Fighting against Cybercrime in Europe: The Admissibility of Remote Searches in Spain

Juan Carlos Ortiz Pradillo*
Associate Professor of Criminal Procedural Law, University of Castilla-La Mancha, Spain

1. The Global Threat of Cybercrime and the World’s Concern about its Criminal Investigation

The use of information and communications technology (ICT), and especially the new opportunities which Internet offers, has caused a radical change not only regarding the modus operandi of traditional crimes and the process of shaping new types of crimes, but also in respect of new available technological advances destined to their investigation and providing evidence. Therefore, as the substantive criminal law has reacted by adjusting itself to these new forms of delinquency related to high technology, criminalising these new types of crimes, the procedural law equally requires an important adaptation to the contemporary digital age, not in respect of the application of the information technology in the proceeding and carrying-out of procedural acts (the most outstanding examples of which, among others, would be the definitive introduction of electronic case files, the telematics’ presentation of texts, documents, as well as notifications, the digital recording of hearings in a digital format suitable for their registration and reproduction, judicial sale of goods by public auction carried out in the internet, the seizure and freezing of

* E-mail: JuanCarlos.Ortiz@uclm.es. This paper was prepared with financial support from the Spanish Ministry of Science and Technology (DER2008-03378: “Problemas procesales de la ciberdelincuencia y de la ciberresponsabilidad”). The author thanks the many people who made this paper possible. Special thanks go to Montserrat Cuesta, Professor Dr. Nicolás González-Cuéllar and Professor Dr. Ulrich Sieber (thanks for his encouragement during my research staff at the Max Planck Institute for Foreign and International Criminal Law in Freiburg i. Br., February–May 2008), without whose support the entire project would have been impossible.
banking assets using the ICT, or the common application of videoconference), but in particular in the aspects concerning diverse IT techniques and instruments in the service of the investigation against crime.

The current technological advances are used by the security forces and police, both in the tasks of investigation and follow-up actions (through what has come to be called technosurveillance or electronic surveillance\(^1\)), and as well in the sphere related to the forensic analysis of varied electronic storage devices (computers, mobile phones, palmtop computers – PDAs, USB memory, and also GPS navigators\(^2\)) through the science called “computer forensics”, despite the lack of sufficient and modern legislation.\(^3\)

Furthermore, the mentioned technology is used to obtain the evidence of any kind of crime, constituting (or not) the so-called ‘computer (cyber) crimes’. It can and should be applied in the investigation of those actions in which the computer equipment, programmes or data, establish the instruments, objects or effects of the crime, or traces of its perpetration, and it is an efficient tool in the investigation of all those ‘traditional’ crimes in which such actions form a valuable source of evidence, due to its present capacities of storage of information and its use for all types of communication. As Professor González-Cuéllar Serrano rightly points out, a violent young person who videotapes a brutal beating of a homeless man with his mobile phone, or a drug dealer who records the transaction details in an electronic document in his notebook, are not cybercriminals but create digital data that gives information about a punishable action.\(^4\)

---


