Powers and Fundamental Rights in Cyber Security

Riitta Ollila

Abstract Protection of privacy and confidential communications are crucial fundamental rights in cyber security. The protection of privacy and confidential communications are twofold in the meaning that active security steps in communications may require interference with confidential communications. The detection and profiling of potential threats may raise suspects on innocent participants of communications. The NCSC-FI inside the Communications Authority has the initial task and powers to monitor the cyber security. The bill for the Code of Information Society introduces new obligations for information security and preparation for emergency situations. If new powers will be granted to authorities they must narrowly tailored and limited to the necessary measures. The interference with confidential communications in information retrieval requires legal remedies against misuse of powers and constitutional accountability of security authorities.

1 Introduction

The threats in cyber space have developed from hacking activism to crimes and espionage. Cyber terrorism and cyber warfare are escalations of threats. The powers of authorities to observe the threats in cyber space are still based on powers of crime investigation and powers of communications authority in information security supervision. These powers rest on detecting specific crimes and security threats in communications networks. The cyber security is not a legal concept as such and it does not mean extra powers to authorities. The powers of authorities must be based on existing legislation. If the threats escalate to massive attacks that risk the vital functions in society the powers to individual crime investigation are not perhaps sufficient.

R. Ollila (✉)
University of Jyväskylä, Jyväskylä, Finland
e-mail: riitta.h.ollila@jyu.fi

M. Lehto and P. Neittaanmäki (eds.), *Cyber Security: Analytics, Technology and Automation*, Intelligent Systems, Control and Automation: Science and Engineering 78, DOI 10.1007/978-3-319-18302-2_4

The National Cyber Security Centre Finland (NCSC-FI) has been established within Finnish Communications Regulatory Authority (FICORA) since 1st of January 2014. The NCSC-FI continues previous activities of CERT-FI within the FICORA. The NCSC-FI prepares guidance and agreements concerning national security activities and the handling of international classified information. The NCSC-FI will monitor cyber security threats of national interest and produce advanced situation awareness services to its constituents. To facilitate that, the NCSC-FI collects and correlates information from a variety of sources.

The establishing of NCSC-FI has been based on government resolution 24.1.2013 concerning cyber security strategy. The activities of the centre have been manifested on the programme of the centre. According to the Article 119 of the Constitution Act the powers of public authorities must regulated by an act of Parliament if they use public power in the meaning that they decide the rights of individuals. The question follows that does NCSC-FI use public power and does it interfere with constitutional rights of individuals? The activities of NCSC-FI rest on the powers prescribed in the Act on the Protection of Privacy in Electronic Communications. However, the powers rest on the previous CERT-FI activities and the act has not been amended to introduce new powers to NCSC-FI activities.

The powers of police aim on crime investigation and prevention of disorder and crime. In cyberspace and communications networks those powers are exercised by intercepting phones and messages and monitoring subscriber data. The general observation of cyber space is approved for the purpose of threats and prevention of criminal activities. The use of the observation data is possible for the protection of national security and for the prevention of crimes and immediate dangers to public security.

The Finnish security intelligence service and military service have no right to general and unlimited surveillance in cyber security. The Department of Defence has set up a working group for preparing legislation concerning powers in cyber security and interference with fundamental rights of individuals. I examine the existing powers of authorities in cyber security and needs for amendments in legislation. The prevention of infringements and damages are primary purposes for cyber security surveillance and not the breaches of fundamental rights of ordinary people. However, the temptations to use data for other possible purposes are alternatives if surveillance authorities get masses of personal data. I examine the obvious risks and safeguards against misuse of personal data.

2 Constitutional Protection of Personal Data and Confidential Communications

The privacy and protection of personal data must be considered in circumstances when data refers to natural persons. Article 10 § of the Constitution Act specifies the protection of personal data: “More specific provisions on the protection of

personal data shall be prescribed and specified by an Act of Parliament". The bases for the processing of personal data must prescribed by law. The Constitutional Committee is the committee in Finnish Parliament that interprets the constitution. The Constitutional Committee has regarded that the purpose of processing and the content of data, the further processing of data including deliveries of data and the legal safeguards of the data subject must be prescribed by law.

The Constitutional Committee has developed the following principles of interpretation in its practice:

1. The basis of the filing systems must be prescribed by law in details. The period of storing and the removal of personal data cannot be prescribed on the level of administrative decrees inferior to acts of Parliament (PeVL 7/1997 and 11/1997)
2. The data subjects must have legal safeguards. The safeguards might vary from the data subject's right of access to the Data Ombudsman's right of access whether the data relating to him are processed and whether the processing fulfils the conditions prescribed by law (PeVL 7/1997).
3. The processing of personal data of public authorities must be based on justified reasons (like crime investigation, PeVL 7/1997)
4. The prescribed-by-law requirement is followed by the requirement of accuracy. "The pressing reasons" are not adequately accurate if they have not been concretized at the level act (PeVL 27a/1998).

The Constitutional Committee has considered in its practice that wide and non-specified access to personal data justified on the necessity reasons for the activities of authority are problematic. According to the Data Protection Act, purpose specification and duty based on law are general conditions for the processing of personal data in activities of authorities. Is purpose of the authority enough for the processing if the authority does not deal with personal data on the consent of the person concerned? If the authority collects information related to individuals it interferes with private life or confidential communications of individuals protected in the Article 10 of the Constitution. The interference with those fundamental rights should be based on justified reasons and should be prescribed by law.

The purpose specification, data quality principles and general legitimacy conditions of processing are the crucial conditions for the disclosure of personal data. All these conditions must prevail and the disclosure must be compatible with the purpose. The special categories of processing have their own special conditions for processing. I have scheduled all the conditions of disclosure in a chain in which the purpose specification and data quality principles must always be fulfilled, but the legitimacy conditions and special categories of processing have their own alternative paths (Table 1).

The general legitimacy conditions and special categories of processing form each of them special paths and categories of processing (Ollila 2004). If there is no consent or contract to the processing of personal data it must be based on legal obligation of the authority. Purpose specification is the prevailing condition for processing of personal data but it must be regulated by law or by consent. If the

Table 1 The purpose specification, data quality principles and general legitimacy conditions of processing

Purpose specification	Data quality principles	Legitimacy conditions of processing
• Adequate • Relevant • Not excessive • Accurate • Up to date	• Consent • Contract • Legal obligation • Vital interest • Client, employee, member • Merger • Payment service • Public service • Permission of the data board	• Sensitive information • Scientific • Historical • Statistic • Credit information • Who is who records • Genealogy • Direct marketing

authority does not have direct relationship with the customer in administrative matters, the conditions for the processing of personal data must be prescribed by law.

The conditions for interference with confidential communications have been prescribed in Article 10 § 3 of the Constitution Act. In criminal investigation necessary restrictions may be provided by an Act of Parliament in the investigation of offences that endanger the security of an individual, society or home. In legal proceedings and in security checks and during deprivation of personal freedom the restrictions must be prescribed by an Act of Parliament but there are no conditions for the quality of the restrictions and offences.

The protection of confidential communications can be divided in the vertical relationship between the state and the citizen and in the horizontal relations between private participants. In the vertical relationship between the state and the citizen the main issue is the restraint from the interference by the state with private communications and the justifications for interference. The restraint from interference conforms to respect for the confidential communications. The crime investigations and legal proceedings are the main reasons for interferences with the secrecy of communications.

In horizontal relations between the participants and service providers of the communications, the main issue is the protection of confidentiality against violations of others and the security obligations of the service providers to guarantee the confidentiality of the communications. The protection of confidentiality in horizontal relations requires active safeguards and legislation from the state to prevent the violations and to impose on security standards for the confidentiality. The telecom operators are obliged to take care of the security in their networks.

The protection of privacy and confidential communications are twofold in the meaning that active security steps in communications may require interference with communications (Ollila 2005). The detection of threats requires identification of those participants who threaten communications. The profiling of potential threats may raise suspects on innocent participants of communications.

3 The Powers of Communications Authority

The Finnish Communications Authority carries out general supervision and powers based on the Act on Protection of Privacy in Electronic Communications. It collects information and investigates violations and threats to information security in communications networks and services. The NCSC-FI agency carries out the data security tasks inside the communications authority. NCSA-FI specialises in information assurance matters in cases concerning technical information security and the security of telecommunications. The NCSA-FI is one of national security authorities besides the Ministry of Defence, the Defence Command and the Finnish Security Intelligence Service. The Ministry of Foreign Affairs acts as leading National Security Authority in implementing international security obligations.

The NCSC-FI has access to the identification information of subscribers in the context of vulnerabilities of communications and data offences. This right covers both the metadata and the content of telecommunications. The NCSC-FI does not need any consent of court for these surveillance activities. The absence of legal remedies has been justified on the reason that NCSC-FI receives only IP-addresses of data and they do not deliver the data to other authorities. They do not process personal data.

4 The Activities of NCSC-FI

- Reports from telecom operators and other enterprises obliged by law
- Surveillance of public sources in traditional and social media and rumours
- Networks of data exchange in autoreporter and Havaro programs
- Analysing data

According to the Article 20 of Act on Protection of Privacy in Electronic Communications, the measures for information security include powers:

Measures for maintaining information security may include:

(1) Automatic analysis of message content;
(2) Automatic prevention or limitation of message conveyance or reception;
(3) Automatic removal from messages of malicious software that pose a threat to information security;
(4) Any other comparable technical measures.

The automatic analysis of message content means that no natural person reads the content. If the contents of a message have been manually processed, the sender and recipient shall be informed of the processing.

The powers prescribed in the Article 20 are proposed to be granted to all telecom operators and service providers according to the Information Society Code bill. The telecom operators and service providers will have similar powers than the Communications Authority for necessary measures to maintain information

security. The telecom operators and service providers shall have powers to process identification information for information security purposes.

The telecom operators and service providers are obliged to inform the communications authority about security violations. The NCSC-FI deals with those reports and it has entitled to access any identification data, location data or messages for the carrying out of its duties if the data is necessary for clarifying significant violations or threats to information security. The NCSC-FI shall destroy any information and data when this information is no longer necessary for carrying out its duties or for any criminal case concerning the information.

The subscribers and telecom operators are entitled to fight against malicious messages and programs in order to prevent damages. Those malware programs and malicious messages as such do not belong to the protected confidential communications and freedom of expression. Subscribers have the right to process their own data in order to prevent malware programs and viruses.

The analysis of public websites and social media is open to everyone and even for authorities. Do the authorities process data in the meaning of data protection law if they copy and store the public data for future purposes? This retrieved content contains personal data if any of the source web pages do. The authority can observe the changes of the web page by retrieving successive source web pages and analysing changes of the content. According to the program of NCSC-FI, enriching public data with confidential data and combining and processing data from different public sources means processing personal data if the data can be connected to individuals. The operation of search engines has been analysed in the opinion of Advocate General Jääskinen delivered to the European Court of Justice in Google Spain judgement.

Second, the search results displayed by an internet search engine are not based on an instant search of the whole World Wide Web, but they are gathered from content that the internet search engine has previously processed. This means that the internet search engine has retrieved contents from existing websites and copied, analysed and indexed that content on its own devices. This retrieved content contains personal data if any of the source web pages do.

If the Google search engine can retrieve contents from existing websites and index that content on its own devices, it is hard to deny similar activities for domestic authorities. However, any further processing of personal data remains under domestic data processing law and European data processing directive. The European Court of Justice has considered in case C-73/07 that the clipping archives of media including already published material remain under data processing directive. Compared to public websites this could mean that public websites are like clipping archives in the further processing of personal data.

5 The Powers of Police in Cyber Space

The powers of police rest on coercive means legislation for detecting crimes that already have happened. Typically the police inspect computer breaks-in, cyber fraud, communications disturbing and espionage through communications systems. The powers for surveillance to detect threats and prevent crimes rest on the general powers of police legislation. The powers for monitoring and processing data from public sources and web pages rest on general powers of police legislation. The conditions and permissions regulated in the Coercive Means Act shall not be applied to surveillance of public sources. The interception of phones and messages means interference with confidential parts of communications. The surveillance of openly available parts of messages does not mean interception in the meaning of Coercive Means Act. According to Article 23 in Chap. 10 of the Coercive Means Act, the surveillance of computer and its contents means interference with secret parts of it. The permission for surveillance is not needed for physical surveillance and processing of data obtained from public sources. However, the act on processing personal data in police activities shall be applied to all processing of personal data concerning natural person.

6 The Powers in Escalated Threats

The NCSC-FI inside the Communications Authority has the initial task to monitor the cyber security. The NCSC-FI will monitor cyber security threats of national interest and produce advanced situation awareness services to its constituents. However, the powers in situations where the cyber threats escalate to massive attacks that threaten the communications infrastructures and critical physical infrastructures have not been regulated by law. The bill for the Code of Information Society includes obligations for information security and preparation for emergency situations. The bill is under consideration in Parliament in 2014.

The bill for the Code of Information Society requires every telecom operator and service provider to take measures for information security of their services. The telecom operators and service operators have similar powers than the Communications Authority to automatic analysis, prevention and removal of messages that may include malicious software. They must report the threats to information security they have identified to Communications Authority. They must report the vulnerabilities of their services to their subscribers and other clients if the vulnerabilities cause serious threats to their services.

The telecom operators and the possessors of radio frequencies are obliged to make plans for preparation to emergency situations. The Communications Authority has powers to impose more precise regulations on those preparation plans. The telecom operators must take care that the control and maintenance of their critical communications infrastructures can be restored to Finland in

emergency situations. The proposals in the Code of Information Society bill increase requirements for preparation for crisis and emergency situations.

The Emergency Act requires military attack or threat of a military or corresponding attack that endangers the vital functions of society in order that the government can take granted those emergency powers. In cyber attacks the distinction between military attack and escalation of cybercrimes is not visible and clearly observable as in traditional military attacks. The Emergency Act requires that authorities use those emergency powers in proportionate manner for only necessary purposes.

The Ministry of Defence has ordered a working group to consider the powers of security authorities for the implementation of Cyber Strategy and obvious needs for new legislation. The working group considers if it is necessary to grant new powers for security authorities in information retrieval. Those powers must be balanced in relation to obligations running from constitutional and human rights. The interference with confidential communications in information retrieval requires legal remedies against misuse of powers and constitutional accountability of security authorities. The constitutional and human rights must be guaranteed in cyber space and information society.

References

Committee for Constitutional Law, Finnish Parliament (2012) Perustuslakivaliokunnan lausunto PeVL 18/2012 vp–HE 66/2012 vp

European Court of Justice (2013) Opinion of Advocate General Jääskinen delivered on 25 June 2013: Case C–131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, section 34

Judgement of the Court (Grand Chamber) 16 December 2008 Tietosuojavaltuutettu (Data Ombudsman) v. Satakunnan Markkinapörssi Oy and Satamedia Oy (Directive 95/46/EC–Scope–Processing and flow of tax data of a personal nature–Protection of natural person Freedom of expression), Case C-73/07

Ollila R (2004) Freedom of speech and protection of privacy. PhD thesis, Edita Publishing Oy, Helsinki. http://www.edilex.fi

Ollila R (2005) Turvallisuus ja urkinta. Lakimies 5(2005):781–791