Telecom Companies as Crime Investigators

Conny Larsson

1 Introduction

This section handles how the telecom operators' and other service providers' (further referred to as the Telecom Companies) can assist in the performance of crime investigations in the telecommunication networks and information systems.

In relation with such investigation there are a number of issues such as what the Telecom Companies can do in order to prevent, detect and react on criminal activities within the networks, but also the legal conditions for such measures – what the Telecom Companies are allowed to do. Another issue is what the Telecom Companies are obliged to do in order to assist the crime-investigating authorities, such as the obligation to assist when legal interception is to be performed.

The complexity of the technology, the border-crossing nature of the communications, the co-operation between the Telecom Companies, the need of quick reactions when searching for evidence and the time-consuming procedures related to international police co-operation are aspects that give rise to the question if the Telecom Companies are more effective than the authorities when it comes to crime investigations in the telecommunication networks and information systems.

It seems reasonable to suggest that the Telecom Companies should have the best knowledge about their networks and information systems and how to perform an investigation in that environment. If so, can it be a better alternative to turn to the Telecom Companies instead of to the crime investigating authorities and will that alternative be more successful in combating crimes using or targeting the telecom networks and services?

2 Background

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. Information from the Telecom Companies suggests that there are about 6-7 million subscribers in the Swedish fixed-wire network and about 3 million subscribers in the mobile telephone network. It is suggested that each day the Telecom Company TeliaSonera[1] transfer about 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

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

use of interlocutory measures.[2] 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 in a limited geographical area at a certain moment.[3] The UMTS-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.[4] 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). In 2003 TL was replaced by the Swedish Act (2003:389) on Electronic Communications (LEK), according to which the regulations also apply on other major service providers within the field of electronic communications. These acts are corresponding to EU-directives, such 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.[5] 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.[6] In November 2001 Convention on Cyber Crime, was ratified by

---

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

3 SvJT 8/92, p. 534.

4 Lloyd, *IT-law*, p. 287.

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

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

Sweden. This convention holds an obligation to store information, including historical data, for the authorities' crime-investigation.[7] 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?

2.1 Telecom Companies' Right to Perform Crime-investigating 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.[8] 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.[9] If the crime-investigating activities are necessary for protecting the network and the services, it can be argued that the Telecom 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 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 the Swedish Personal Data Act (1998:204) (PuL).[10] 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 be superior to 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 be regarded as superior to 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 the Swedish LEK so that the telecom act will prevail.[11]

The question of which law should be regarded as superior could 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

7 *Convention on Cyber Crime*, ETS No. 185.

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

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

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

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

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.

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.[12] 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 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.[13]

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.[14] 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

12 Lloyd, *IT-law*, p 291, Grabosky, Smith, *Crime in the Digital Age*, p. 29 f.

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

14 *E.g.* TeliaSoneras' general terms and conditions, sections 6.5 and 10.1.4.

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.

2.2 Telecom Companies' Crime-investigating and Telecom Secrecy

The handling of traffic data can also be questioned from another perspective. Traffic data is protected by telecom secrecy, which can prevent 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 such activity with providing them with information necessary for taking action against the activity.

However, the telecom secrecy does not apply with regards to subjects that have participated in the actual communication or to the actual subscribers. In 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.[15]

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.[16] In addition the crime investigating authority can be entitled to the information by an interlocutory measure, such as legal interception.

2.3 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.[17]

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 (SIS, Subscriber Identity Security) for mobile telephones in the analogue NMT-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

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

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

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

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.[18]

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 ways of handling the security problems, such as locks and alarms protecting localities where the equipment is placed, access control systems etc.[19]

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.[20]

2.4 Telecom Companies' Crime-investigation in Practice

The Swedish Telecom Companies have specialized personnel or other entities working with security issues.

At TeliaSonera Sweden AB there are a number of entities 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 entities are specialized in performing investigations concerning unauthorized activities on the fixed telecommunication network and the mobile telecommunication network (TeliaSonera Network Security), computer incidents (Computer Emergency Response Team - TeliaSoneraCERT), and illegal information on the Internet (TeliaSonera Sverige Abuse). The normal procedure is that a subscriber that has been victimized contacts TeliaSonera's Customer Service. The Customer Service decides what entity should be competent to handle the case and refers the subscriber to that entity.

At Tele2 AB there is a special entity, Customer Security that handles issues regarding incidents. This entity is organized under the Customer Service. Among the issues handled by the Customer Security are data intrusions, harassments, threats, misuse of identities, intrusions regarding intellectual property rights, Internet abuse such as child pornography etc.

Vodafone AB has a similar organisation as Tele2, which means an entity named Customer Security organized under the Customer Service.

---

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

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

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

The Telecom Companies co-operate in matters concerning preventing, detecting and acing 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 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.[21]

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

21 *Televärlden* nr 4, 26 februari 1998.

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.

2.4.1 "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.

2.4.2 "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[22]. 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.

2.4.3 "071-fraud"

Cloned mobile phones have also been used for other kinds of unauthorized activities, such as the "071-fraud". In such cases the perpetrator enters a "071-subscription", which consists in a certain kind of pay-call service, where the Telecom Company charges the caller a certain fee and pays 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 without authorization. The perpetrator was sentenced to imprisonment for 1,5 years for fraud of the first degree.[23]

2.4.4 "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

22 Huddinge TR, April 1997.

23 Stockholms TR, May 1995.

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.[24]

2.4.5 "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.[25]

2.4.6 "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.[26]

2.4.7 "Demon Phreaker"

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

24 Hovrätten för Nedre Norrland, October 1996.

25 Enköpings TR, October 1996.

26 Stockholms TR, October 1996.

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 (!).[27]

2.4.8 "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 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.[28] 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

27 *Televärlden* nr 6, 26 mars 1998, Göteborgs TR.

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

addition the trials rarely lead to sentences to major imprisonment, which indicates that the present cases hardly deter the perpetrators from continuing their activities.

2.5 Telecom Companies Obligation to Assist

In some situations the Telecom Companies are obliged by law to assist the crime investigating authorities. First, the companies are obliged to technically adapt their networks and services in a way that enables the crime investigating authorities to perform legal interception within these networks and services. Second, the crime investigating authorities can access information while performing search and seizure at the Telecom Companies. Third, the Telecom Companies are obliged by applicable telecom laws to provide the crime investigating authorities in certain situations with certain information, such as subscriber information and traffic data. Fourth, according to the Cyber Crime Convention the EU member states to take legislative measures to oblige the Telecom Companies and other service providers within the field of electronic communication to store traffic data for some time for crime investigating purposes.

2.5.1 Legal Interception

Legal interception consists in *interception of communications* and *provision of call associated data*.

To perform legal interception a court order is required and the measure must concern a certain subscription, a phone-number or another connection, an address, an e-mail address, a code or a similar object that can be used by the suspect.[29] In addition there must be some evidence of certain strength against the suspect, and the measure must also be of significant importance for the investigation.[30] The measure may not continue for more than a month after the decision on the court order. [31] In practice the measure concerns telephone calls or mobile telephone calls, but the regulations apply on every kind of telecommunication, such as telex, telegram, telefax and data communication such as e-mail.[32]

The interlocutory measures are regarded as valuable instruments for the authorities when investigating crimes. This is especially so with regard to drug related criminality, organised crime, financial crimes and crimes against national security. IT-development also changes the conditions for interlocutory measures.[33] In addition to the regulations within the Swedish Procedural Act, there are some special regulations that apply in certain situations. These

29 RB 27:21, prop. 1994/95:227 p. 21, 31, SOU 1998:46 p. 60.

30 RB 27:20.

31 RB 27:21.

32 SOU 1998:46 p. 59.

33 Ds 1995:48 p. 19 f, prop. 1994/95:227 p. 15 f, prop. 1995/96:180 p. 17 f.

regulations extend the instances where the measures may apply concerning foreigners and their participation in certain terrorist organisations, warfare and crimes against national security.[34]

Interception of communications refers to the secret interception in the form of listening in to, recording or tapping a certain telecommunication, such as a fixed line or mobile telephone call. Again, this measure only applies where the crime investigated is punishable by imprisonment for not less than two years. There must be a court order and the measure may not continue for more than one month from the decision on the order.[35]

Provision of call-associated data does not relate to the content of the actual communication, but to other information about the communication, such as the calling or the called telephone number, code or other connection identity. Other kind of information may be the time or duration of the communication, or the base station involved in the exchange of the communication.[36] This measure applies only when a crime is investigated that may lead to not less than imprisonment for six months or concerns a drug-related crime.[37]

There will probably be legislative adjustments that entitle the crime investigating authorities to perform legal interception in an increased number of situations. This may be a result of the increased threat from terrorism as well as the technical development in the field of electronic communication. A Swedish Commission ("Buggningsutredningen") suggests that the prerequisite for performing interception of communications should be changed to not less than imprisonment for one year.[38] There is also a present governmental bill that suggests that legal interception should be allowed even if the imprisonment prerequisite is not fulfilled, but it can be expected that the actual crime will actually lead to imprisonment of a certain period of time.[39]

The regulations on interlocutory measures differ between countries even within the European Union. Some efforts have been made to harmonise the legislation with regard to legal interception. An example is a European Council resolution that provides a specification of requests that should be considered in the national legislation.[40] In addition there is a working party, which has provided a recommendation on privacy protection issues related to legal interception.[41]

---

34 Lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål, lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara mm, lagen (1991:572) om särskild utlänningskontroll.

35 RB 27:18, 21.

36 Prop. 1994/95:227 p. 15, SOU 1998:46 p. 59, SvJT 1992/8 p. 534, SOU 1998:46 p. 59.

37 RB 27:19, 21.

38 RB 27:18, SOU 1998:46 p. 27, 482 f.

39 Prop. 2002/03:74 p. 31 ff.

40 Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications (9529/95 ENFOPOL 90).

41 Recommendation 2/99 on the respect of privacy in the context of interception of communications.

2.5.2 Search and Seizure

Search and seizure is an interlocutory measure that entitles the crime investigating authority to search a house, room or another private place to look for objects that shall be confiscated or to collect evidence. The measure may only be performed when imprisonment is provided and no court order is necessary to allow the performance.[42] During a search and seizure objects or written documents may be confiscated and if the measure is to be performed at a Telecom Company, the measure must concern a crime where imprisonment for at least one year can follow. The measure can be performed without a court order.[43]

A more detailed comparison between the regulations cannot be provided in this work, but would be an interesting issue for the future. These countries face the same problems regarding interlocutory measures, but may have to solve them in different ways depending on the actual political system, culture and legal tradition etc.

Search and seizure may at a Telecom Company lead to certain problems. First, the Telecom Company is not obliged to *actively* provide the information and can be held responsible for breaching of secrecy if assisting. Second, the authority may not know how to access the information, so the confiscation can be impossible to perform.

According to Swedish law it is more or less clarified that the crime investigating authorities cannot access traffic data by performing search and seizure at a Telecom Company. Court decisions suggest that the police is not allowed to circumvent the telecom secrecy so that the secrecy overrules the regulations on search and seizure.[44]

With respect to search and seizure rules, it can be expected that the legislation differ even more between the countries than the regulations on legal interception. Compared with the Swedish legislation the crime investigating authorities of United Kingdom may require a printout of information while exercising a search warrant (Section 19 (4) of the Regulation of Investigatory Powers Act 2000). [45]

2.5.3 Obligation to Provide Information

There are a number of countries where the Telecom Companies are obliged by law to assist law enforcement and national agencies by providing access to communications for certain purposes.[46]

LEK obliges the Swedish Telecom Companies to provide the crime investigating authorities with traffic data. A condition for the obligation is that

42 RB 28:1.

43 RB 27:1.

44 Göta Hovrätt, mål nr Ö 1098/99, prop. 2002/03:74 p. 45.

45 Lloyd, *IT-law*, p. 287 ff.

46 Grabosky, Smith, *Crime in the Digital Age*, p. 28 f.

the investigated crime can lead to imprisonment for not less than two years.[47] The information that shall be provided to the authorities is the same kind that the authorities can access when performing provision of call-associated data; other information about the communication than the content, such as the calling or the called telephone number, code or other connection identity, the time or duration of the communication, or the base station involved in the exchange of the communication. A difference between this obligation and provision of call-associated data is that the obligation concerns historical data, while the provision of call-associated data concerns data occurring after the actual court decision.

2.5.4 Obligation to Store Information (Convention on Cybercrime)

There is yet no obligation for the Telecom Companies to store information about telecommunications for assisting the crime investigating authorities, unless there is a decision on legal interception and a request from the crime investigating authority. The crime investigating authorities suggest that stored historical data from the Telecom Companies would be of significant importance for the investigations.[48]

Within the EU there are discussions on implementing general obligations for Telecom Companies and Internet Service Providers to store call-associated data for the investigation of crime. The discussions have resulted in the Convention on Cybercrime, ETS No 185, which suggests that the Telecom Companies and Internet Service Providers for the investigation of crime should store information such as traffic data.[49]

From the Telecom Companies' viewpoint such an obligation will be questionable on the same ground as the obligation to adapt the telecom networks and services for legal interception (se above). The Convention on Cybercrime doesn't say what kind of information should be stored and for how long time, which means that this question is left to be answered by the national legislators. As mentioned above, TeliaSonera AB daily transfers about 50.000.000 electronic communications through its telecom network in Sweden. Should the Telecom Companies be obliged to store all traffic data regarding such communication and for unlimited time, the costs and the administration relating to the obligation could be significant. The Telecom Companies must compensate themselves for these costs and the consumers, as usual, will pay the final costs for such an obligation. A general obligation to store all traffic data will of course also be strongly challenging to the individual integrity.

The Convention on Cybercrime was ratified by the EU member states in November 2001, but so far it has not lead to any legislation in Sweden.

47 LEK 6:22.3, Directive 2002/58/EC, Article 15.1.

48 SOU 1998:46 p. 276, 279, 283, 289, 293, 296, 300.

49 *Convention on Cybercrime* (ETS No 85), Article 14-21.

2.6 Legal Interception - Practical and Technical Issues

According to the legal obligation with respects to secrecy this thesis cannot provide any detailed information on how legal interception is carried out by the Telecom Companies. Also the crime investigating authorities are obliged by law to keep such information secret.[50]

However it is appropriate to give a brief, general description of the actual procedures.

From the Telecom Companies' viewpoint, there are some essential questions related to the obligations. First, it can be argued if it is acceptable from a constitutional point of view that private subjects such as the Telecom Companies are obliged to build their information systems considering crime investigation. Second, it doesn't seem reasonable that the private subject also should carry the costs for any technical measures that are necessary for the police work, which is a general public interest and therefore should be carried by the state. Third, the expenditures in the actual technology can in some cases prevent the Telecom Companies from investing in new technology and therefore become a hindrance for IT development. Fourth, it would also be questionable from a constitutional viewpoint if the Telecom Companies become obliged to store historical information for purposes of investigating crime. Such an obligation will also lead to costs such as for the technical equipment, personnel and administrative costs, which again brings to the fore the issue of who is going to pay for these necessary costs.

Denmark, France, Germany, Italy, Netherlands and United Kingdom have legislated on obligations for their telecom operators to enable legal interception within their systems. Ireland has adapted a Ministerial Order that obliges the telecom operators to enable legal interception. In Australia and in USA the telecom operators are obliged to enable legal interception but are also entitled to compensation from the state.[51]

During the investigation of crime and once the police has decided that a legal interception measure is necessary, the public prosecutor is asked to apply to the court for an order on the actual measure. After a court order is granted, the police request the actual Telecom Company to carry out the measure by connecting the police equipment within the telecom network. When the time for the measure has expired, the Telecom Company disconnects the equipment. The kind of connection and equipment used depend upon the technical conditions within the network.[52]

The main Telecom Companies are obliged to adapt their existing telecom networks and services and to implement such new networks and services that facilitate the carrying out of legal interception. The obligations are technical, organisational and administrative. The Telecom Companies must use such technology as to enable the carrying out of legal interception, which means suitable hardware, such as machinery and other equipment, as well as software.[53]

---

50 LEK 6:21, SekrL 5:1.

51 Prop. 1995/96:180 p. 14 ff.

52 Ds 1995:48 p. 27 och SvJT 8/92 p. 537 ff.

53 Prop. 1995/96:180 p. 25.

Many countries have implemented a similar legislation, including Australia, Denmark, Germany, Great Britain, France, Italy, Netherlands and the USA.[54]

The obligations are motivated by the fast development of telecom technology and the fact that the Telecom Companies have a very important role regarding interlocutory measures within the telecom field. In addition, compared with the authorities the Telecom Companies have a unique knowledge about telecommunications and the telecom networks. If the authorities themselves connect their equipment within the networks, this could jeopardise the integrity of the system. For that reason the Telecom Companies are better positioned for the performance of such connection.[55]

From a legislative perspective this obligation may be regarded as something between an obligation to actively provide the information and an obligation to remain passive. It should also be kept in mind that the obligation to adapt the technology for legal interception does not apply to minor Telecom Companies. In such situations, the authorities themselves may carry out legal interception in the actual network, but without any assistance from the telecom operator.[56]

The adaptation of the Telecom Companies' telecom network and systems will result in large financial expenditure. For the Telia group the expenditure was at first estimated to be about 34 million Swedish crowns.[57] According to more recent information from the Telia group the outlays have so far reached nearly 100 million Swedish crowns. Under LEK the Swedish Telecom Companies are not entitled to reimbursement from the state for these outlays. This will result in that the subscribers will finally bear the costs for the outlays are, which may seem a little bit inequitable when the state normally will cover the costs for the activities of the crime investigating authorities.

LEK doesn't mention how the adaptation is supposed to be effected. Instead this task is left for the supervisory authorities to handle, that is to say the Swedish Post- and Telecom Office (PTS).[58] To be able to decide upon closer regulations regarding the adaptation, the PTS has to get the Telecom Companies and the crime investigating authorities to participate. The PTS has to find a proper balance between what the authorities request and what the telecom operators reasonably are capable to provide. In these situations agreements between the authorities and the Telecom Companies are of great importance.[59]

When the PTS decides upon the specific regulations the authorities benefit from the actual adaptation should be balanced against the expenditure of Telecom Companies, so that the expenditure will not be unreasonable or the benefit will only be of minor importance for the authorities.[60] Special considerations should be taken when the adaptation concerns networks or systems that existed already before the regulations were decided, so that the

54 Ds 1995:48 p. 22 ff.

55 Ds 1995:48 p. 11.

56 Prop. 1995/96:180 p. 22, LEK 6:19.

57 Prop. 1995/96:180 p. 31.

58 LEK 6:19.

59 Prop. 2002/03:110 p. 267 ff., 396, prop. 1995/96:180 p. 28 f, 37.

60 Prop. 2002/03:110 p. 396, prop. 1995/96:180 p. 37, Ds 1995:48 p. 43.

requests on the telecom operators may be of a lower degree than will be the case according to new technologies that are planned. If the expenditure will be of a burdensome extent or the technical solutions will be very complicated, the PTS may decide that the obligation to adapt will not apply in certain situations, or at least give the telecom operator a longer time to effect the actual adaptation.[61]

It is important that the technology used by the authorities and the telecommunication technology employed by the Telecom Companies can work together. If this is not the case it may be questioned who should take the steps that are necessary. From the Telecom Companies' viewpoint it would be unjust to require the incurrence of costs to reconstruct the entire network because of a decision by the authorities to employ outmoded or obsolete equipment.

The Telecom Companies have taken different organisational measures in order to handle the requests on legal interception. Within TeliaSonera there is a special entity that handles relations with the crime investigating authorities. The entity handles not only the performance of legal interception, but also requests in other situations for providing information on telecommunications not only from crime investigating authorities. The reasons for this special staff are to secure the authorities competent service, and that no information is disclosed in conflict with legal obligations.

The variety of services that can be provided by the GSM-system complicates the situation. An example of such services is the pre paid phone-cards where the user is anonymous. Another example is the feasibility to code or encrypt the communication.[62] There are some indications that criminal organisations such as certain "bike gangs" have access to encryption equipment.[63] It should be noticed that the Telecom Companies are not obliged to decode or decrypt communication that is encoded or encrypted by another subject.[64]

2.7 Legal Interception - Effectiveness

In this section some statistic figures are given that show the scope of legal interception. The figures indicate that most performance of legal interception concerns drug-related crimes.[65] The figures relating to investigations of the Swedish National Security Police (SÄPO) are secret, but 80-90 % of interception of communications requested by the SÄPO takes place in accordance with special legislation and relate to crimes against national security.[66] The regulations on provision of call-associated data also apply to hindering communications from or to the connection of a certain subscriber. So far, this has not been used, and is of no practical importance.[67]

---

61 Prop. 2002/03:110 p. 396, prop. 1995/96:180 p. 29, Ds 1995:48 p. 26.

62 SOU 1998:46 p. 285, 293, 299, 317.

63 SOU 1998:46 p. 311.

64 Prop. 1995/96:180 p. 27.

65 SOU 1998:46 p. 67 f.

66 Lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål, SOU 1998:46 p. 285, 460.

67 SOU 1998:46 p. 366.

Scope of Legal Interception

Interception of communications 1985 – 1996

Year	Drug-related	Other	Total
1985	233	6	239
1986	213	15	228
1987	205	15	220
1988	210	15	225
1989	214	24	238
1990	214	13	227
1991	243	31	274
1992	258	61	319
1993	261	84	345
1994	309	81	390
1995	333	83	416
1996	306	91	397

Provision of call-associated data 1993 – 1996

Year	Drug-related	Other	Total
1993	54	6	60
1994	62	6	68
1995	33	11	44
1996	70	29	99

The figures indicate that legal interception has become more important and that it can be expected that the use of these measures will increase.

Efficiency of Legal Interception

Efficiency of legal interception 1985-1996 (SOU 1998:46 p. 67 f)

	Interception of communications			Provision of call-associated data		
	Effect	No effect	Interrupted	Effect	No effect	Interrupted
Year						
1985	77%					
1986	64%					
1987	68%					
1988	44%					
1989	51%					
1990	47%					
1991	48%					
1992	47%					
1993	56%			35%	10%	55%
1994	52%			28%	44%	28%
1995	51%			52%	25%	23%
1996	49%	34%	17%	33%	58%	9%

The importance of legal interception is that it can provide information which makes it possible to map and to track connections and activities of the suspects. It may also contribute to further investigation and other steps of the authorities, which is a kind of an indirect effect.[68] The figures above do not give a clear picture, but indicate that interception of communications is more efficient than provision of call-associated data.

Another issue relating to legal interception, which may be regarded as of some sensitivity, is the use of "supplementary information".[69] That is if the accessed information may be used in other investigations or to stop a planned crime or for the activities of other authorities, such as the tax authority etc.[70]A later decision by the Swedish Supreme Court clarifies that the crime investigating authorities are entitled to use such supplementary information in other crime investigations.[71]

2.8 Telecom Companies as Witnesses or Experts in Court

When employees at the Telecom Companies appear in courts 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 courts 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.[72] 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.[73] A witness is only entitled to a quite limited payment for its expenses.[74] 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. This could be valuable e.g. in a situation where the actual employee is threatened and frightened to testify.

---

68 SOU 1998:46 p. 61, 308, 321.

69 "Överskottsinformation".

70 SOU 1998:46 p. 87.

71 HD, B 2076-03.

72 RB 36:1.

73 RB 40:4 and 17.

74 RB 36:24.

3 Conclusions

3.1 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. IT is essential for the structure of the states, nationally as well as internationally and inflicts also on the co-operation between states and the security of the states. Thereby IT will also be of great strategically importance for the states. The Swedish Security Law that traditionally has applied upon authorities indicates this importance, as the law since 1996 also applies on certain private subjects, such as the telecom operators. The focusing upon the Y2K problem is another indicator of the importance of the information systems. Neglecting IT-crime and telecom crime may damage the public faith in the communications and thereby hinder the IT-development. Therefore the criminality must be taken seriously not only by the telecom operators, but also by the states.

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.[75]

3.2 The Impact of Telecom Crime

Information provided by the Telecom Companies suggests that cloned mobile telephones peaked in the late 1990: s where the Telia group suffered damage exceeding 180 million SEK (1998). More than 50 % of that amount was paid to other Telecom Companies as “roaming agreement fees” caused by the fact that 50 % of the unauthorized communication was transferred through the other companies’ networks. The information further suggests that the present most relevant telecom criminality are, carding, subscription fraud, free surfing, illegal content on web sites and different kinds of illegal interception (hacking etc.). The loss relating to telecom crime is according to The Telecom Companies estimated to exceed 100 million SEK a year.

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

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

there are a lot of opportunities in the telecom field.[76] 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.

3.3 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 Telia group, it is often critical for the success of the investigation to get the actual information as fast as possible.

3.4 Information from the Telecom Companies used as Evidence

There are as stated before special 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 technology. This assistance is also often needed to explain the circumstances before a court.[77]

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?[78] How can the trustworthiness of the information be held beyond any reasonable doubt before a court of law in a criminal case? It is 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

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

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

78 Lloyd, *IT-law*, p. 295 ff.

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.

3.5 How can we Improve the Measures Against Telecom Crime?

IT-crime is not only a question of super-intelligent young boys performing hacking on different computer systems, but also consists in different ways of using telecommunication services without paying. There are still a lot of unanswered questions, such as how adequate measures can be provided for estimating the crime rates and reducing the dark figures. It should also be considered how the Telecom Companies and the authorities can co-operate more effectively in combating crime and how internationally performed crime should be handled in the most efficient way.

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. The possibilities to get the perpetrators extradited will of course also contribute.[79] At the moment there is a Swedish Commission discussing the organisation and methods of the crime investigating authorities. It is suggested that there should be specialized crime-investigators that are not policemen but shall have certain authorization partly similar to the policemen. Perhaps could such "crime-investigators" employed by the Police[80] even be placed at the telecom operators in order to speed up and otherwise improve the investigations?

3.6 Legal Interception and the Convention on Cybercrime

Above the different Swedish regulations on legal interception and other interlocutory measures are described. Some conclusions can be drawn from these regulations, especially concerning the impact of the technical development, the privacy aspects and the relationship between the regulations. The Swedish legislation is reasonably clear and understandable. Due to this fact, very few problems arise for Telecom Companies with respect to issues arising from legal interception. Because of the procedures regulated by the Swedish Procedural Act, the crime investigating authorities cannot exercise a legal interception without a court order. The involvement of the court system gives the Telecom Companies a fair reason to be assured that the privacy considerations of their subscribers are properly addressed.

Nevertheless an increasing use of legal interception may result in that the public develop doubts concerning the privacy of telecommunications. From this point of view it can be questioned whether the legislation should allow an extended application of legal interception. Another aspect is that the target subjects of legal interception, the criminals, may change their use of the

79 Lloyd, *IT-law*, p. 207, Grabosky, Smith, *Crime in the Digital Age*, p. 11.

80 SOU 2003:114

telecommunications so that the use of legal interception will become more and more ineffective. As an example the criminals will use anonymous pre-paid phone cards instead of common mobile phones to hide their identities and whereabouts.

The obligation to build telecom networks so that they are compatible with legal interception may cause some discussions, especially with regard to the compensation issue, but also according to how the obligation should be interpreted. For instance, Telecom Companies may have to employ more people or reorganise their administration in order to handle an increasing amount of requests. It is not quite clear whether this would be regarded as included in the obligation or as a certain execution for which the Telecom Companies are entitled to payment. It is of great importance that the obligation does not become such a burden for the Telecom Companies that it hinders the technical development. In addition the Telecom Companies can only compensate themselves to a certain limit by payment from the subscribers. Increasing prices for the telecom services will probably result in a decreasing use of the services, which will have an impact on the investments and also inflict the technical development.

If the legislation leads to large investments for the Telecom Companies and no significant benefit can be expected, there should be no extension of the obligation. In this situation the Swedish Post- and Telecom Office should play an active role to make the legislator aware of this impact of legal interception.

It can also be questioned from a constitutional viewpoint if it is appropriate to oblige private subjects, such as the Telecom Companies, to be responsible for providing and bear the financial expenditure for facilities for crime investigations. This responsibility has traditionally been an issue for the authorities. After obliging the Telecom Companies to technically adapt their networks and systems for legal interception, the EU has now implemented the Convention on Cybercrime that oblige the member state to oblige their Telecom Companies and Internet service providers to store information for the crime investigating of the authorities. One thing leads to another and other similar obligations may be the case in the future. In such a perspective the role of the Telecom Companies may slowly turn from providing telecommunications to become more or less a tool for the authorities.

Therefore the authorities ambitions on fighting cyber crime and other unauthorized activities in the networks and services should not go too far and thereby damage the technical development, the business itself and the public faith in telecommunications.

3.7 Search and Seizure and other Interlocutory Measures

Regarding other kinds of interlocutory measures the situation is somehow different. From a legal point of view the problems are largely related to the different regulations that oblige a subject to provide different authorities with information and especially with regard to such regulations that are given in other legislation than LEK.

With regard to search and seizure the priority issues now seem to have been settled by Swedish case law. Since the latest decision of the Swedish Appeal Court there have been no disputes concerning search and seizure. This has probably been positive for the co-operation between the Police departments and the Telecom Companies as well as for the public faith in the telecom privacy.

The question still stands with respect to other legislation, but so far the authorities have seemed quite reluctant to handle the priority issues in court. If these issues continue to be unanswered by the legislator, it may be interesting to watch the further development of case law and to make a deeper analysis, based on comparison with other national legislation and court practice.

It is of great importance for the Telecom Companies as well as for the subscribers to clarify that secrecy regulations cannot be circumvented in a way that is legally questionable.

3.8 Supervision of Telecom Companies

The present legislation may even lead to conflicts between different supervision authorities, for instance between the Swedish Post- and Telecom Office (PTS) and the Swedish Data Inspection Board (DI) concerning how the Telecom Companies handle information on subscribers. According to one authority the information may be handled correctly, while the other authority will find the information handled in conflict with the law. Such a situation will naturally be difficult to handle for the Telecom Companies. According to the expressed hierarchy between telecom law such as LEK and personal data protection law such as PuL, the supervision of PTS should prevail.

Even if this is a question that is still unanswered it will probably not prevent the Telecom Companies from handling information in order to deal with the incidents.

3.9 Taking Civil law Actions Instead of Criminal law Procedures?

It will probably be more effective to fight telecom-crime by using preventive methods rather than crime investigating and prosecuting.[81] 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.[82] Such measures have shown effective against the problems with free surfing and there

81 Lloyd, *IT-law*, p. 214, BRÅ-report 2000:2, p. 42 f, 59 f.

82 Telia's General Terms and Conditions, sec 2.5.

are no reasons that they shouldn't be effective also against other unauthorized activities.

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.

3.10 Other Issues

When the information becomes more and more digitised there will also be a problem relating to the definitions of information. In some regulations there are formal requirements on documents in "writing" and where it can be questioned if digital information will be regarded as "written". In the digital world the paper document will gradually be replaced by digital documents, which will make it necessary to clarify the relationship between digital documents and the formal requirements given in different regulations.

From a more practical point of view it will be important to measure the effectiveness of the interlocutory measures and to see how this will be balanced against privacy and integrity aspects. The development of IT and telecommunication will lead to new forms of technology and services. The borderlines between different technologies become more and more blurred. The more the different information technologies converge; it will become harder and less suitable to keep a legal system based upon different regulation for different technology. In this situation it can also be questioned if it will be useful to keep special regulations for special subjects such as the Telecom Companies. Therefore the impact of the development of information technology may lead to that the legislation becomes more confusing.

It will be interesting to see how prospective legislation will handle the new situations and the conditions that follow. There are reasons for further analysis of the international perspective, which becomes more urgent because of the globalisation of networks, such as the Internet. This will cause jurisdictional problems, such as if and how interlocutory measures may apply in a more and more internationalised situation. 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.

Anyway, the Telecom Companies capability to assist in crime investigations shall not be neglected. There is a lot of useful information at the Telecom Companies' disposal. As described above, they have the best knowledge of their networks, services and information systems. This knowledge may be useful for the police as well as for the victim. In IT-environments it is essential that the investigation starts quickly and without destroying the evidence, which generally makes a co-operation between the victim, the police and the Telecom Companies the most efficient way to handle the investigation.

Abbreviations

Ds	Departementsserien
f	following page
ff	following pages
LEK	lagen (2003:389) om elektronisk kommunikation (the Swedish Act on Electronic Communications)
p	page
pp	pages
Prop.	Regeringens proposition (Swedish Governmental Bill)
PuL	personuppgiftslagen (1998:204) (the Swedish personal Data Protection Act
RB	rättegångsbalken (the Swedish Procedural Act)
SekrL	sekretesslagen (1980:100) (the Swedish Secrecy Act)
SOU	Statens offentliga utredningar
SvJT	Svensk Juristtidning
TL	telelagen (1993:597) (the Swedish Telecom Act)
TR	tingsrätt (district court)

References

Literature

Borgström, P, Lindborg, L, *Säker data- och telekommunikation*, Affärsinformation AB, Stockholm 1992.
Grabosky, PN, Smith, Rossell G, 1998, *Crime in the Digital Age, Controlling Telecommunications and Cyberspace Illegalities*, Transaction Publishers/The Federation Press 1998.
Lloyd, Ian J, *Information Technology Law*, 3d ed, Butterworths, 2000.
Svensk Juristtidning 8/92.
Televärlden.

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

BRÅ-rapport 2000:2, *IT-relaterad brottslighet*
SOU 1992:110, *Information och den nya InformationsTeknologin - straff- och processrättsliga frågor mm*
SOU 1998:46, *Om buggning och andra hemliga tvångsmedel*

Conventions, Directives and Legislation

Convention on Cyber Crime, ETS No. 185.
European Convention on Human Rights 1950 Council Resolution of 17 January 1995 *on the Lawful Interception of Telecommunications* (9529/95 ENFOPOL 90).
Recommendation 2/99 on the respect of privacy in the context of interception of communications.
Directive 2002/58/EC of 12 July 2002 on Privacy and Electronic Communications.
Lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål (The Swedish act on interlocutory measures applying to investigation concerning certain crimes).
Lagen (2003:389) om elektronisk kommunikation (The Swedish Act on Electronic Communications).
Personuppgiftslagen (1998:204) (The Swedish personal Data Protection Act).
Rättegångsbalken (The Swedish Procedural Code).
Sekretesslagen (1980:100) (The Swedish Secrecy Act).
Telelagen (1993:597) (The Swedish Telecom Act).