Crime investigators have always been running behind technological developments. However, it seems like they start having some smart ideas as well. How can investigators get hold of the data that is saved on a private computer? Data which might be important evidence and possibly give hints on a planned or already committed crime? One way is a normal and traditional house search with the seizure of the computer. However, this can have many disadvantages. A house search requires a search warrant along with a bundle of strict procedural rules, and after all the suspect will know that the police is after him. Perhaps the police may want to remain secret without the suspect knowing that an investigation is going on at all. A very tempting solution could be the secret access to the suspect’s computer – through the Internet. Can this work? An idea is that a special spy software is secretly installed on the suspect’s computer. This could be done for example through a disguised e-mail attachment (like a computer virus), or manually in secret. The software would automatically install itself on the computer, similar to a Trojan. Then it would automatically search the hard disk, and – once the computer goes online anytime – it would automatically transfer the detected data to the police. That plan sounds indeed very tempting, and not difficult at all. Germany and Austria are publicly and controversially discussing this possibility. US law enforcement authorities already seem to use a similar procedure.

The paper will compare such an “online house search” with a traditional house search. It will continue to analyse legal problems that might arise, especially with connection to fundamental rights. A core problem might be what on the other side is the main motivation behind that idea for investigators, i.e. that the suspect will not know that his computer is spied out. The paper will then address the question whether a spy software should certainly belong onto the agenda of modern crime investigators or intelligence agencies in order to ensure effective means in times of digitised and globalised crime and terrorism. Does the age of Web 2.0 require a
Spy 2.0 as a logical answer? The paper will also consider these issues in the context of other perhaps related technological provisions that are used in order to combat crime, such as e-mail surveillance or telecommunications data retention.