Hearing of the European Economic and Social Committee (EESC)

9 February 2010

Counter-Terrorism Policy and Data Protection

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor

1. The need for a transparent ongoing discussion on the fragmented policy framework of counter-terrorism

The search for a balance between security, especially in the counter-terrorism arena, and fundamental rights, particularly regarding privacy and data protection, is not a new topic. But discussions on this matter are ongoing.

Security and data protection are two fundamental values shared by the EU as a whole, which are not incompatible one with another. They should both be taken into careful consideration in the discussion on what an EU counter-terrorism policy should look like.

Stemming from the wider framework of the Stockholm Programme ¹ – and its implementing action plan ² – new policy initiatives are popping up: not only those mentioned in the Communication on The EU Counter-Terrorism Policy ³, starting point of our discussion today, but also those contained, for example,

in the Communication on the EU Internal Security Strategy 4 and in the Communication related to the Overview of information management in the area of freedom, security and justice 5. Moreover, it’s also worth bearing in mind the content of the recent EU Action Plan on combating terrorism presented by the EU Counter-Terrorism Coordinator6.

At European level, the framework is complex and subject to constant change and fine-tuning on a day by day basis, often incident driven (e.g. the body scanner case), due to the interplay of several initiatives in different areas involving many parties, both on the law enforcement side as well as, with a growing intensity, in the private sector. While the clarity and uniformity of the definition of terrorism should be improved, it is also evident that counter-terrorism activities are horizontal and have a wide impact in the area of police and judicial cooperation in criminal matters, in the development of the Internal Security Strategy as well as, finally, in the Common Foreign and Security Policy.

But this is only one side of the coin: from the data protection perspective – and (more widely) from a fundamental rights perspective – we should bear in mind that many significant anti-terrorism measures at this stage still remain within the remits of (the competent authorities of) the Member States: potential compression of the rights of individuals are therefore more relevant than the picture we gain by considering only the legislative framework at the European level.

The first reaction to this complex, fragmented and mobile landscape is, therefore, the need for all stakeholders – policy and rule makers, civil society and citizens as individuals – to have a clear picture of the existing policies and of those which are going to be introduced and, as far as possible, an unambiguous and understandable description of the data processing involved in the process 7.

---


6 EU Counter-Terrorism Coordinator (CTC), EU Action Plan on combating terrorism, 15893/1/10, Brussels, 17 January 2011.

7 In this respect see the See Communication relating the "Overview of information management in the area of freedom, security and justice", COM/2010/0385 final, p. 10 et seq. See also Amann v. Switzerland of 16 February 2000 (ECHR 28341/95) and Rotaru v. Romania of 4 May 2000 (EChHR 27798/95).
Data protection is not the only perspective to be taken into account in the debate on EU counter-terrorism strategy, but it has strategic consequences on this debate, since counter-terrorism measures often involve (or are very likely to involve) a processing of a vast amount of (possibly) sensitive personal data. This has been highlighted in various opinions of the EDPS and Article 29 Data Protection Working Party. Both of them emphasised as well that effective data protection is a key factor for success of any strategy in areas like this one 8.

As a consequence it is strongly desirable to have a coherent and more comprehensive approach providing for explicit links and interactions between different initiatives as a pre-requisite for lawful and fair processing of personal data9, particularly in the area of home affairs and internal security, providing for appropriate and positive synergies, and avoiding duplication of work and efforts 10.

Indeed, transparency in the data flows and accountability on the side of the body in charge of law enforcement activities in the area of counter-terrorism are the pre-conditions for the fundamental rights of the individual in a democratic society. I want to be clear on this point: not only EU institutions and bodies, including the EDPS, the European Union Agency for Fundamental Rights, and the national data protection authorities (within their respective remits), but also organised civil society should play an important role in the process of:

- keeping fundamental rights as an ongoing priority for law makers in order to preserve and reinforce the democratic nature of our society, in conformity with the values recognised in the Charter of Fundamental Rights of the European Union, which is binding for European institutions and Member States when they apply European law, and in the constitutional traditions of the Member

---

8 See: EDPS's Opinion of 14 January 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of regions - "A comprehensive approach on personal data protection on the European Union"

9 It should be recognized that a first step has been done thanks the communication mentioned in footnote 7.

States 11, also considering the Union’s accession process to the European Convention on Human Rights made obligatory by the Lisbon Treaty (Article 6(2) TEU);

- increasing awareness and foster a “fundamental rights culture”, introducing, as a counterbalance to the growing (mass) "dataveillance", a wide social control and an ongoing public discussion on the "surveillance infrastructures" built into our societies.

2. The current EU policy: a development of the (traditional, well established) four layer approach and its impact on (fundamental rights and) data protection

We all are familiar with the "traditional" four layer approach of the EU counter-terrorism strategy based, since 2005, on different measures, most of them based on personal data processing, aiming to A) "prevent", B) "protect", C) "pursue" and D) "respond" to terrorism 12. Recognising the crucial role to be played by civil society in the prevention of terrorism 13, other speakers will give us an updated overview on these four pillars in counter-terrorism; I will not go in to details.

On my side, it is enough to say that in every layer we could easily find clear data protection implications 14: starting with, for example,

---

11 See also Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen, Brussels, 4 November 2009, COM(2009) 262 final, point 3.4.: "Any policies adopted in the area of security must protect the values of freedom and the rule of law. These policies must be rooted in the protection of the fundamental rights as guaranteed by the European Convention on Human Rights and the EU’s Charter of Fundamental Rights”.


13 On this topic see the Opinion of European Economic and Social Committee, Prevention of terrorism and violent radicalisation, Brussels, 22 April 2008, SOC/301, highlighting the complexity of factors (socio-economic and cultural ones) in the influence of terrorism and the need to effectively intervene on them in order to reach effective prevention.

14 A more detailed picture could be obtained from the EDPS Opinion of 24 November 2010 on the Communication from the Commission to the European Parliament and the Council concerning the EU Counter-Terrorism Policy: main achievements and future challenges,
the data retention debate on Directive 2006/24/EC, to the policy relating to so-called ‘terrorists’ lists’ (in order to adopt restrictive measures — like asset-freezing and travel bans — on natural and legal persons suspected of being associated with terrorist organisations and/or certain governments); the use of biometrics in order to identify individuals 15; the security scanners discussion; the weapons precursors preventive measures 16 and, last but not least, to the cross-border cooperation in criminal matters within the EU and the exchange of data outside the EU (the PNR and Swift cases) 17.

Moreover data protection issues are clearly involved in the Prüm Decision 18, in the Schengen Information System (and SIS II) and in the aforementioned EU Information Management Strategy.

Finally, it is also beyond question that these measures are not limited within the European borders: international cooperation in the fight against terrorism, widely based on exchanges of personal information, is without doubt a significant part of the European strategy. It is patent, therefore, the need to ensure adequate safeguards when personal data are processed in this context, while promoting the development and implementation of data protection


principles by third countries and international organisations; the existing (bilateral and multi-lateral) agreements between European Union and non-European countries in the field of police and judicial cooperation in criminal matters, including the fight against terrorism, should be monitored on regular basis and improved. As a general rule, they should all be in conformity with the EU legal framework of data protection.

What are the (major) risks for the individuals?

a. Data processing related to broad categories of individuals (e.g. groups of flight passengers, electronic communication services users, groups of financial transactions) and adoption of "preventive measures" involves the risk of discrimination and stigmatisation of individuals and/or groups of the population (especially through ethnic profiling) 19;

b. reliance on automated decision-making, often based on data mining techniques, involves the high risk of “false positives”/“false negatives”, exacerbating in the meantime the risks of discrimination, inequality and disregard for human dignity;

c. increasing "partnership" between law enforcement authorities (LEAs) and private subjects (such as internet service providers, financial institutions and transportation companies) results in an increasing erosion of the finality principle.

3. Basic proposals in order to prevent a clash between security and data protection

Surveillance information technologies and personal data processing are the building blocks of a large part of the EU counter-terrorism strategy. The strategy, (apparently) stemming from the emergency 20, will probably remain for a long period of time.

---


20 Indeed counter-terrorism strategies have been developed in the past by many Member States.
Precisely for this reason, this strategy needs to be accompanied, at every stage of its development, by a concrete and robust policy on the front of the fundamental rights. This policy, limiting my considerations to the privacy and data protection aspects, should always be based (at least) on four legs:

- *ex ante*, the minimum interference principle on the fundamental rights of the individuals shall be the default rule: it means that
  - the principles of strict necessity and proportionality (also in the design of the information infrastructure), data quality \(^{21}\) and, with the appropriate exceptions, transparency in relation to the individuals concerned are the golden rules in this field; the necessity of such measure should be truly demonstrated based on facts and evidence and not pure assumption; moreover, particular care should be reserved in the case of sensitive data processing: the more sensitive they are, the more limited should be the purposes for which they can be used (and the more limited the access);
  - privacy by design: data protection principles have to be fed into the information systems and other technical tools at a very early stage, so as to guide policy options and to ensure that privacy is embedded to the fullest possible extent in security-oriented technologies;
  - tools to evaluate the impact on privacy and data protection, particularly in case of large scale databases or interconnection between existing databases, have to be developed;
  - proper privacy and data protection impact assessment – done in collaboration with relevant civil society stakeholders – is the basic tool for the assessment of several possible policy options, in order to select the least privacy-intrusive one and,

---

\(^{21}\) For example, concerning the so called "terrorists’ list" data quality should be ensured by taking into account relevant developments in the police and security investigation on which listings are based and by carrying out regular reviews of the lists and listed persons should be provided with adequate information and with the right to have access to personal data concerning them (in order to ask, if the case, for the rectification of the information).
more radically, to evaluate the real need for a new instrument considering the existing ones 22;

- if legislative measures involving personal data processing need to be adopted, then:
  
  o a clear legal basis should be provided and detailed descriptions of the essential elements of the data processing (data subjects concerned, category of subjects who can have access to the information processed and recipients of the same, logic involved in the automatic processing of data concerning individuals, at least in case of automatic decisions and data profiling, data retention time) should be provided in the legislation;

  o in the area of counter-terrorism measures, general clauses and vague rules 23, as well as wide area of intervention given to the secondary legislation, should be prevented;

  o effective judicial remedies, liability and adequate compensation be ensured in case of the unlawful processing of personal data;

- ex post, the periodic, comprehensive and objective (i.e. showing also weakness of the systems) evaluation of the effectiveness of the legislative and organisational measures introduced via an independent and multidisciplinary panel. This evaluation should serve, first of all, the lawmakers (at European and national level), in order to evaluate the efficacy of the measures introduced 24; but also the public


23 See Copland v. The United Kingdom - 62617/00 [2007] ECHR 253 (3 April 2007), point 46: "the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures".

24 It doesn't happen very often: see, e.g., with regard to the revision of the data retention directive the conclusions of the Article 29 Data Protection Working Party, WP 172, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, adopted on 13 July 2010, p. 2: "The lack of available sensible statistics hinders the assessment of whether the Directive has achieved its objective".
at large who should be allowed to have access, through the mediation of organised civil society, to these information in order to ascertain the real need for the restriction of individual rights. Often it is said that rights have a cost. Also security implies costs; therefore an accurate and truthful cost/benefit analysis needs to be done in order to efficiently allocate the resources assigned to the (multifaceted) anti-terrorism strategy. Periodic evaluation of the effectiveness of the counter-terrorism strategy could be driven by "sunset" regulations that "force" lawmakers to evaluate the ongoing utility and efficacy of the existing measures;

- effective controls: counter-terrorism measures are based, to a large extent, on personal data processing and, the powers of the individuals concerned to be informed or to have access to their own data are strongly restricted. The right of informational self-determination, usually based on transparency and autonomy, should therefore be reinforced and assured introducing and increasing, in parallel with the usual "individual control", other forms of institutional control. This is a task that belongs, first of all, to the data controllers themselves (and could be carried out by introducing adequate procedures to guarantee the data quality principle and with the designation of “qualified” data protection officers); increased weight, equipping them with sufficient powers and appropriate resources, should be given to the supervisory role of the independent data protection authorities (if the case, in cooperation between them).

4. Closing remarks: The EDPS' active role in its “advice-giving” function and the need to respect fundamental rights and data protection: from theory to practice

The EDPS has closely followed, with opinions 25 the developments at EU level of this very sensitive area, highlighting the risks for the individuals as a result of the development amongst others of large

25 Apart from those just mentioned, see EDPS Opinion on the Initiative of several Member States with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ C 169, 21.7.2007, p. 2.
scale information systems and strongly supporting the idea that the respect of the rule of law and the effective protection of fundamental rights – and, between them, in particular of privacy and data protection – should be the pre-requisite in the fight against terrorism, as well as an essential legal condition to build and develop new data collection systems and foster international cooperation.

I see a clear need of consistency between all the policies and initiatives in the area of home affairs and internal security, instead of the present fragmented framework; moreover, a systematic approach in this area should be preferred to incident-driven policy-making.

Against this background, the EDPS looks forward to a comprehensive and consistent framework for the protection of personal data covering counter-terrorism policy, also when these activities are carried out in the framework of the Common Foreign and Security Policy.

The Lisbon Treaty provides the appropriate tools (Article 16 TFEU and Article 39 TEU) and the EU legislator should profit from them.

You can easily find this fil rouge in all our opinions where it is clearly stated that strong data protection commitment serves to:

• obtain better quality of the data processed, and therefore improve the counter-terrorism action;

• ensure a reduction in racism, xenophobia and discrimination, which can also contribute to preventing radicalisation and recruitment into terrorism.

* * *

A short closing remark: I wish to emphasise that the EDPS is glad to see that all the recent policy documents clearly recognise that privacy and data protection, as fundamental rights, are building blocks of any counter-terrorism strategy.26

26 See The Stockholm Programme, point 4.5. and passim: "Respect for the Rule of Law, fundamental rights and freedoms is one of the bases for the Union’s overall counter-terrorism work. Measures in the fight against terrorism must be undertaken within the framework of full respect for fundamental rights and freedoms so that they do not give rise to challenge. Moreover, all the parties concerned should avoid stigmatising any particular group of people, and should develop intercultural dialogue in order to promote mutual awareness and understanding"; Communication, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, p. 3: "Our counter terrorism policies should be proportionate to the scale of the challenges and focus on preventing
But this is only a first step: the future legislative proposals should clearly describe how this target will be achieved in practice.

The EDPS is ready and willing to play its part in achieving this ambitious objective.