EU counter-terrorism policy: main achievements and future challenges

2010/2311(INI) - 24/11/2010 - Document attached to the procedure

OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS).

The EDPS recalls that by building on the structure of the 2005 EU Counter- Terrorism Strategy, the Communication first analyzes the four major strands of EU Counter-Terrorism Policy: prevent, protect, pursue and respond.

The areas of ?prevention? and ?protection? are the most delicate ones from a data protection perspective, for various reasons:

(1) these areas are by definition based on prospective risk assessments, which in most cases trigger a broad and ?preventive? processing of vast amounts of personal information on non-suspected citizens (such as, for example, internet screening, e-borders and security scanners);

(2) the Communication envisages increasing partnerships between law enforcement authorities and private companies (such as internet service providers, financial institutions and transportation companies) with a view to exchange relevant information and sometimes to ?delegate? to them certain parts of law enforcement tasks. This entails an increased use of personal data, collected by private companies for commercial purposes, for the use by public authorities for law enforcement purposes;

(3) ?preventive? use of personal data is more likely to lead to discrimination. The preventive analysis of information would entail the collection and processing of personal data relating to broad categories of individuals (for example, all passengers, all internet users) irrespective of any specific suspicion about them. The analysis of these data ? especially if coupled with data-mining techniques ? may result in innocent people being flagged as suspects only because their profile (age, sex, religion, etc.) and/or patterns (for example, in travelling, in using internet, etc) match those of people connected with terrorism or suspected to be connected.

The EDPS welcomes the attention that the Communication pays to fundamental rights and data protection, and recommends further concrete improvements in the area of counter-terrorism policy.

The EDPS recommends supporting with concrete initiatives the respect of fundamental rights in this area, and in particular of the right to the protection of personal data. It also supports the approach that systematic policy making in this area should be preferred to incident-driven policy-making. In this perspective, it recommends the EU institutions to ensure that policies and initiatives in the area of home affairs and internal security are designed and implemented in a way which will ensure a consistent approach and clear links between them, providing for appropriate and positive synergies, and avoiding duplication of work and efforts.

Against this background, EDPS recommends the EU legislator to step up the role of data protection, by committing to specific actions (and deadlines), such as:

- assessing the effectiveness of existing measures while considering their impact on privacy is crucial and should vest an important role in European Union's action in this area.
- when envisaging new measures, considering possible overlapping with already existing instruments, taking into account their effectiveness, and limiting the collection and exchange of personal data to what is really necessary for the purposes pursued;
- proposing the establishment of a data protection framework applicable also to the Common Foreign and Security Policy;
- proposing a comprehensive and global approach to ensuring, in the area of (asset-freezing) restrictive measures, both the effectiveness of the law enforcement action and the respect for fundamental rights, on the basis of Article 75 TFEU;
- putting data protection at the heart of the debate of the measures in this area, by ensuring for example that Privacy and Data Protection Impact Assessments are carried out and competent data protection authorities are timely consulted when relevant proposals in this area are put forward;
- ensuring that data protection expertise is fed into the security research at a very early stage, so as to guide policy options and to ensure that privacy is embedded to the fullest possible extent in new security-oriented technologies;
- ensuring adequate safeguards when personal data are processed in the context of international cooperation, while promoting the development and implementation of data protection principles by third countries and international organisations.