Privacy issues with EU Law Enforcement Cooperation Developments
Meryem Marzouki - European Digital Rights
The Public Voice Conference: Global Privacy Standards in a Global World
Madrid – 3 November 2009

European Digital Rights (EDRI) is an association of 27 digital rights organizations active in 17 European countries. This allows EDRI and its members to promote and defend, inter alia, privacy and data protection at the European level as well as at the national levels. This specificity makes EDRI particularly well placed to observe the national trends as well as the EU trends, which are reinforcing each other, most notably in a process identified by some as policy laundering, which results in some member States pushing for adoption at EU level of legislation that would raise strong resistance at national level. In this short presentation, I will focus on data sharing and data protection issues in EU law enforcement cooperation.

One of the main current concerns is the so-called Stockholm program, which will determine the EU plans for the next five years in the "Freedom, Security and Justice" area. In terms of data sharing, the Stockholm program aims at achieving full integration through total interoperability, and full access of databases for police purposes. It comes after the Tempere program of 1999, relying on information exchange, and The Hague program of 2004, relying on the "data availability" principle.

At the EU level, an example of threats is the proposal to give access to EUROPOL and member States law enforcement agencies to EURODAC database, which contains information on refugees and asylum seekers. Such plans raise important concerns, given the fact that some EU countries run an incredibly high number of databases, some of them set up without proper legal basis and lacking proper control. A report entitled "The Database State", published in the UK in May 2009 and authored by one EDRI member, has found that, of 46 public sector databases, almost a quarter were certainly illegal. In France, a parliamentary report has identified more than 55 police databases, some of them containing an incredible level of erroneous or not updated data, as highlighted by a report from the French Data Protection authority in December 2008. Such databases contain highly sensitive information, like DNA and other biometric identifiers.

This raises the issue of control. Reaffirming principles such as the proportionality and limited purpose principles is not enough. The EU legislation must implement actual guarantees which are not currently adequately fulfilled.

Among the main observed trends are the extension of purposes, the enlargement of scope and means of the databases, and the fact that they more and more target vulnerable groups, such as migrants, minorities, children and youngster. Minor are particularly targeted in the UK, where children can have their DNA taken and filed in the national DNA database starting from age 10. In France, intelligence databases looking to prevent public security infractions may register children starting from age 13. Databases once set up to fight terrorism and serious crime are now used to fight minor delinquency. This is the case, for instance, with the French DNA database.

Current protecting legislation does not provide enough guarantees. The EU Data Protection Framework Decision, which rules data protection under 3rd pillar (police and justice cooperation), has only been adopted in December 2008. Yet, it still lacks protection with regards to the transfer

of member States domestic data to third countries, which means that, for instance, it does not apply to the transfer of European airline passenger data (PNR) to the USA.

Moreover, these databases lack protection against loss or theft of data, as millions of personal data lost by or stolen from UK government services have shown since 2007. The current revision of the EU Telecom package includes some provisions on data breach notification, but they would be mandatory only for Internet service providers and telecom operators.

Biometric identity (as in passports and national identity cards) is an important issue in Europe, with the creation in many countries of national centralized databases containing biometric identifiers. The biometric passport, which is an obligation since the 2004 Regulation of the EU Council, has been an opportunity for some member States to go beyond EU requirements. In France, a central database has been established, while in Germany, such a central database has been forbidden by law.

Finally, despite important resistances at national level in many countries, especially in Germany, the data retention Directive of 2006 has been implemented, sometimes going beyond the Directive requirements in terms of retained categories of data.

These are only some of the main concerns currently at the EU level. The expected entry into force of the Lisbon Treaty early next year will not be enough to ensure the required guarantees. With the adoption of the Stockholm programme probably by the end of this year, the need will be even greater for better data protection provisions at EU level, such as:

- The need to establish actual implementation of the proportionality and purpose limitation principles;
- The need to drastically limit the use of biometric and genetic data;
- The need to better protect against risks of uncontrolled data sharing; and
- The need to better protect of vulnerable groups.