Law and ethics in the modern EU 'surveillance society': Are the data protection principles 'dead' in the Area of Freedom Security and Justice? The case-study of the information systems of VIS and EURODAC.

It has been observed that after the September 9/11 terrorist attacks and especially after the Madrid and London bombings, the European Union (EU) is acting as an emerging 'surveillance society'. This is based on the emphasis that the EU has placed over the past years on the creation of an extensive toolbox for the collection, storage, and exchange of information between national authorities and other European players in the area of freedom, security, and justice.

A particularly powerful weapon in the new surveillance era is the database: the storage and exchange of information through large-scale information systems that interlink to each other and can be used by a range of different authorities. For this reason, a proliferation of cross-border information systems used for law enforcement purposes has been witnessed over the past few years. This 'security web' is currently being spun at national, supranational and transatlantic levels alike.

However, despite the obvious benefits, large-scale databases raise many questions. What are the channels of information used at the EU level for law enforcement? What links exist between them? How does information reach these databases? What data is stored and for how long? How does information exchange in the area of Freedom, Security and Justice take place? Which states participate and which authorities have access to each system? How 'secure' are the databases? But above all: what are their implications on the rights to privacy and data protection of the individuals? What rights has the individual to check and, if necessary, to correct data held about himself or herself? These questions are of particular importance in the field of police and judicial cooperation, where information held in such databases may seriously affect the fundamental rights of those who are subject of an entry.

Within the EU context a further particularity threatens the very existence of basic data protection principles: Most of the EU databases have nothing to do with the fight against terrorism or crime. They are created for different purposes such as the Visa Information System that was created to support the common visa policy, or Eurodac that was establish to enhance the common asylum policy. Yet, data contained in the former database can be accessed by designated authorities of Member States and by Europol to fight terrorism; the same with even more serious consequences is proposed with respect to Eurodac. This raises many concerns: once the information has been collected and stored in centralized databases it can be very easily used for law enforcement purposes. This is required in the name of the 'surveillance society'. However, what are the implications of this on the 'purpose limitation' principle which has been characterized as the keystone of data protection laws? More generally, are data protection principles 'dead' in the surveillance society?