HOW TO ACHIEVE A BALANCE BETWEEN EFFECTIVE PREVENTING CRIME AND PROTECTING PRIVACY OF CITIZENS

ONLINE SEARCH – AS A NEW CHALLENGE FOR EJUSTICE

by

JUSTYNA KUREK*

The natural consequence of development of Information Society is that investigators should be able to collect evidence in digital environment. Access to data stored on personal computers enables collection of important information about suspects - for example their plans, habits and contacts. Using hacking tools investigators can detect bank account numbers or secret pin codes. The development of Internet technologies made it possible to do it secretly, without people knowing that they are being watched. Furthermore, the methods typically used to commit crimes on the Net such as: Trojan software, keyloggers or sniffers can be also used by investigators and police to protect citizens and to fight terror effectively.

Are traditional legal measures, typical for off-line police operational activities such as surveillance, bugging telephones, searching homes or requesting data from third parties, sufficient for on-line investigation? Or is it necessary to adopt a special legal regime to deal with this situation? Another important question is how to seek a delicate balance between effective crime-fighting law and one which respect constitutional rights? New investigation methods that are based on hacking tools can easily violate citizens' rights such as the right to privacy, information self-determination or home inviolability.

KEYWORDS:
Online search, e-justice

* The author cooperates with the Centre for Law of the New Technologies at the Faculty of Law and Administration of the University of Warsaw, jkurek@cpnt.wpia.uw.edu.pl

Development of information society services has moved a large part of our life activity from the real world to the virtual one. New Internet tools are applied not only in shopping or banking transactions, but they also "effectively" support criminals in stealing, swindling, or blackmailing. In numerous cases conventional crimes committed off-line are also prepared via the Internet. That is why the development of information society services poses new challenges for legal protection bodies. It becomes necessary to gather all evidence in the virtual world, and, what is very important, protect and evaluate it. Gathering of evidence may not be, however, limited to confiscation of hardware. The majority of digital traces is to be found on encrypted disks or external servers. Therefore, in order to conduct efficient operational activities in the digital environment, it is necessary to use more advanced information technology tools, in particular such software which secretly traces activity of criminals and suspects without their knowledge. Those instruments will include in particular software of "spyware" type. Nevertheless, application of such tools, in a degree greater than with traditional operational methods used in the real world, touches sensitive aspects, to include the right to privacy, freedom and protection of communication, as well as the right to inviolability of domestic peace, all guaranteed, among others, in art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

At the same time however, the feeling of threat caused by terrorist attacks and an increase in the level of organised crime results in the society having higher and higher expectations towards the State within the area of public security. They are accompanied by widespread consent to the State entering the sphere of fundamental rights guaranteed to every individual, on condition that this is intended to serve accomplishment of the goal, i.e. guaranteeing the protection of citizens' safety. Take the following example - in the real world we agree to omnipresent cameras installed in public places which record us in lifts, supermarkets, or at streets. Although this means of protection breaches our privacy, and – many's the time – even our dignity, we accept it allowing for the goal for accomplishment of which they are used – fighting terrorism and organised crime. In the virtual world such consent to activities conducted by state authorities, resulting from the necessity to guarantee the public security, is also high.

In Poland plans of the government to extend the obligation of data retention up five years have not aroused any social controversies. What is interesting, the argument supporting the extension of the period required for data retention was the necessity to secure the evidence. This resulted, indir-

ectly, from the serious problem of the Polish judicial system seen as lengthiness of proceedings, not from the necessity to fight terrorism and organised crime, which both constitute a threat to security of the State. Those plans have been criticised mainly by telecommunication operators, who would have to directly bear the costs of such solution, and by experts in Community law. The latter emphasised incompliance of the Polish draft act with the requirement of Article 12 of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services. The Directive provides for extension of the maximum two-year period of data retention on condition that a given Member State facing „particular circumstances" states the grounds for introducing such measures and they will be approved by the European Commission.

New information technologies go hand in hand with the development of tools which may be effectively used by law enforcement bodies in their operational activities, and they may support the protection of public order and public security. One of examples may be software enabling remote penetration of computers, such as *Trojan horses*, *sniffers*, or *keyloggers*. A *Trojan horse*, also known just as *Trojan*, is a name of malware which, while acting as a useful or interesting application, it in fact activates an undesirable and hidden functionality (e.g. spyware or logic bombs). A *sniffer* is computer software designed to intercept and, possibly, analyse data flowing across the network. A common feature of many such analysers is switching the network card into a promiscuous mode, in which the device captures all frames from the network, including the ones not addressed directly to it. In addition, s*niffers* may be activated also on a router or a computer which is one of the parties in the communication. The s*niffer* may also be applied for monitoring of network activity of third parties. Another type of computer software used for stealing passwords is a *keylogger*. These programmes take over the control of procedures of the operating system responsible for operation of the keyboard. Each keystroke is recorded in a special file. Optionally, information on keys being struck is supplemented with additional data, such as the name of the active application or window. *Keyloggers* contain functions which protect them from being discovered by an inexperienced computer user, and the file in which the data is recorded is hidden, e.g. among system folders. That is why, if undetected, they can "reside" on a victim computer and cause disclosure of all passwords used. The majority of *keyloggers* have also a specially developed function which enables sending of a file with passwords to a defined e-mail address. Hardware *keylog-*

gers are usually small adapters to be connected to the port of the computer keyboard. The keyboard is then connected to the adapter which records all struck keys in the built-in memory or sends the information via radio. In the case of *keyloggers* of the first type, physical access to the device is necessary in order to read the data. There are also hardware *keylogges* built in the keyboard or the cable connecting the keyboard with the computer.

The effectiveness of such hacking tools are confirmed by American experiences with application of the CIPAV (Computer and Internet Protocol Address Verifier) software. CIPAV is Windows software deployed by the FBI via e-mail or the Instant Messaging communicator. The software is installed on the target computer or on a MySpace or Google Mail account from which it infects the target computer. Upon installation, CIPAV searches the entire hard disk and sends to the FBI recorded information on running programmes, the browser being used, the type of operating system (along with its serial number), as well as other data concerning the user. Facts disclosed by the FBI related to the use of CIPAV prove high effectiveness of the spyware. In 2007 FBI used it during an investigation to identify a person who had repeated bomb threats by e-mail against Timberland High School from 4th to 7th June 2007. After on 12th June 2007 FBI had been granted a court approval to use CIPAV,[1] the perpetrator was arrested on 14th June 2007. Pursuant to the court warrant, the software was only allowed to be used for collection of such data as IP address, Media Access Control address for the network card, list of open TCP and UDP ports, the list of running programs, type of operating system and its version and serial number (in Windows, the serial number is the 25-digit alphanumeric product activation key), default browser and its version, default language of the operating system, currently logged-in user (username), registered company name (the latter is optional in Windows.), the last visited URL. The court warrant expressly limited the possibility to control contents of the suspect's correspondence. Although one may have well-grounded doubts as to whether the FBI restricted themselves to the control of transmission data only and they did not read through the correspondence and the data recorded on the suspect's computer, or whether the spyware had not been deployed earlier in order to identify the perpetrator, the effectiveness of CIPAV seems unquestionable allowing for the fact that there was only a ten-day lapse between the first bomb threat and the actual apprehension of the perpetrator. None of the traditional investigation methods, even analys-

[1] Court search warrant from 12th of June 2007, United States District Court, Western District of Washington, case Nb. 07-MJ-05114-APPL

is of the transmission data taken from the Internet Service Provider would ever result in the perpetrator being captured so swiftly.

Nevertheless, considering the potential scope of their applications, new investigation tools being used in the European legal environment raise numerous doubts. Their usage poses the need to answer crucial questions related with the protection of fundamental rights of individuals, e.g. whether traditional legal protection measures typical of police operational activities in the real world, such as surveillance, bugging telephones, searching or requesting information from third parties are sufficient for investigation methods in the digital environment, or is it necessary to introduce special legal regime controlling such activities? We must also identify a way to achieve a balance between effective criminal law and such criminal law which respect constitutional norms.

In Germany there has been a very interesting discussion continuing in this respect. At the request of the federal authorities special spyware was prepared to conduct remote search of computer hardware. As the German authorities argued, such information technology tools are frequently the only way to access data stored by criminals on computer disks. It is often the case that on confiscation the data has already been permanently deleted and disks – formatted. Moreover, due to potential problems with infecting computers, it was demanded that in further phases appropriate software should be installed in computers at the production stage. In the future this would make it easier to infect computers by spyware used by investigation bodies. Initially, under German law, Strafprozessordnung [the German code of criminal proceedings, hereafter referred to as "StPO") norms were set up to legitimise application of techniques of remote computer penetration. That, however, did not meet with approval of the German Federal Tribunal (hereafter referred to as "BGH"). In its judgement of 31 January 2007 on StB 18/06,[2] the Tribunal stated that remote searches on-line were not covered by the provisions of §102 StPO related with searches performed at the suspect's in connection with §110 sec. 3 StPO on searching electronic data carriers.

Pursuant to §102 StPO it is allowed to search an apartment, other premises or property of a person suspected of being, among others, a perpetrator, co-perpetrator, beneficiary, participant or leader of the crime, if it is supposed that such search may result in obtaining evidence. Based on §110 sec. 3 StPO it is permitted to search electronic data carriers, as well as

[2] http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2007&Sort=3&nr=38779&linked=bes&Blank=1&file=dokument.pdf

seizing thereof, if it is suspected that otherwise the data may be lost. According to the interpretation of BGH, these norms do not apply to secret on-line searches. Regulations of the German code of criminal proceedings, pertaining to searches, base on fundamental pre-proceedings guarantees which cannot be fulfilled in the case of remote penetrations of computers. In the first place it is the guarantee of openness of actions undertaken by officers. During a search, the owner of the premises has the right to be present, and – in the event of their absence – their representative or an adult member of their family. Outside persons should also be present (§§105 and 106 StPO). Moreover, at the request of the interested party, after the undertaken activities have been completed, a written record of the performed activities should be made, based on which it is possible for the investigation bodies to examine legality of those actions, and, in particular whether they are stipulated by applicable law. Moreover, as BGH pointed out, under the applicable StPO regulations, the examining judge might not order a secret search which would exclude the protection guarantees stipulated by §§105 and 106 StPO. The Tribunal also stated that secret on-line searches could not be governed by the regulations of §100a and the subsequent StPO related to the monitoring of telecommunication. These regulations provide for this measure being ordered only upon suspicion of committing particularly serious crimes. That is why application of such searches is subject to highly restrictive and tight formal requirements. In addition, the very disposition of this rule diverges from the aim of secret on-line searches. Disposition of the norm stipulated in §100a of StPO refers to the control of communication between the suspect and a third person, whereas the goal of the ordered search of a computer serves achievement of other results. Hence, the German Federal Tribunal's judgement leads us directly to a finding that the applicable regulations of the German criminal procedure have not created any legal framework for new investigation instruments, based on such spyware as, for instance, a Trojan horse.

The judgement of the German Federal Constitutional Tribunal [Bundesverfassungsgericht, hereafter referred to as "BVG"] of 27 February 2008 on 1 BvR 370/07[3] and 1 BvR 595/07 also constitutes interesting contribution to the public debate in Germany concerning the legal framework of remote searches. The Tribunal examined compliance of the regulations governing on-line searches applicable in the *Land* of *North Rhine-Westphalia* (Nordrhein-Westfalen) with the constitutional patterns contained in the German Constitution Act [Grundgesetz, hereafter referred to as "GG"]. In particular exam-

[3] http://134.96.83.81/entscheidungen/rs20080227_1bvr037007.html

ination of BVG related to the norms in art. 2 § 1 GG [protection of personality development], art. 1 § 1GG [protection of human rights] as well as art. 10 GG [secrecy of correspondence] and art. 13 GG [home inviolability].

Pursuant to art. 2 § 1 GG every individual has the right to unhindered personality development, as long as it does not infringe rights of third parties, and if it is not in contradiction with the constitutional order and moral rights. According to art. 1 § 1 GG, human dignity is inviolable, and the state authorities are obliged to respect and protect it. The regulation in art. 10 GG refers to secrecy of correspondence. According to its disposition, secrecy of correspondence, as well as secrecy of letters and parcels, or communications, is also inviolable. Limitations in this respect must result from statutory regulations. If such limitations serve the protection of free, democratic constitutional regime or existence or protection of the Republic or a state, the Act may stipulate that they shall be applied without the interested party's knowledge, and that instead of legal course consequent control shall be implemented and conducted by democratically established authorities and auxiliary organs. Pursuant to art. 13 GG, inviolability of apartment is guaranteed. In particular, searches may be ordered by a judge, and in cases of the utmost urgency, also by organs prescribed by statutory law. Searches must be conducted in a form dedicated to achievement of that goal. If particular facts ground an assumption that a crime has been committed, which is stipulated by the Act as particularly serious, it is allowed, based on a judge's instruction, and in order to pursue the perpetrator, to reach for technical means of acoustic monitoring of an apartment which is believed to be the suspect's current whereabouts, provided that examination of a given case otherwise would be disproportionally hindered or objectless. Such measures must be limited in time. The order must be issued by the panel composed of three professional judges. In the most urgent cases it is enough if such an order is issued by one professional judge. To repel a direct and inevitable danger to public security, in particular public danger or danger to life, it is allowed to use technical means to monitor premises only based on a court order. In cases of the utmost urgency, such measures must be ordered also by other organs prescribed by statutory law. In such an event they must be confirmed by a court warrant issued forthwith. In the remaining cases intervention and limitations may be applied only to repel public danger or danger to life, as well as based on regulations of the act, for protection against a sudden threat to security and public order. The aforementioned provisions of the German Constitution, in particular art. 13. clearly stipulate that a measure in a form of home search may be deployed only on

an exceptional basis, and it is hedged with tight procedural requirements intended to protect citizens against unfounded interference in their fundamental entitlements subject to legal protection, such as the right to privacy, dignity and inviolability of secrecy of correspondence or domestic peace.

In its judgement, BVG decided in particular that the constitutional guarantees of art. 2 § 1 in relation with art. 1 part. 1 GG, with respect to personal rights include also confidentiality of correspondence and integrity of teleinformation systems. Secret infiltration of the information system which is used to monitor the system and which enables searching through contents of data carriers is, under the Constitution, acceptable only if there is actual evidence supporting the existence of specific threat to an essentially important entitlement subject to legal protection. As essentially important entitlement subject to legal protection are deemed corporeal inviolability, human life and freedom or general values, the existence of which relates to the grounds of existence of the state or its citizens. These measures may be deemed legally founded if there is a justified probability that the threat or danger will emerge in the near future, or if certain facts indicate a threat to an essentially important entitlement subject to legal protection, that might be posed by specific individuals. Secret infiltration of teleinformation system must be, in principle, conducted on the basis of a court order. The act which allows application of such measure must additionally include arrangements to protect the essence of private life. That is why legal admission of application of remote searches requires, as assumed by BVG, amendments to articles 10 GG and 1 GG.

The German Federal Constitutional Tribunal made a reference indirectly to the principle of proportionality and adequacy. It recognised that application of investigation measures which interfere in privacy so drastically, such as remote search of computers, may be performed only when this appears to be the only method which may effectively eliminate threats to essentially important entitlements subject to legal protection. Therefore, searches online must constitute an exceptional measure justified by reasons of supreme significance. With reference to the proportionality and adequacy principle, I believe that it is worth discussing the argumentation presented by the German government to a question presented during the parliamentary question time with regard to remote searches.[4] The government's reply clearly indicated that in the period of two years (2005–2006) examining judges issued only four decisions ordering remote searches of computers. Simultaneously, the government did not see any possibility to assess the number of such

[4] http://dip21.bundestag.de/dip21/btd/16/039/1603973.pdf

searches in the future, but was able to present costs of infrastructure investments reaching EUR 200 000. What is really important, and what in my opinion, puts under a question mark the need for introduction of so radical measures, is the fact directly confirmed by the German government - that out of the four described cases of ordering remote searches of computers, none had been ordered due to the necessity to directly repel a threat.

The consequence of BGH's judgement dated 31 January 2007 on StB 18/06,[5] as well as of BVG's dated 27 February 2008 on 1 BvR 370/07 was the commencement of legislative works with a view to establish special legislation for the purpose of remote searches. Due to the lack of political consensus, it is difficult to predict in what form new legal regulations will come into force. It appears that the new German law will allow usage of remote searches of suspects' computers. Each time, application of such measure will have to be accepted by an independent judge. Moreover, also the manner of using data obtained as a result of such search will have to be each time specified in a court decision. That requirement is intended to protect privacy of citizens against arbitrariness of law enforcement bodies. Additionally, the entitlement to apply for court approval for usage of spyware in order to perform a remote search will be limited to cases in which there are suspicions of terrorism.[6]

It is also likely that under the Polish constitutional norms, in particular art. 47 of the Constitution of the Republic of Poland which guarantees the legal protection of private life to every individual, as well as art. 49 relating to the freedom and protection of secrecy of communication, the situation might be settled analogously as in German law. These guarantees will be strengthened by the regulation in art. 51 § 2 of the Polish Constitution, under which public authorities may not acquire, gather or make available information of the citizens other than such as is necessary in a democratic rule of law. Additionally, in its decision dated 26 April 2007 on case I KZP 6/07[7], the subject of which was, among others, interpretation regulation art. 19 of the act on police, related with police operational activities, including bugging telephones also the Polish Supreme Court, and the Criminal Chamber composed of seven judges, directly stated that the norm unquestionably entered the sphere of constitutional civil rights and liberties, in particular the protection of private life, freedom of communication and the right of protection of home inviolability. This statement proves that ordering applic-

[5] http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2007&Sort=3&nr=38779&linked=bes&Blank=1&file=dokument.pdf

[6] Analysis as at December 2008 after rejection by Bundesrad a draft act on Bundeskriminalamt.

[7] http://www.sn.pl/orzecznictwo/uzasadnienia/ik/I-KZP-0006_07.pdf

ation of operational activities which interfere in privacy, such as bugging telephones or provocations, may be applied on an exceptional basis, only if there is a suspicion of committing the most serious crimes by specific persons, enumerated in art. 19 § 1 of the act on police. Therefore, in my view, also under Polish law, law enforcement bodies could not use modern operational techniques based on technologies such as "sniffer", "Trojan horse", or "keylogger", without special relevant legislation, and perhaps even with no appropriate amendments to the Polish Constitution related with the protection of privacy, secrecy of communications and inviolability of domestic peace.

That is why, I have come to a conclusion that nowadays, when a large part of our life activity has been moving to the virtual world, it is necessary to develop tools supporting bodies of legal protection in the Internet environment. Such instruments may not, however, be used without deep reflection and wide debate over their technological potential, as well as threats which they may bring for the basic human and civil rights. I believe that increased awareness in this respect and an open discussion may lead to a compromise between criminal law effective in the online environment and criminal law respecting all constitutional norms, as well as to definition of rational legal framework needed modern technology used to protect security of citizens.