Data interception vs. professional confidentiality

The contradiction between governmental or private wiretapping of electronic communications and the obligation to confidentiality held by lawyers, doctors, or tax advisors destroys any basis of trust. Professionals as well as their clients or patients are exposed to direct risks. This situation necessitates a broad discussion.

The revelations of spying on electronic data and global internet traffic probably only adds to the work load of some very few sufficiently specialized colleagues. I hope their number will increase at the same fast pace as the extent of our knowledge about a world of transparent data. These lawyers are needed.

Politicians and thus legislators, too, are failing (and refusing) to act or to be even willing to act effectively, because they are (a major) part of the problem: the revelations are painfully embarrassing in a literal sense. Painfully, because it becomes clear that the relevant control mechanisms are intentionally or unintentionally ineffective. Painfully, because an antidemocratic spirit was revealed. Painfully, because the political realm can no longer profit from data abuse so brazenly.

But it becomes clear, too, that there is no effective control whatsoever that would protect a company's personal data or sensitive data. The interconnected infrastructure of global internet traffic uses technologies which only their developers can handle until such time as they are hacked by someone else who in turn uses his new found knowledge – with a slight head start – to gain an advantage. The result: an epidemic race without antidote. Since intelligence services work secretly, there is no one who can control them. Parliamentary control panels, which often lack the technical competence, are merely an act of tokenism.

Data interception and the systems behind it pose a threat to lawyers as well as any other profession bound by confidentiality. How is the security lack of electronic data traffic to be reconciled with professional confidentiality, the latter being sanctioned by civil law, criminal law and the law governing professions? The internet is an uncontrolled à la carte supplier for intelligence services, private communications companies, or perpetrators and victims of data abuse. Therefore, it is no longer of any use to secure information exchange. Under these circumstances, how can legislators still pursue the project of carrying out the courts' official correspondence only electronically? The half-life of the security systems that the government today intends to use to that end will probably not keep up with the terrific speed at which security systems get cracked.

With today's knowledge, provisions on electronic data exchange as exclusive mode of correspondence with courts and public authorities cannot be reconciled with the unconditional obligation to confidentiality. In the latter case as in cases of e-mail traffic, even the most careful professionals bound by confidentiality have no control over the data and have neither the possibility to find out who accesses the data and how they do it nor how and when the data is used.

The obligation to confidentiality is but one side of the story. The confidentiality of lawyer-client relationships is threatened, as well. Will it be downgraded because we as representatives of the profession can no longer ensure confidentiality? Am I, as a lawyer and/or notary, still allowed to participate in international electronic data exchange consisting of confidential contracts on an M&A transaction, if, as we now know, unauthorized third parties can read along as they please and potentially abuse information? How will courts decide in cases where data abuse has caused damage to the client? Is it enough to argue: “I didn’t know, I couldn’t have prevented the data abuse”? Was there any confidentiality protection in place before Wikileaks and Snowden and does it still exist? And for how long? Am I rendering myself liable to prosecution or to pay damages? What does the liability insurance say to all this? Do the daily occurring new revelations give cause to an increase of risk as set out by Section 23 of the VVG (German Insurance Contract Act)?

Where does a lawyer’s obligation to due diligence end, if we do not even know the mechanisms at play, i.e. how to make security systems fail? What kind of due diligence obligations do I have when it comes to applying encryption software and checking its effectiveness, when at the same time the NSA-revelations in the USA have also shown that governments are putting encryption software companies under pressure to disclose or conceal their methods for the purpose of unashamed data access? To what extent can and must I check, whether the data is stored in some cloud in the nirvana of the internet and who can or could potentially access it? The warning against American servers and the recommendation to use German ones seem to evaporate in the wake of the revealed cooperation between intelligence services all over the globe, which is apparently even said to be based on secret intergovernmental agreements. Can I trust authorities which themselves seem to be both victims and perpetrators?

I do not have a solution. I can only encourage an open discussion. With the risk of data abuse, does legislation have to release us by law from adhering to confidentiality requirements, when communications network providers, with or without government support, cannot guarantee the security of their services while nonetheless everybody depends on these services? This should be rather difficult, since the government would have to protect us from itself.

By Dr. Ekkehard Helmig, lawyer and notary,

Wiesbaden (Germany)

Translated from German into English by Charlotte Kieslich

The original was published in NJW-aktuell *volume 36/2013*