Telecom Operator's Incident Investigations

Conny Larsson

1 Introduction

The importance of telecommunications has increased rapidly during the last decades. It is not long since telecommunication was limited to traditional telephone calls; telefax etc and first in the 1980's mobile telecommunication began to be generally available to the public. This development has provided new and varying forms of telecommunication systems and services. Additionally there are an increasing number of users. It is indicated that there are more than 5,5 million subscribers in the Swedish fixed-wire network,10 million subscribers in the mobile telephone network and 3,5 million subscribers with Internet access.[1] It is suggested that the Telecom Company TeliaSonera[2] on a daily basis transfer more than 50.000.000 electronic communications through TeliaSoneras' telecom network in Sweden.

Furthermore it has become more and more important for the authorities involved in investigating crime to get access to different kind of information and the development within the IT-field leads to new and changed conditions for the use of interlocutory measures.[3] As an example of the new and changed technical conditions the use of cell phones makes it possible to establish where a certain phone has been located in a limited geographical area at a certain moment.[4] The developing technology will provide information, positioning data, which enable the Telecom Companies to closely establish addresses or other defined areas where the user of the phone is present at the moment. From a crime-investigating viewpoint a lot of useful information can be found in the Telecom Companies' and other service providers' information systems. This information can in different ways serve as evidence for the activities and who is to be held responsible.[5] The information is normally stored for some time in the telecommunication network, or can at least be traced in the network. Information on telephone calls - such as time and duration of a certain call and the phone-numbers involved - can be accessed in the systems. Activities on the Internet will normally involve the telecommunication network, which means that information on IP-addresses that have been involved may be found in the systems. It must be kept in mind that the information doesn't point out the actual perpetrator, but only the actual connections. Additional investigation is necessary in order to reveal individuals.

Telecom Companies are subject to special regulations, such as the Swedish Telecom Act (1993:597) (TL), which in 2003 was replaced by the Swedish Act (2003:389) on Electronic Communications (LEK). In accordance with LEK the regulations also apply on other major service providers within the field of electronic communications. These acts are corresponding to EU-directives, such

[1]1 SOU 2007:76 p. 109.

2 TeliaSonera is a result of the merging between the Swedish Telecom Company Telia AB and the Finnish Telecom Company Sonera o/y.

3 Ds 1995:48 p. 10 ff, 19 ff, prop. 1994/95:227 p. 7 f and 15 ff, prop. 1995/96:180 p. 7 ff, SOU 1992:110 p. 127 ff, prop. 2002/03:74 p. 31 ff, SOU 2007:76 p. 129 ff.

4 SvJT 8/92, p. 534.

5 Lloyd, IT-law, p 264 ff.

as the directive 2002/58/EC of 12 July 2002 on Privacy and Electronic Communications which means that similar legislation applies within the EU. TL was corresponding to the directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

LEK establishes the situations in which the Telecom Companies are entitled to handle information on subscribers and information on telecommunications ("traffic data") as well as the conditions for handling such information.[6] Such information handling is essential for the performance of the telecom services and for invoicing the subscribers for their use of the services and to provide the subscribers with call specifications etc. The right to handle the information is also of great importance for the security measures needed to protect the telecom network, the services, the subscribers and the users, and – of course – for the Telecom Companies crime-investigations in their networks and systems.

In 1996 an amendment to TL obliged the major Telecom Companies to technically adapt their systems to enable and facilitate the carrying out of interception of communications and provision of call-associated data in accordance with the Swedish Procedural Act (RB), here referred to as legal interception.[7] In November 2001 the Convention on Cyber Crime, was ratified by Sweden. This convention holds an obligation to store information, including historical data, for the authorities' crime-investigation.[8] The obligations raise some interesting questions, not only from a legal point of view but also from a technical and financial perspective. For instance, how can it be assured that the telecom systems and technology used by the authorities will be able to communicate and that the information can be provided in accordance with the law and properly considering the security, secrecy and integrity aspects? In addition, is it reasonable that the Telecom Companies shall bear the costs for the measures that are necessary to fulfil the obligations?

2 Telecom Companies' Right to Perform Crime-investigation Activities

The Telecom Companies are allowed to handle traffic data to prevent or detect unauthorized use of the telecom network and the services, here referred to as the Telecom Companies' crime-investigating activities.[9] Besides that the companies are obliged to take such measures that are necessary for the security in their network and also to take reasonable measures for protecting the information handled by the companies.[10] If the crime-investigating activities are necessary for protecting the network and the services, it can be argued that the Telecom

6 LEK 6:5-8, Directive 2002/58/EC, Article 6 and 15.1.

7 17 § TL, LEK 6:19, Directive 2002/58/EC, Article 15.1, RB 27:18-19.

8 Convention on Cyber Crime, ETS No. 185.

9 LEK 6:8 p.3, Directive 2002/58/EC, Article 15.1.

10 LEK 6:3, Directive 2002/58/EC, Article 4.1.

Companies not only are allowed to handle the information, but also that they are obliged to do so.

Information on subscribers and traffic data handled by the Telecom Companies can also relate directly or indirectly to an identifiable natural person. Such information may be regarded as personal data according to the directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and PuL.[11] The use of such information for crime-investigating purposes may then be in conflict with the personal data legislation, while the information may be processed for such purposes according to the telecom-legislation. This conflict may be solved in different ways. The personal data legislation may overrule other legislation concerning data processing because this is expressively stipulated or is in accordance with legal principles. On the other hand the telecom-legislation may overrule the personal data legislation. This could be the case because this is expressively stipulated or because the telecom-legislation is more specialised (the principle of *lex specialis*). The conflict between these regulations is expressively handled in the Directive 2002/58/EC and LEK so that the telecom act will prevail.[12]

With regards to PuL the Telecom Companies are not allowed to keep their own crime registers. In accordance with PuL *personal data* may only be handled when the data relates to a certain case and must be removed when the case is closed.[13] Therfore the Telecom Companies must conduct their crime-investigating activities in accordance both with LEK and PuL. This can be rather tricky, especially when the investigation demands a lot of information being handled for a longer time.

The question of which law will overrule the other can also cause a conflict between the different supervisory agencies, such as the Swedish Post- and Telecom Agency (PTS) and the Swedish Data Inspection Board (DI) when supervising the Telecom Companies handling of traffic data that also contains personal data. The outcome of such simultaneous supervision may as well be that one of the authorities decides that the information handling is correct; while the other finds that it is not. The involved Telecom Company will then find itself regarded as "innocent and guilty at the same time", a situation that can be looked upon as somehow contradictory. Therefore these authorities co-operate to avoid such conflicts.

It can always be discussed in what extension and for what purpose the Telecom Companies should be allowed to keep the actual information. In every situation this will actualise the balancing between the individual rights on privacy and the public interest in effective crime investigating. The Directive 2002/58/EC as well as the Swedish LEK allow such processing of data that is necessary for the purpose of protecting from, discovering and act upon unauthorised activities on the telecom-network. This enforces the member-states to allow the Telecom Companies to store call-related data and other information

11 Directive 95/46/EC, Article 2 a), 3 § PuL.

12 Directive 2002/58/EC, Article 1.2, LEK 6:2.

13 21 § PuL.

for that purpose. Therefore the Telecom Companies have a good chance to trace the origin of an unauthorised activity in the network or in the systems. However, traffic data may not be kept for an unlimited period of time. According to LEK and the governmental bill relating to LEK, data may be stored for at most one year for crime investigating purposes. Additionally the Telecom Companies must especially authorize the personnel that handle the information, which indicates that such tasks may only be carried out by a limited number of individuals at the companies.[14]

The Telecom Companies' right to perform the investigations is also founded on the general terms and conditions which are applicable towards the subscribers. These terms and conditions often give the companies the right to close the subscriber's connection or even to cancel the actual contract if the connection is used for unauthorized purposes.[15] When the actual connection is located in another operator's network, the general terms and condition of the Telecom Company does not apply on the actual subscriber. In this case the company cannot itself take actions against the other operator's subscriber, but must turn to the other operator and request for assistance. Therefore it is in the Telecom Companies' interest to agree upon procedures regarding how to handle such situations and to co-operate in matters regarding unauthorized activities in their networks.

Compared with the procedures that follow criminal law, these contractual measures give certain advantages. First, it will not be necessary to find a certain perpetrator. Second, the actual evidence must not be as strong as required in a criminal case. It will be sufficient if the Telecom Company can prove that a certain connection has been used for unauthorized activities and that these activities have not stopped after the subscriber being informed. These procedures have shown effectiveness according to information from the Telecom Companies. Third, it doesn't matter if the actual connection belongs to a subscriber in another country. The Telecom Company can turn directly to the company in the other country without having the investigation delayed in the same way as a border-crossing crime investigation carried out by the police.

3 Telecom Companies' Crime-investigation and Telecom Secrecy

The handling of traffic data can also be questioned from another perspective. Traffic data is protected by telecom secrecy, which can be an obstacle for the Telecom Companies to handle such information. This may have an impact when the Telecom Companies wish to assist external subjects that have been victimised by a crime, with providing them with information necessary for taking action against the crime.

However, the telecom secrecy does not apply with regards to subjects that have participated in the actual communication or to the actual subscribers. In

14 Directive 2002/58/EC, Article 15.1, LEK 6:8.3, prop. 2002/03:110 p.259 f. and 392.

15 E. g. TeliaSonera *General Terms and Conditions*, sections 4.1-2 and 7.1.

almost every case some of these subjects are concerned. Therefore the Telecom Companies normally can assist the victims in a crime investigation by providing them with the actual information without breaking the telecom secrecy.[16]

It may be the case that the Telecom Company finds that it should report the actual incident to the police and that providing the police with call specifications containing traffic data would be necessary for a successful police investigation. Due to the fact that such information is protected by the telecom secrecy, the Telecom Company cannot provide the information to the police without approval from the subject protected by the secrecy. Such approval will not be necessary in a case where the actual crime is of a certain severity. At the request from a crime investigating authority the Telecom Company then will be obliged to provide the information according to LEK.[17] In addition the crime investigating authority can be entitled to the information by an interlocutory measure, such as legal interception.

4 Telecom Companies' Security Measures

As mentioned before, the Telecom Companies are obliged to take such measures that are necessary for the security in their network and also to take reasonable measures for protecting the information handled by the companies.[18]

The Telecom Companies have taken security measures of different kinds, technical as well as organizational. Relating to telecommunications and telecom networks, the companies have installed locks and alarms on stations, junctions, cables and wires etc in the fixed telecom network. In the mobile telecom networks there are measures like the identity system, encryption of signals and other registers such as the EIR (Equipment Identity Register). Some telecom operators have installed certain warning systems such as FDS (Fraud Detection System) and EWS (Early Warning System). These systems react upon different signals from the telecommunication systems and will alarm on certain conditions, such as abnormal quantity of calls or calls from or to a certain telecom address. There are also systems that may be programmed to react in a certain way upon certain signals, FCS (Fraud Control System). In addition security codes may be installed in certain equipment, such as the GSM mobile telephones.[19]

With regards to computer communications different kinds of security systems, security programs or security functions can be installed, such as password systems, encryption, firewalls etc. There are also more traditional

16 Directive 2002/58/EC, Article 5.1 and 15.1, LEK 6: 20.

17 LEK 6:20, prop. 1992/93:200 p. 310.

18 LEK 6:3, Directive 2002/58/EC, Article 4.1.

19 Borgström, Lindborg, *Säker data- och telekommunikation*, p 77, 84 ff, Grabosky, Smith, *Crime in the Digital Age*, p 79 ff.

ways of handling the security problems, such as locks and alarms protecting localities where the equipment is placed, access control systems etc.[20]

The Telecom Companies are obliged to inform their subscribers on certain risks, such as unauthorized access etc. relating to the security within the networks and services. Therefore the companies should inform the subscribers on for instance the need to encrypt information transmitted through the Internet or on the cell phone network.[21]

5 Telecom Companies' Crime-investigation in Practice

The Swedish Telecom Companies have specialized personnel or other entities working with security issues which also includes handling incidents in ways that can be regarded as crime investigation. These entities are performing technical investigations within the telecom network, the services and the information systems. The Telecom Companies also co-operate in matters concerning preventing, detecting and acting on unauthorized activities in their networks and services.

The subscribers and the public can report incidents to the Telecom Companies, but the companies are not obliged to perform an investigation in a certain case. This means that the Telecom Companies can be forced to perform the investigation only if it is regarded as necessary in order for the actual company to fulfil its (general) legal security obligation. The investigation may engage a lot of resources at the Telecom Company, which may cause the company expenses that are not to be neglected. For these reasons the Telecom Companies may be willing to perform the actual investigation first after an agreement on payment. The investigation and the potential outcome must then be worth the efforts from the viewpoint of both the company and the subscriber or the victim.

Another way of detecting unauthorized activities is provided by security systems such as Fraud Detection Systems (FDS) or the Fraud Control Systems (FCS) installed by the Telecom Companies in the network and information systems. These security systems are programmed to react upon certain anomalies in the telecommunications, such as abnormal traffic from or to a certain telecom address, large amounts, simultaneous calls from one mobile telephone from different locations etc. After receiving signals from such systems the Telecom Company can act either immediately or after communicating with the concerned subscriber to discuss on how the problems should be properly addressed.

When the telecom operator is aware of the activity and the actual telephone numbers who are used, evidence will be secured, such as call specifications etc. There will also be an investigation regarding the geographical location of the activity. After that the case will be reported to the police, who will perform

20 Borgström, Lindborg, *Säker data- och telekommunikation*, p 149 ff, 213 ff, Grabosky, Smith, *Crime in the Digital Age*, p 79 ff.

21 Directive 2002/58/EC, Article 4.2, LEK 6:4.

further investigation, such as search and seizure, in order to secure additional evidence. In this situation the telecom operators can give valuable assistance by showing the actual equipment and other relevant objects to the police.[22]

The Telecom Companies have a similar point of view regarding what kind of unauthorized activities are most common in their networks and services and the scope of the activities. The present figures indicate that spam is among the most common problems. One problem related to spam is that it is normally originating from other countries and that spam is not subject to criminal law. Therefore it will be rather pointless to file a police report when victimized by spam. Data virus and computer related fraud is other incidents of some significance. The use of other people's identities when entering subscriptions is a minor problem, which is easily discovered and dealt with. The earlier problems with cloned mobile phones occurred in the analogue NMT-network and due to certain measures taken by the Telecom Companies these activities have more or less ceased. In addition it has not been confirmed that cloning is a problem within the digitalized GSM-network. There are some examples on intrusions in the networks and services such as data intrusion, breach of telecom secrecy etc (hacking, cracking, phreaking etc), but this is also regarded as a minor problem. Illegal content such as child pornography, unlawfully accessed material protected by intellectual property rights are now and then found in the networks and services and the Telecom Companies put a lot of efforts in keeping their networks and services clean from such material.

The conclusion on the situation is that the unauthorized activities are not a major problem for either the Telecom Companies or the subscribers. The situation is mostly under control and the companies are well prepared to see to that their subscribers are unharmed by the incidents. Nevertheless there are good reasons for the companies to pay attention to what is going on in their networks, the services and the information systems. When new services are established there are also new opportunities to commit crimes and other illegal activities, which has to be dealt with in order to protect the business and the subscribers.

The Telecom Companies also suggest that the crime investigating authorities and the courts should get more resources and competence to handle reports on unauthorized activities. Even though it in some cases may seem pointless to make a report to the police, the report will become an addition to the criminal statistics and therefore be a reason for increased resources to the crime investigating authorities. Anyway, the companies can always act in accordance with their general terms and conditions and take adequate measures against the connections that are used for the unauthorized activities. Such measures have shown efficiency in a number of cases. Border-crossing co-operation in accordance with international law can be carried out between telecom companies without considering the same kind of bureaucracy that is needed when the crime investigating authorities shall act internationally.

The passed two or three decades have shown some interesting cases where the Telecom Companies investigations have been effective. Among these cases the following are worth some attention.

22 Televärlden nr 4, 26 februari 1998.

"Cloned" mobile phones

In the end of the 1990's "cloned" mobile phones appeared. The perpetrators found out how to technically manipulate mobile phones connected in the analogue Swedish mobile telecommunication network (NMT). The manipulation caused the equipment to send false identification signals to the network that made the actual phones appear as belonging to other subscribers. This can be compared with using false number plates on a car etc. The purpose with these activities was to avoid being charged for the use of the services and the result was that the Telecom Companies billed other subscribers instead of the perpetrator. After receiving the bills the subscribers complained to the Telecom Company, who started to investigate the case. By using information in the mobile telecommunication network, the Telecom Company could find out a certain geographical area from where the "cloned" equipment was transmitting and report the information to the police. The police could then use the information to locate and arrest the perpetrators.

"Illegal Tele-Centers"

The cloned mobile phones and fraudulent subscriptions have in some cases been systematically used as an enterprise, where the perpetrator provides the public or a limited group of people with telecommunications for payment. This enterprise is called "Illegal Tele Centers" and has in some cases generated essential income to the perpetrators. A Swedish case established that the perpetrator had earned more than 800.000 SEK and he was sentenced to imprisonment for 1,5 years for fraud of the first degree[23]. The normal procedure is that the perpetrator invites the users to a certain locality, where the illegal equipment is installed. In other cases the users can call a certain telephone number held by the perpetrator, which connects the actual call to the illegal equipment. The simplest way for performing such a connection is to put the legal telephone together with the illegal one. This kind of activity is detected relatively soon, because the legal subscriber of the cloned mobile telephone will react upon the clearly abnormal bills send by the Telecom Company.

"071-fraud"

Cloned mobile phones have also been used for other kinds of unauthorized activities, such as the "071-fraud". In such a case the perpetrator entered a "071-subscription", which consisted of a certain kind of pay-call service, where the Telecom Company charged the caller a certain fee and paid another and lower sum to the subscriber of the 071-number. The perpetrator got some cloned mobile phones, which he frequently used to call his own 071-number. The total amount for these calls was more than 200.000 SEK, which was paid to him by the Telecom Company Telia AB. Because of the fact that the mobile phones were cloned, Telia AB billed the actual subscribers of the used mobile phone numbers, but couldn't get any payment due to the fact that they had been used

23 Huddinge TR, April 1997.

without authorization. The perpetrator was sentenced to imprisonment for 1,5 years for fraud of the first degree.[24]

"Carding"
Unauthorized use of other people's credit cards and credit card numbers can also be performed on the telecommunication networks as well as on the Internet. In such a case the perpetrator called a "free of charge-number" ("020-number") where he ordered connection to other phone-numbers, especially to numbers located in the USA and being subscribers to the American Telecom Company AT&T. To pay for these connected calls he used a credit card number without being authorised and AT&T couldn't charge the owners of the used credit card numbers. When performing a search and seizure in the perpetrators home the police found a list containing several credit card numbers, which was confiscated and used as evidence. The total amount for the phone calls was more than 750.000 SEK and the perpetrator was sentenced to imprisonment for fraud of the first degree.[25]

"Blue-box and Carding"
In another case of "carding" the perpetrator used certain equipment called "Blue-box". The Blue-box was used to change the signals from the actual phone so that the calls were registered as originating from another subscriber. The perpetrator also used some credit card numbers without being authorized. When the police performed a search and seizure in the perpetrators home, this equipment and a list containing credit card numbers were confiscated and used as evidence. The Swedish Telecom Company Telia AB couldn't bill the actual subscribers or the owners of the credit card numbers and suffered damage for a total amount of 26.000 SEK. At the same time and for the same reasons the American Telecom Company AT&T suffered damage for a total amount of 30.000 SEK.[26]

"The DIAB-case"
In this case the perpetrators had without being authorized got access to certain passwords, which were used to access certain computers and information systems (hacking). In addition the perpetrators called "free of charge-numbers" ("020-numbers") where they ordered connection to other phone-numbers etc. These activities were regarded as fraud, data intrusion and industrial espionage, but due to the youth of the perpetrators and that they did not have a criminal record, they only got a conditional sentence and a sentence to pay fine.[27]

"Demon Phreaker"

24 Stockholms TR, May 1995.

25 Hovrätten för Nedre Norrland, October 1996.

26 Enköpings TR, October 1996.

27 Stockholms TR, October 1996.

During the winter 1996, there was a case of phreaking, where the perpetrator was able to get access to and reveal some codes and thereby could access certain telephone numbers and communication systems. The perpetrator was a man 19 years of age, located in Gothenburg in Sweden who called himself the Demon Phreaker. He succeeded at different occasions in blocking the 911-system of Florida, USA. Thereby he hindered distress signals to be carried out through the system. During a period of six months he made 60.000 telephone calls, for a total time of 1.800 hours and amounting to nearly 2 million SEK, of course without paying. The accessed codes, telephone numbers etc. belonged to subscribers of AT&T, a telecom operator in the USA. AT&T reported the incident to the FBI, who thereafter requested for assistance from the Swedish police who contacted the Telia-group. After investigating the case, experts of Telia found that the telephone number who was initially used to conduct the crime belonged to Demon Phreaker. After performing search and seizure in the apartment of Demon Phreaker, relevant evidence was secured.

The actual case raised some interesting questions. First, it was realised that telecommunications and service have been victimised both in the USA and in Sweden, which caused jurisdictional problems. Another problem was that the experts of Telia had to present a technically complex and complicated material to persons who were in lack of adequate technical knowledge. According to US legislation the conduct was regarded as quite severe and could lead to imprisonment for about 22 years. The American prosecutor requested for extradition, but the Swedish authorities denied the request. Swedish law does not permit extradition to other than the Nordic countries or to countries within the EU. Demon Phreaker was sentenced in Sweden to a conditional sentence and to pay fine (2.000 SEK) for harassment and drug abuse (!).[28]

"Free-surfing"

The Telecom Companies have also experienced unauthorized use of different services on the Internet. Examples on such use are the activities named "free-surfing". These activities are performed on a computer connected to the Internet and by using other individuals' passwords or credit card numbers without being authorized. As described in the cases above, the Telecom Companies bill these individuals until it is detected and clarified that the use is unauthorized. In these cases the Telecom Companies could normally track the activities to a certain IP-address and to a certain subscriber. True or false, these subscribers regularly denied any knowledge of the problem. After reporting a number of such cases to the police and finding that the police were unable – or in some cases even unwilling – to take any action, the Telecom Companies instead tried to deal with the problem in accordance with their general term and conditions. The companies informed the subscribers on the terms and conditions and that there is an obligation for the subscriber to use their connections in a way that doesn't harm others. The companies also informed the subscribers that such harmful use had been tracked to their connections (IP-addresses) and that the companies would be forced to close the connection if the harmful activities don't stop. This

28 Televärlden nr 6, 26 mars 1998, Göteborgs TR.

method was found to be quite efficient and the activities ceased in almost all these cases.

The actual cases illuminates the problems connected to criminality that is conducted internationally, such as the jurisdictional issues, the evidence problems, the differing between legislation's etc.[29] It also clarifies that criminal activities targeting the telecommunication networks, the services or the information systems don't only hit the Telecom Companies, but also the innocent individuals who dispose the phone numbers or other identifications that are used for the activities. The material is often complex and complicated to understand, which actualise the need of experts taking part in the trials. In addition the trials rarely lead to sentences to major imprisonment, which indicates that the present cases hardly deter the perpetrators from continuing their activities.

6 Telecom Companies as Witnesses or Experts in Court

When employees at the Telecom Companies appear in court to describe the technical conditions in an investigation it is discussed if they are appearing as witnesses or as experts. According to Swedish law the difference between a witness and an expert is that the witness has made a unique observation and cannot be replaced by another person, while the expert is a person with a certain competence who can be replaced by a person with the same competence.

In most of the cases the employees appear in court to describe the functionality of the networks, the services or the information systems. In these situations they are normally not there to describe a certain observation or event. Nevertheless they are frequently called upon as witnesses and not as experts. Every individual that is present in Sweden is obliged by law to testify in court and if the actual person refuses to appear, he or she can be fined or even collected by the police to be presented in court.[30] A person cannot be forced to accept the task of being an expert. This task is based upon a voluntary agreement and the expert is entitled to "reasonable" payment for the work.[31] A witness is only entitled to a quite limited payment for its expenses.[32] This indicates that the authorities have a financial incitement to define the person as a witness instead of as an expert. In addition the Telecom Company cannot provide an employee that is more suitable or competent to give a correct statement if another employee is called upon as a witness. The possibility to replace the witness with another person could be valuable e.g. in a situation where the actual employee is threatened and frightened to testify.

7 Conclusion

29 SOU 1992:110 p. 144 f, 335 ff.

30 RB 36:1.

31 RB 40:4 and 17.

32 RB 36:24.

The importance of telecommunication and IT

The use of IT and telecommunication is increasing rapidly. This is shown by the number of users, the internationalisation of the communication systems, the expanding ways of using the technology etc. Unfortunately this also provides new possibilities and incitements for conducting crime.

The spreading and the development of IT and telecommunications make the technology more and more complex and complicated. This leads to the need of increasing competence. The experience of the Telecom Companies indicates that the criminals will be in possession of increasing technical knowledge, which makes it necessary for investigators, experts of the police, prosecutors and judges etc. to keep up. Without adequate knowledge on the technology, how the networks, the services and the information systems work, it will be almost impossible to realise and explain how a crime has been conducted, what information can be used for evidence and how the actual information can be accessed. This has been known for many years.[33]

When the Telecom Companies provide a new technology or new kinds of telecom services, there will always be individuals who try to use the technology or the services for unlawful or illegal purposes. Crime follows opportunity and there are a lot of opportunities in the telecom field.[34] The risks of being detected are not especially deterring, and the reactions from the society are in many countries not especially powerful. There will still be a lot to study with regards to the issues on telecom crime.

Assistance from the Telecom Companies

A major part of IT-related crime involves a telecom network or services provided by a Telecom Company. This fact should be kept in mind whenever an IT-related crime has occurred. Therefore the involvement of a Telecom Company might be regarded as essential for the possibilities to commit an IT-related crime, or at least as facilitating the performance of the actual crime. This might as well be the misfortune for the criminal, because of the information that is stored within the telecom network and the information systems of the actual Telecom Company. This information can be very useful for tracing, detecting and convicting the criminal. It would then be a good advice to involve the Telecom Company as early as possible in the crime investigation. Referring to my colleagues and to my own professional experience as a corporate counsel at the TeliaSonera group, it is often critical for the success of the investigation to get the actual information as fast as possible.

There are certain difficulties regarding the crime investigating in information systems such as a telecom network. The crime investigating authorities are often dependent on the assistance by expertise from the telecom operators to be able to access the right kind of information and to understand the functionality of the

33 Grabosky, Smith, *Crime in the Digital Age*, p 77 f.

34 Grabosky, Smith, *Crime in the Digital Age*, p 1 f.

technology. This assistance is also often needed to explain the circumstances before a court.[35]

A question of great delicacy concerns the reliability of the actual information from the Telecom Company. How can it be granted that the information is not manipulated, especially when the structures of the telecom network and the information systems are becoming more and more complex and complicated?[36] How can the trustworthiness of the information be held beyond any reasonable doubt before a court of law in a criminal case? It is still not common that the defence counsels challenge the information by asking the prosecutor or the expert to describe how the information is provided and how it can be guaranteed that the information is correct and not manipulated by any person or by lacks or malfunctions in the network or in the information systems.

The information from Telecom Companies will still be of significant importance as evidence in the courts. It will then be necessary that this information can be made understandable and that it cannot be questioned from a technical and security perspective. If the trustworthiness of such information is lowered it will be harder to prove the activities and to hold the suspects responsible.

From the Telecom Companies' viewpoint it will be of major importance to increase the authorities' resources and competence. With regard to the international issues, law harmonisation and co-operation are essential.

It will probably be more effective to fight telecom-crime by using preventive methods rather than crime investigating and prosecuting.[37] This is very much in accordance with the experiences of the Telecom Companies.

The experience of the Telecom Companies is also that civil law enforcement is more efficient than criminal law procedures. According to the Telecom Companies' general terms and conditions the subscribers are responsible for activities that relate to their subscriptions. In a civil case it will then be sufficient if the Telecom Companies proves that a certain phone number, IP-address or other identification has been the source of the criminal activity and thereafter take the measures provided in the general terms and conditions, such as disconnecting the telephone or the computer, or other similar measures.[38] Such measures have shown effective against the problems with free surfing and there are no reasons that they shouldn't be effective also against many other unauthorized activities.

When the criminal activities get more international there will also be an increased need for international crime-investigation. Today international bureaucracy as well as differences between the legislation of the actual countries obstructs effective international crime-investigation.

It may then be suggested that the Telecom Companies take more actions in accordance with their general terms and conditions in addition to reporting the incidents to the police.

---

35 SOU 1992:110 p 144, SOU 1992:110 p 335 ff.

36 Lloyd, *IT-law*, p 273 ff.

37 Lloyd, *IT-law*, p 216, BRÅ-report 2000:2, p 42 f, 59 f.

38 TeliaSonera *General Terms and Conditions*, sec 7.1.

References

EU Directives:

Directive 95/46/EC

Directive 2002/58/EC

Governmental Bills:

Ds 1995:48, Teleoperatörernas skyldigheter vid hemlig teleavlyssning och hemlig teleövervakning

-Prop. 1992/93:200, Telelag och en förändrad verksamhetsform för Televerket, m m

-Prop. 1994/95:227, Hemlig teleavlyssning och hemlig teleövervakning

-Prop.1995/96:180, Teleoperatörernas skyldigheter vid hemlig teleavlyssning och hemlig teleövervakning

Prop. 2002/03:74, Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering

Prop. 2002/03:110, Lag om elektronisk kommunikation m.m.

Official reports etc:

European Committee on Crime Problems, Committee of Experts on Crime in Cyber-space, Draft Convention on Cybercrime (Draft No 23 REV.)

SOU 1992:110, Information och den nya InformationsTeknologin - straff- och processrättsliga frågor mm

SOU 1993:10, En ny datalag

SOU 1994:149, Säkerhetsskydd

SOU 1997:39, Integritet, Offentlighet, Informationsteknik

SOU 1998:46, Om buggning och andra hemliga tvångsmedel

SOU 2007:76, Lagring av trafikuppgifter för brottsbekämpning

Literature:

Borgström, Lindborg, *Säker data- och telekommunikation* (Borgström, P, Lindborg, L, "Säker data- och telekommunikation", Affärsinformation AB, Stockholm 1992)

- Grabosky, Smith, *Crime in the Digital Age – Controlling Telecommunications and Cyberspace Illegalities*, Transaction Publishers and The Federation Press, 1998

- Lloyd, IT-law (Lloyd, Ian J, 2008, *Information Technology Law*, 5th edn, Oxford University Press)

Journals:

Svensk Juristtidning 8/92

Televärlden nr 4, 26 februari 1998

Televärlden nr 6, 26 mars 1998

Cases

Appeal Courts

Svea hovrätt 1996-12-20 (Ö 4105/96)

Svea hovrätt 1997-03-25 och 1997-05-07 (Ö 1241/97)

Hovrätten för Västra Sverige 1997-05-14 (Ö 155/97)

Göta hovrätt, 1999-09-27 (The Göta Appeal Court, September 1999) (Ö1098/99)

Others

TeliaSoneras General Terms and Conditions

Legislation

Lagen (2003:389) om elektronisk kommunikation (the Swedish Act on Electronic Communication

Personuppgiftslagen (1998:204) (the Swedish personal Data Protection Act)

Rättegångsbalken (The Swedish Procedural Code)

Telelagen (1993:597) (The Swedish Telecom Act)

Abbreviations

DI Datainspektionen (the Swedish Data Inspection Board)

Ds	Departementsserien
EIR	Equipment Identity Register
EWS	Early Warning System
f	following page
ff	following pages
FCS	Fraud Control System
FDS	Fraud Detection System
IP	Internet Protocol
IT	Information Technology
LEK	Lagen (2003:389) om elektronisk kommunikation (the Swedish Act on Electronic Communication
NJA	Nytt Juridiskt Arkiv (Swedish case-law)
p	page
pp	pages
Prop	Regeringens proposition (Swedish Governmental Bill)
PTS	Post- och telestyrelsen (the Swedish Post- and Telecom Agency)
PuL	personuppgiftslagen (1998:204) (the Swedish personal Data Protection Act
RB	Rättegångsbalken (the Swedish Procedural Act)
SOU	Statens offentliga utredningar
SvJT	Svensk Juristtidning
TL	Telelagen (1993:597) (the Swedish Telecom Act)
EU	The European Union