

CCBE Statement on governmental practices involving mass data mining for the purpose of surveillance

01/07/2013

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 32 member countries and 11 further associate and observer countries, and through them more than 1 million European lawyers.

The CCBE has noted with great concern the recent revelations of governmental practices involving mass data mining for the purpose of surveillance.

The CCBE has repeatedly stressed the importance of professional secrecy (known in some countries as legal professional privilege) and would point out that the European Court of Justice itself expressly stated in its decision in the AM&S case (case C-155/79): “that confidentiality serves the requirements, the importance of which is recognized in all of the member states, that any person must be able, without constraint, to consult a lawyer whose profession entails the giving of independent legal advice to all those in need of it”, and added that “the principle of the protection against disclosure afforded to written communications between lawyer and client is based principally on a recognition of the very nature of the legal profession, inasmuch as it contributes towards the maintenance of the rule of law and that the rights of the defence must be respected”.

This core value of the legal profession is, however, under attack from organisations with highly sophisticated technical capabilities and financial means, including state bodies having secret investigatory powers.

Lawyers have no choice but to use modern technology when communicating with clients, courts, lawyer colleagues and others. Yet it now appears that such technology is not safe to use.

The erosion of the confidentiality of lawyer-client communications also erodes the trust of a citizen in the rule of law.

Therefore, the CCBE calls upon the EU institutions to take steps to protect and enhance the confidentiality of lawyer-client communications when modern technology is used. Such steps could include work in the area of technical standardisation (e.g. the possibility of setting up a lawyer account that is subject to greater protection against data mining) or in the area of instruments of international law.