

Law Enforcement Agencies (LEAs) Activities in the Cloud Environment: A European Legal Perspective

ABSTRACT

The paper aims to discuss some major issues in relation to the complex and highly debated relationship between Cloud Service Providers (“CSPs”) and government agency responsible for the enforcement of the laws (Law Enforcement Agencies – “LEAs”). Our analysis focuses on the EU situation and investigates whether the protection of personal data of EU citizens against LEAs' access is adequately guaranteed and what are the main elements that have to be taken into account by CPSs when dealing with LEAs' requests.

The topic is a challenging one. The protection of the individual's personal data from government intrusion has historically been at the core of the notion of privacy. As it has been held in the famous English common law Semayne's case, *“the house of everyone is to him as his castle and fortress”*, protected even against the forceful access of police officers. Right to privacy is directly connected to the very essence of fundamental human rights: the establishment of a legal status for the human being, which shields him/her against all unjustified interventions into his/her body and private sphere (being such interventions material or not) by external (more powerful) entities.

After a brief overview of the existing international scenario, the legal grounds of LEAs' activities in the cloud is examined. The main focus is on the Council of Europe Cybercrime Convention, which establishes the common ground between the US and majority of the EU Member States and is regarded by the EU Commission as *“the main legal instrument”* in the fight against cybercrime. The whole analysis is then applied to the relationship between CSPs and their clients. In this respect, we consider the position recently expressed by the Art. 29 Working Party on cloud computing technologies (opinion no. 5/2012) and the repeated EU Commission calls for

transparency in the relationships between the CSP and its clients, in order to increase trust in such technology. In our conclusions we highlight the very delicate position of CSPs, precisely taken between an obligation to comply with LEAs' requests, data protection regulations and obligations of transparency towards their clients.

The paper also takes into account the European cloud strategy published by the EU Commission on 27 September 2012. However, this strategy bears little impact on the present analysis. While the strategy reinforces the strong commitment of the Commission on cloud technology, it dedicates only marginal attention to the delicate relationship between data protection and LEAs' powers: *“The Commission will also build on its on-going international dialogues with the USA, India, Japan and other countries, as regards, inter alia, key themes related to cloud services as discussed above, such as data protection; access to data by law enforcement agencies and the use of Mutual Legal Assistance Agreements to avoid confronting companies with conflicting requests from public authorities”*.

Status: Published by Taylor & Francis in *Information & Communications Technology Law* journal



CITATION

Balboni, P., & Pelino, E. (2013). Law enforcement agencies' activities in the cloud environment: a european legal perspective. *Information & Communications Technology Law*, 22(2), 165-190. doi: 10.1080/13600834.2013.821812

Access the article [here](#).