lack of accountability continues to erode the European human rights system, producing a broader democratic backsliding in a number of countries. European governments must be held accountable and admit their share of responsibility for such abuses. They must undertake measures to provide redress for victims, ensure compliance with human rights standards, and prevent the recurrence of human rights violations.

I. Effective human rights protection and non-discrimination are essential to decreasing terrorism

In 2006 the United Nations ("UN") put forward a Global Counter-Terrorism Strategy. One of its major purposes was to stop terrorism at its roots by acting for prevention. The UN strategy listed a number of conditions conducive to the spread of terrorism, namely:

- Prolonged unresolved conflicts
- Discrimination and intolerance
- Xenophobia
- Poverty and economic inequalities
- Social exclusion and high youth unemployment
- Political exclusion
- Human rights deficits and lack of good governance.

Common for these conditions is that they tend to lead to injustices for the individuals and to cause deep frustration and a sense of personal humiliation. Unfortunately, the protection of human rights has been presented as an *obstacle* to effective counter-terrorism work when, in fact, it is essential to preventing and decreasing the incidence of terror around the world.

Along those lines, national security and human rights protection are not mutually exclusive. In European and international human rights law, "national security" is not a card that trumps all other considerations. Indeed, the very question of what legitimately can be said to be covered by the concept of "national security" is justiciable.

II. Legality of counter-terrorism measures

Increasing use has been made of non-criminal, yet effectively punitive, "administrative" measures against identified, suspected "extremists" or new-type "enemies of the state". This robs suspected individuals of fundamental safeguards, both against the specific measures taken against them and, as groups, against such discrimination. It leads to alienation of the groups in question, and thus actually undermines security.
It is a fundamental principle that respect for human rights, fundamental freedoms and the rule or law be upheld in times of tension and crisis – by everyone. Terrorism is a serious threat and counter-terrorism operations are often necessary and justified. Actions must be taken to prevent, pre-empt, prosecute, judge and punish terrorist acts. But all means of action are not justified, not justifiable. There is a compelling duty for the State to protect the general interest of security and rule of law without violating the fundamental rights of the individuals which it has agreed to protect in all circumstances.

Any new anti-terrorist legislation should be elaborated and adopted cautiously and be subjected to thorough, effective human rights proofing. This is even more so in legal texts of a pre-emptive character, such as those which set forth offences of a preparatory nature in relation to terrorist acts. European history has shown that emergency legislation targeting terrorism may easily lead to serious human rights abuses and therefore be counterproductive. When provisions are imprecise and unclear, this can result in an overbroad scope and lead to the criminalisation of acts that are, in fact, far removed from the principal act of terrorism. Anti-terrorist legislation and counter-terrorism measures should never be used to persecute vulnerable or marginalized groups.

III. Absolute prohibition of torture and effective investigation of torture allegations

The prohibition of torture and inhuman or degrading treatment is one of the most fundamental values of democratic society. Under the ECHR, the prohibition of torture allows for no limitations or derogations, not even in the event of a public emergency.

The reintroduction of torture as an interrogation method was a betrayal of the very ideals states are called upon to defend against the forces of extremism and violence. Moreover, such unlawful methods did not provide security agencies with reliable information. Rather, incidents from Guantanamo Bay and Abu Ghraib have strengthened the position of the extremists, including in Europe.

Interrogation under unlawful conditions takes advantage of the detainee's extremely vulnerable situation. The reliance on information provided by foreign intelligence services in court proceedings raises serious questions in regard to the absolute prohibition of using evidence extracted under torture.

The absolute prohibition of torture not only obliges state officials to abstain from torture or any degrading or inhuman treatment but also implies the obligation to provide individuals with adequate protection against such serious human rights violations, to carry out effective investigations and impose dissuasive sanctions on every person responsible.

IV. Accountability for extraordinary rendition and complicity in CIA secret detention

From late 2001 onwards, the US Central Intelligence Agency ("CIA") developed a vast network of clandestine counter-terrorism operations to capture and detain its most wanted suspects, including the unlawful programme of "extraordinary renditions" – involving the abduction, detention and ill-treatment of suspected terrorists. The CIA's partner agencies in various foreign countries – including across Europe – lent their close collaboration. The value of the intelligence produced by this network has been questioned; but one clear result was a pattern of abusive and excessive actions in flagrant violation of human rights**.**

Secret and highly secure detention facilities, so-called "black sites", were established in at least seven different overseas locations, to which the CIA delivered its detainees for "enhanced interrogation". Detention in CIA custody meant being kept indefinitely in secret, incommunicado, solitary confinement.

European government authorities have been deeply complicit in the counter-terrorism strategies pursued by the CIA. They permitted, protected and participated in CIA operations which violated fundamental tenets of our systems of justice and human rights protection. By allowing unlawful detentions and interrogation techniques amounting to torture, European governments caused further suffering and violated human rights law.

At least 25 European countries have co-operated with the CIA. To date, governments have largely been unwilling to establish the truth and ensure accountability for their complicity in these operations. Little justice has been achieved or even initiated, and many countries have yet to fully account for their co-operation including the use of their airspace and airports for suspected rendition flights, capture and transfer of individuals

to U.S. custody and participation in interrogation, as well as knowledge of secret detention and extraordinary rendition operations.

Concealment and cover-ups have been more characteristic responses. In many cases, an abuse of the state secrets privilege has hampered judiciary and parliamentary initiatives to determine responsibility. Though secrecy is sometimes necessary to protect the state, it should never serve as an excuse to conceal serious human rights violations.

The full truth must now be established and guarantees given that such forms of co-operation will never be repeated. Effective investigations are imperative and long overdue. The purported cost to transatlantic relations of pursuing such accountability cannot be compared to the damage inflicted on our European system of human rights protection by allowing ourselves to be kept in the dark.

V. Secret surveillance and the right to respect for private life

While some legislation granting powers of secret surveillance over mail, post and telecommunications is necessary in a democratic society, states do not enjoy unlimited discretion to subject persons within their jurisdiction to secret surveillance.

Secret, massive and indiscriminate surveillance programmes are not in conformity with European human rights law and cannot be justified by the fight against terrorism or other important threats to national security. Such interferences can only be accepted if they are authorized by law, strictly necessary and proportionate to a legitimate aim.

Recent revelations, many of them based on files from the whistle-blower Edward Snowden, have showed the stunning scale and sophistication of the surveillance to which we can all be subjected. The CIA, the NSA, and its British counterpart, GCHQ, target encryption techniques that are used by Internet services such as Google, Facebook and Yahoo, making them vulnerable to surveillance. There is extensive co-operation between different security agencies – but also between such agencies and private companies. All this leaves us open to abuse of our fundamental human right to privacy.

The ECHR, by which all 47 member states of the Council of Europe are bound, guarantees the right to respect for private life (Article 8) and access to an effective remedy to challenge intrusions into one's private life.

Article 8 extends to protecting individuals from the improper collection, storage, sharing and use of data. As the placement of personal data on the Internet, especially social media, increases, so do the risks to individual privacy. Attempts by states to interfere with an individual's right to privacy in the aforementioned ways require legitimate justification by the state – it is not for individuals to have to justify why they are concerned about attacks on their human rights.

VI. Strong data protection regime to prevent data mining, surveillance and retention

Data protection is often seen as an obstacle to effective anti-terrorist measures – and thus is a prime area in which basic international commitments are ignored. Yet data protection is crucial to the upholding of fundamental democratic values.

Surveillance technology is developing with breathtaking speed, including a massive expansion in “dataveillance”: the monitoring of “data trails” left by individuals in numerous transactions, through access to private and public-sector databases.

Nowadays, technologies exist which allow for millions of telephone and e-mail communications to be monitored, screened and analysed simultaneously; for the use of virtually undetectable listening and tracing devices; and for the surreptitious installation of “spyware” on someone’s computer capable of secretly monitoring the online activities and e-mails of the user, and even turning on the computer’s camera and microphone.

States are also creating ever more powerful central databases of their own, with biometrics such as computer-readable facial photographs, fingerprints, DNA, etc. Banks, insurance companies and other businesses also develop databases on clients and their transactions. The storing of enormous amounts of personal data in social security, medical, police, travel, and consumer “lifestyle” databases built by specialised data mining companies, is a matter of serious concern.

Combining these databases and linking them with other databases creates a previously unimaginably detailed picture of our lives and interests, including financial and medical aspects, and cultural, religious and political affiliations. Yet the data protection safeguards against the transferring of information are weak – and further weakened by anti-terrorist legislation.

Police and secret services search through such databases in order to find a “match” against a pre-determined “profile”. The use of such new surveillance methods by the police and security services requires enhanced democratic and judicial control. This is because these technologies suffer from built-in biases which lead to actions against large numbers of innocent people – and, in the anti-terrorist context, often risk discriminating on grounds of race, gender, religion or nationality.

Attempts to identify very rare incidents or targets from a very large data set are mathematically certain to result in either an unacceptably high numbers of “false positives” (identifying innocent people as suspects) or an unacceptably low number of “false negatives” (not identifying real criminals or terrorists). Extensive research has failed to show any significant positive effect on clear-up rates for crime, and especially not for terrorism-related crime, as a result of compulsory data retention.

VII. Freedom of expression and of media

A number of laws and provisions adopted in the general context of combating terrorism restrict freedom of expression. With regards to the criminalization of statements which national courts have judged as inciting violence or encouraging, justifying, or supporting ‘terrorism’, the ECtHR has established a cautious, context-dependent approach which upholds the rights of free expression, especially political speech, and undertakes an in-depth examination of the potential impact of the statement, particularly whether it actually incited violence.

Freedom of the media is one of the prime achievements in a democracy. Restricting freedom of expression under cover of anti-terrorism activities is tantamount to handing victory to the terrorists. It is absolutely vital to enable journalists to carry out their work and to be free to decide what cannot or should not be disseminated. The installation of microphones and geolocation tags, as well as the use of tools allowing interception of communications, are liable in particular to violate the secrecy of correspondence, the

confidentiality of journalistic sources, and the professional secrecy of lawyers and other professions.

VIII. Free and open Internet

The fight against terrorism has seen potential threats to the free flow of online information. Even a number of 'old democracies' have considered or implemented various restrictions, including new ways to block, filter, monitor, and otherwise obstruct or manipulate the openness of the Internet. Some states have proposed making Internet service providers responsible for taking down content that incites to terrorism without any judicial review, a problematic proposition which, along with other filtering measures, could be used to silence undesired voices.

Motivated by national security concerns, some states have developed vast surveillance measures over online communications, invoking the need to combat terrorism to justify the interception of communications.

While certain protective measures are important to ensure that the Internet remains a safe place and not a tool that can be used to perpetrate crimes, the Internet must only be subjected to restrictions that are strictly necessary so as to protect the free flow of information. There should be prior judicial authorization of restrictive measures as well as judicial review; the principle of proportionality must be strictly respected in this endeavour.

IX. Democratic and effective oversight of intelligence and security service activities

Ongoing revelations by former US intelligence contractor Edward Snowden have brought renewed attention to the implications of large-scale electronic surveillance and to inadequacies of the oversight of security services.

Council of Europe member states have taken diverse approaches to structuring and undertaking oversight of their security services. While progress has been made in establishing external oversight of security services, very few countries have gone on to undertake reviews of the efficacy of these systems. And there is no Council of Europe member state whose system of oversight comports with all of the internationally or regionally recognised principles and good practices.

An overarching principle is that all aspects of security service activity, policy, finance, administration and regulation should be subject to scrutiny by at least one institution that is external to and independent from the security services and the executive. This external scrutiny should be *ex ante* (where appropriate), contemporaneous and *ex post*.

Security services provide a public service to and on behalf of the public and therefore elected representatives should be involved in ensuring that this service is provided effectively, efficiently and lawfully. The "democratic" aspect of oversight is primarily achieved through the involvement of parliament, including by: ensuring that national laws provide for comprehensive oversight of security services; allocating the necessary budgetary resources to non-parliamentary oversight institutions; overseeing the work of expert oversight bodies; keeping under review the efficacy of oversight institutions; and conducting both ongoing scrutiny and ad hoc inquiries into security service activity.

Access to classified information by parliamentary oversight committees is an essential feature of effective oversight.

There is growing recognition that human rights and the rule of law are best protected when oversight by parliamentarians is supplemented by expert oversight. Expert oversight bodies are generally better placed to undertake the ongoing, detailed and politically neutral scrutiny that human rights protection requires. This type of oversight is particularly necessary with regards to the scrutiny of security service activities that impact upon the rights to privacy, freedom of expression, assembly and association. Such activities include the collection, use, storage, transfer (including to domestic law-enforcement agencies and foreign bodies) and deletion of personal data.

Most security services have growing capacities to collect, share and receive information and use increasingly complex systems for doing so. Accordingly, recourse to independent technical expertise has become indispensable for effective oversight. Including different types of expertise in the process of authorising intrusive measures may provide stronger safeguards than authorisation by a body that is either political or judicial. An authorization process undoubtedly needs to encompass legal and human rights assessments of proposed measures but it may also be beneficial to address any political risks associated with proposed measures. Accordingly, a two-level authorisation process combining authorisation by a (quasi-)judicial body with that of a minister may offer the most robust model of *ex ante* scrutiny.

It is essential that oversight systems are periodically evaluated to assess whether or not they possess the necessary attributes to be effective. Evaluations may be periodic or ad hoc; it may be effective to include an evaluation requirement in legislation governing oversight bodies.

X. Terrorist black-listing

“Blacklisting” refers to procedures under which the UN or the European Union (“EU”) may order sanctions targeting individuals or entities suspected of having links with terrorism. These sanctions include the freezing of financial assets.

The formal basis for such procedures lies in a Security Council resolution in 2000 which established a list of individuals suspected of having connections with al-Qaeda, Osama bin Laden and the Taliban. The European Union followed suit with its own regulations, taking the view its own action was also essential. Consequently, EU regulations freeze the funds and other economic resources of persons and entities whose names appear on the UN list.

These measures have affected a number of the rights of the targeted individuals, including the right to privacy, the right to property, the right of association, and the right to travel or freedom of movement. There has been no possibility of appeal, or even to know all the reasons for the blacklisting, which means that a person’s right to an effective remedy and to due process have been ignored.

More than a few have been targeted by these measures. The UN Special Rapporteur on human rights and terrorism has expressed his concern at the fact that the listing

regime “has resulted in hundreds of individuals or entities having their assets frozen and other fundamental rights restricted”.[1]

XI. Asylum and expulsion decisions

The norm in dealing with terrorists should be prosecution, not expulsion. Expulsion may be the easy option, but it simply shifts the threat, and does not eliminate it. Accelerated procedures must not deprive individuals of their right to defend themselves properly.

Individuals are often unable to contest asylum and expulsion decisions taken on grounds of national security, to access the information on which such decisions are based, or to appeal against such decisions. It is particularly important in cases where the risk of torture or other forms of ill-treatment is elevated, that proceedings leading to expulsion are surrounded by appropriate legal safeguards, at the very least a hearing before a tribunal and right to appeal.

[1] Statement by Martin Scheinin Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 63rd session of the UN General Assembly Third Committee, 22 October 2008.

Key Recommendations

States should adopt national preventive policies as part of their counter-terrorism efforts. Among these policies figure those that should promote tolerance by encouraging inter-religious and cross-cultural dialogue, involving NGOs, with a view to preventing tensions capable of contributing to the commission of terrorist offences. Such policies should also provide for the effective elimination of discrimination, especially on ethnic or religious grounds, in law and practice, and for everyone's access to inclusive, quality education.

All counter-terrorism measures in Europe should be subjected to thorough, effective human rights proofing. Counter-terrorism measures must be taken in accordance with the law; must pursue a legitimate aim; must be necessary in a democratic society and justified on relevant, objective grounds; and must be supervised or monitored by an independent authority.
With respect to counter-terrorism legislation, the principle of legality (covering the requirements of non-retroactivity and foreseeability as well as precision and clarity of the law) as well as the presumption of innocence should be strictly upheld. The scope of special investigative methods should be narrowly defined.

If a limited range of preventive measures may be justified in the event of a clearly identified danger, it is important that their exceptional nature is made clear. Ordinary criminal prosecution must be the preferred means of tackling terrorist activity and limiting important rights. In the fight against terrorism, the relevant authorities should work in co-operation *with* and not against human rights defenders.

Safeguards against enforced disappearance and protection against torture must be established. Attempts to redefine the very meaning of torture must not be accepted. Evidence obtained under inhuman or degrading treatment or torture should never be admissible in court proceedings. The burden to prove beyond reasonable doubt that evidence has not been obtained under such unlawful conditions should be shifted to the public prosecutor and not rest upon the defendant.

There should be clear guidelines for intelligence services and all law enforcement authorities regarding the interrogation of detainees abroad. Individuals should *never* be detained without due process, denied access to a lawyer, or subjected to inhuman or degrading treatment or torture.

There should be accountability for European complicity in CIA black sites. Independent, public, and effective national investigations should be established whenever there are credible allegations of unlawful renditions or secret detentions. Victims should be granted reparation and the possibility of redress before an independent body, and measures should be taken to ensure that these human rights violations will not recur.

Rigorous procedures should be in place with regard to the examination, use and storage of the data obtained. Those subjected to surveillance or other counter-terrorism measures should be given a chance to exercise their right to an effective remedy in order to contest the validity of the measures applied to them, as well as decisions on the use and storage of data concerning them.

States should establish or designate one or more bodies that are fully independent from the executive and the security services to oversee all aspects of security service regulations, policies, operations, data collection and administration, and ensure that their systems for the oversight of security services comply with human rights requirements.

States should strengthen the link between expert oversight bodies and parliament by giving a designated parliamentary committee a role in the appointment of members, empowering parliament to task expert bodies to investigate particular matters, and requiring that expert oversight bodies report and take part in hearings with a designated parliamentary committee.

Independent *ex ante* authorisation should be extended to: untargeted bulk collection of information; the collection of and access to communications data (including when held by the private sector); and, potentially, computer network exploitation. The process by which intrusive measures are authorised or re-authorised should itself be subject to scrutiny. Given the difficulties that may arise when seeking to evaluate judicial decisions on the authorisation of intrusive measures, consideration may be given to quasi-judicial models.

States should consider the introduction of security-cleared public interest advocates into surveillance authorisation processes, create or designate an independent, external oversight body to receive and investigate complaints relating to all aspects of security service activity, and give an external oversight body the power to quash surveillance measures when such activities are deemed to have been unlawful. Independent, external bodies responsible for scrutinising security services should publish public versions of their periodic and investigation reports.

Exemptions to freedom-of-expression legislation based on national security considerations should be strictly limited. Vague notions such as providing communications support to terrorism or extremism, the ‘glorification’ or ‘promotion’ of terrorism or extremism, and the mere repetition of statements by terrorists, which does not itself constitute incitement, should not be criminalised. Proposals to make Internet service providers responsible for taking down content that incites to terrorism without any judicial review, as well as the blocking of Internet sites without prior judicial authorization, are highly problematic and should be avoided.

Anti-terrorism measures such as telephone tapping and disturbance of an individual should be subject to full judicial oversight. Suspects should be provided with procedural safeguards. Legislation in this area must be as detailed as possible in its definition of the criteria for entering a person into an anti-terrorist database and in its determination of the use of such databases.

An independent assessment of the use and impact of individual information databases must be carried out in order to ensure that they are necessary and proportionate. The use of data collected through telecommunication surveillance or other forms of undercover investigations should be strictly limited to the purpose of investigating serious crimes. Surveillance activities should be authorised by a judge, set out strict limits on its duration, as well as rules on the disclosure and destruction of surveillance data, and provide for ex post remedies to all individuals concerned.

The principle of making data available to other authorities should not be used to circumvent European and national constitutional data-protection standards. The collection of data on individuals solely on the basis of, for example, ethnic origin, religious belief, sexual behaviour or political opinions should be prohibited.

All victims of terrorism should be rapidly afforded assistance, including the right to support, adequate care, and compensation.