Project Number	**AC095**
Project Title	**ASPeCT: Advanced Security for Personal Communication Technologies.**
Deliverable Type	**Major**
Security Class	**Public**

Deliverable Number	**D25**
Title of deliverable	**Legal aspects of fraud detection**
Nature of deliverable	**Report**
Document reference	**AC095/KUL/W26/DS/P/25/1**
Contributing WP	**WP2.6**
Contractual Date of deliverable	**July 1998 (Y4M5)**
Actual Date of Delivery	**24 December 1998**
Editor	**MarkHyland (KUL)**

Abstract	This report has been written with the objective of determining the legal rules applying in the various fields of law affected by the use of fraud detection systems by mobile communications operators or service providers.
Keywords	**ACTS, ASPeCT, telecommunications fraud, GSM, UMTS, privacy, personal data, electronic evidence,**

ASPeCT

Advanced Security for Personal Communications Technologies

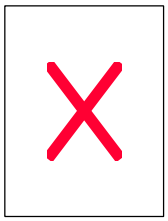
WP 2.6: Legal Issues

Final Report

Jos Dumortier

Mark Hyland

Diana Alonso Blas



http://www.law.kuleuven.ac.be/icri/

ACKNOWLEDGEMENTS

To compose this report we were very pleased to have received contributions of the following correspondents from the E.U. Member States:

- Mr Ulrich Wuermeling – Germany
- Ms Maeve McDonagh – Ireland
- Mr. H.W. K. Kaspersen and Mr Jan Peter Bergfeld – The Netherlands
- Mr Lionel D. Fernandez – Spain
- Mr Walter Jaburek – Austria
- Ms Lucilia Seixas – Portugal
- Ms Britt Marie Svensson – Sweden
- Ms Giusella Finocchiaro and Désirée Fondaroli – Italy
- Mr Matti Vasara and Mr Paivi Maunuksela-Malinen – Finland
- Mr Mark Hyland – England & Wales
- Mr David Stevens – Belgium
- Mr Paul Lambert – Belgium

Jos Dumortier

Mark Hyland

Diana Alonso Blas

December 1998

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

This report has been written in the context of the ASPeCT-project. It has, as its objective, the determination of the legal rules applying in the various fields of law affected by the use of fraud detection systems by mobile communications operators or service providers.

Mobile telecommunications operators use call data records for fraud detection purposes. These data records are called toll tickets. They contain details relating to every mobile phone call attempt. Toll tickets are transmitted to the network operator by the cells or switches that the mobile phone was communicating with. They are used to determine the charge to the subscriber, but they also provide information about customer usage and thus facilitate the detection of any possible fraudulent use.

We examined four legal questions with regard to the use of fraud detection systems:

1) Don't operators monitoring calls on the network for fraud detection purposes, act against the fundamental principle of the **confidentiality** of private telecommunications? The confidential character isn't limited to the content of the calls but extended to all kinds of data with regard to the call, such as the identity of the calling and the called party, the time and the duration of the call, etc.

2) Are operators processing call data for fraud detection purposes, controllers of a processing of personal data in the legal sense? If so, what are the consequences of the application of personal **data protection** rules? Which law will be applicable to the processing of call data, when more than one country is involved as is often the case in the context op mobile communications?

3) Given the fact that the results of the fraud detection system is always computer-readable data, how has this data to be presented as **evidence** in court? Will the courts in the E.U. Member States accept the data resulting from fraud detection systems as admissible evidence?

4) If the data resulting from the fraud detection system is accepted and there is no doubt that fraud has been committed, how will the different fraud types identified in mobile telecommunications be legally qualified? Is telecommunications fraud considered as a specific type of crime or do we have to use general qualifications such as theft, ...

Each of these questions is dealt with in a separate chapter of this report.

As far the issue of telecommunications privacy is concerned, there seem to be three types of national legislation with regard to the possibility for network operators or service providers to process call data concerning their subscribers.

- A first type of legislation doesn't explicitly grant an exception to network operators or service providers to process call data but accepts such practices implicitly.
- A second type of legislation explicitly grants an exception to network operators to register call data as far as this is necessary for the proper functioning of the network or the provision of the telecommunications service.
- A third type of legislation explicitly grants an exception to network operators or service providers to register call data for fraud detection purposes but may submit this exception to specific conditions.

It is evident that the data protection laws of the E.U. Member States, enacted over a period of more than twenty years, contain a wide variety of solutions. It is precisely on this point that the European Commission took the initiative to propose a Directive in this field. This Directive – 95/46/EC – was enacted on 24 October 1995. All Member States of the E.U. have to transpose the provisions of this Directive in their national law by 24 October 1998 at the latest.

At the time of writing these pages, all the Member States are changing their data protection law in order to make it compatible with the provisions of the European Directive.

For the ASPECT-project it doesn't seem useful to describe the current law of every single E.U. Member State in this area, because it will be subject to considerable changes on a very short term. Because every national law has to be the transposition of provisions of the European Directive, it is primordial to analyse the text of the Directive and examine the practical consequences for the processing of personal data in the context of mobile communications fraud detection. It should however be kept in mind that data protection legislation only applies where "personal data" is being processed. Call data from which every possibility to identify the person concerned has been removed, is not considered as personal data in the legal sense.

An essential principle of the European data protection Directive is the so-called "finality principle" stating that personal data collected for a certain purpose (billing, for example) should not be used for other – secondary – purposes, unless certain conditions have been fulfilled. One of the conditions is the duty to inform the data subject about the secondary use.

The European data protection directive contains also very specific rules about the question which law has to be applied when personal data are processed in more than one Member State. The criterion set forward by the Directive is the "establishment of the controller". Export of personal data outside the European Union is forbidden to countries without an "adequate level" of personal data protection".

Electronic data is adducible as evidence in all the EU Member States.. Legislation enacted in 1984 (UK) and 1992 (Ireland) ensure the admissibility of such evidence in the common law jurisdictions while the principle of free proof is used in the civil law jurisdictions to guarantee the admissibility of data as evidence. In addition, civil law courts sometimes have a broad discretion regarding what they will accept as evidence.

The last chapter of this report focuses on the issue of how one legally qualifies various types of mobile telecommunications fraud. Does the law of the E.U. Member States contain a legal qualification of "telecommunications fraud" as a specific incrimination. Is there a specific criminal treatment of telecommunications fraud. Or do we have to fall back on traditional criminal categories such as theft, deceit, forgery, etc.

The task of qualifying different types of cellular fraud does not fit neatly into one particular field of law. In addition to qualifying the different types of cellular fraud, the last chapter also contains the relevant legislation used to prosecute cellular fraud and the possible legal remedies available to counteract mobile fraud in the relevant member states.

II. TELECOMMUNICATIONS PRIVACY

A. INTRODUCTION

A mobile communications network operator planning to register call data for fraud detection purposes has to take into account the legal rules concerning the protection of telecommunications privacy.

The starting principle of these rules is the confidential nature of all private communications. The confidentiality doesn't only include the content of the calls but also concerns all other data relating to the calls such as the identity of the correspondents, their location, the time and the duration of the call, etc.

The question in this chapter is therefore the following one: can the rules with regard to the confidentiality of private telecommunications constitute an obstacle for the processing of call data for fraud detection purposes?

The right of the individuals to keep their communications confidential is recognised at international level, in the European Convention for the Protection of Human Rights and Fundamental Freedoms[1] and in the very recently adopted European directive concerning the processing of personal data and the protection of privacy in the telecommunications sector[2].

Also the national laws of the Member States, and sometimes even the Constitutions, contain provisions protecting the confidentiality of communications.

These rules are however not absolute and often exceptions are provided by the national laws in order to allow police, courts or other authorities to circumvent the privacy of communications.

This first chapter aims at analysing the national rules regarding confidentiality of telecommunications and the exceptions to these rules The aim is to evaluate any possible legal problems which network operators can face when putting in practice fraud detection systems in the field of mobile communications.

B. ARTICLE 8 OF THE EUROPEAN CONVENTION OF HUMAN RIGHTS

It is recognised at the international level that everyone has the right to respect for his private and family life, his home and his correspondence, as it is stated in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

However, this article of the European Convention of Human Rights (ECHR) allows certain exceptions to this rule when the following conditions are fulfilled:

any interference with this right should be in accordance with the law: this means that the network operator can only take fraud prevention measures which interfere in one way or another with the privacy rights of the mobile telephone users if this interference is regulated by a law.

the interference should be necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder of crime, for the protection of heath or morals or for the protection of rights and freedoms of others.

---

[1] This Convention was signed in Rome on the 4th of November 1950, in the framework of the Council of Europe.

[2] Directive 97/66/EC of the European Parliament and the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ [1998] L 24, Volume 41, of 30 January, p. 1.

The European Court of Human Rights has clarified somehow the scope of these conditions in the framework of the Malone case[3], in which the applicant alleged violation of article 8 of the ECHM under two heads:

Interception of his postal and telephone communications by or on behalf of the police;

"Metering" of his telephone by or behalf of the police.

Regarding the first condition, the Court made it clear that the expression "in accordance with the law" should be interpreted in the light of the general principles as stated in the Sunday Times judgement of 26 April 1979[4] to apply to the comparable expression "prescribed by law":

The word "law" is to be interpreted as covering not only written law but also unwritten law.

The interference in question must have a basis in domestic law.

Both expressions were however also taken to include requirements over and above compliance with domestic law. Two of these requirements are the following:

- the law must be adequately accessible;
- a norm can not be regarded as law unless it is formulated with sufficient precision to enable the citizen to regulate his conduct[5].

The Court also reiterated its opinion that the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention.

It appears at first sight that the second condition imposed by article 8.2 of the ECHR will be less difficult to satisfy since it is clear that the measures which a network operator might wish to put into practice to prevent fraud are motivated by the need for preventing a disorder or crime: fraud.

However, it should be also taken into account that the European Court of Human Rights specified, in the above-mentioned Malone case, that an interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse.

The essential rule to be deducted from the analysis of article 8 of the European Convention of Human Rights is that any exception on the principle of the confidential nature of private communications has to be based on a law. The conclusion is that a network operator or service provider is not allowed to process call data for fraud detection purposes unless a law permits him to do so.

C. ARTICLE 5 OF THE EUROPEAN TELECOMMUNICATIONS PRIVACY DIRECTIVE

After more than seven years of negotiations, the European telecommunications directive was formally approved by the Telecommunications Council on the 1st of December 1997 and published in the Official Journal of 30 January 1998. This directive bears the date of 15th December 1997.

The aim of this directive is to apply for the specific purposes of telecommunications networks the general data protection principles laid down in Directive 95/46/EC[6]. It is designed, in a

[3] Malone judgement of 2 August 1984, Publ. Court, Series A, vol. 82, page 30 and following.

[4] Series A, no. 30.

[5] Sunday Times judgement, p. 31, § 49; Silver and other judgement, p. 33, §§ 87 and 88.

constantly changing field, to prevent Member States 'legislation from developing along different lines in ways which may jeopardise the single market in telecommunications services and terminal equipment, while ensuring a high level of protection for the rights of individuals, in particular, their right to privacy.

This directive emphasises the increasing risk associated with automated storage and processing of data relating to subscribers and users[7].

The European telecommunications privacy directive can have important consequences for the ASPeCT project since it regulates the type of information that telecommunications operators may collect on their customers and extends protection to subscribers who are natural and legal persons. According to this directive, traffic data collected by telecommunications operators must be in principle erased or made anonymous at the end of the call.

It will be necessary to take into account the provisions of this directive, together with the ones of the general data protection directive of 1995[8], at the moment of building security tools for the detection of fraud in mobile telecommunications.

The telecommunications privacy directive contains specific provisions dealing with security and confidentiality of the communications, processing of traffic and billing data, itemised billing, presentation and restriction of calling and connected line identification, automatic call forwarding, directories of subscribers, unsolicited calls, technical features and standardisation.

In particular, article 6 of the draft directive, which refers to traffic and billing data, can play a fundamental role in the ASPeCT context since it specifically refers to the use of these data for purposes of fraud detection and makes this use subject to certain conditions[9].

The most important article of this directive when dealing with telecommunications privacy is article 5, which is dedicated to the confidentiality of the communications.

This article reads as follows:

"1. Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14(1).

2. Paragraph 1 shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication."

The content of article 5 of the European telecommunications privacy directive is actually very similar to the article 8 of the European Convention of Human Rights. In practice, it brings us exactly to the same conclusion: the confidentiality of communications should be respected as a general principle but certain exceptions are allowed when they are authorised by law.

In other words, the solution will have to be found by examining the national legislation of the Member States; as we will do in the following section of this chapter.

The deadline for implementation of this directive is October 1998, with a two-year extension for the provisions in confidentiality of telecommunications (article 5 of this directive).

---

[6] See ALONSO BLAS, D., *The implications of the new European privacy directive on telecommunications,* Proceedings of the 9th ACTS Concertation Plenary and Domain Meetings, 17-18 February 1998, ACTS, European Commission, DG XIII, Directorate B, p. 213-216.

[7] See recital n. 6 of the preamble to this directive.

[8] European directive 95/46/EC of the European Parliament and 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, OJ L 281, 23.11.95., p.31.

[9] We will discuss the consequences of this article more in detail in the second chapter of this report.

D. NATIONAL LEGISLATION

Not only the European Convention of Human Rights but also the European Telecommunications Privacy Directive require the existence of a law as a condition "sine qua non" for network operators or service providers wishing to register call data for fraud detection purposes. Therefore we have to look at the national laws of the E.U. Member States to examine whether or not such a law exists and how it is formulated.

There seem to be three types of national legislation with regard to the possibility for network operators or service providers to process call data concerning their subscribers.

- A first type of legislation doesn't explicitly grant an exception to network operators or service providers to process call data but accepts such practices implicitly.
- A second type of legislation explicitly grants an exception to network operators to register call data as far as this is necessary for the proper functioning of the network or the provision of the telecommunications service.
- A third type of legislation explicitly grants an exception to network operators or service providers to register call data for fraud detection purposes but may submit this exception to specific conditions.

1. IMPLICIT ACCEPTANCE

In most of the E.U. Member States there is no explicit legislation with regard to the possibility of telecommunications network operators or service providers to monitor and process call data concerning their subscribers. This doesn't however mean that such a monitoring or processing is not allowed in these Member States. The registering of call data can often be deduced from other legal rules. The classical example is the existence of rules containing the obligation by network operators or service providers to deliver call data to law enforcement authorities in the context of criminal proceedings. The application of this rule presupposes that operators and providers have the permission to register this kind of data. A typical example is Finland.

The inviolability of the privacy of one's personal life, home and postal, telephone and other confidential communications is guaranteed in Finland as a constitutional right in article 8 § 2 of the Finnish Constitution. Article 8 § 2 of the Constitution provides that the privacy of postal, telephone and other confidential communications is inviolable.

The inviolability of privacy of confidential communications is however not absolute. According to article 8 § 3 of the Constitution, legislation may be passed setting forth absolutely necessary restrictions on the privacy of communications during periods of imprisonment or during preliminary investigations, trials and security checks concerning crime that threaten an individual's or society's security or privacy of the home. An example of this is article § 29.2-3 of the Finnish Telecom Act and Article § 5a of the Coercive Measures Act , which grant police the power to tap telephone wires.

Section 50 of the Telecommunications Market Act of 1997[10] deals with the secrecy obligation of telecommunications operators, which may not disclose information regarding the content of a telecommunications message that has come to his knowledge in connection with his work.

The secrecy obligation also applies to the identities of telecommunications parties as well as to any information making their identification possible.

Without prejudice of the secrecy obligation provided in paragraph 1 of section 50, the police may, by permission of the holder of the telecommunications subscription, obtain:

[10] Act 396/1997.

1) identification information of telecommunication connections made to the subscription necessary for solving a crime referred to in chapter 24, section 3a of the Penal Code;

2) identification information relating to messages sent from a mobile station as far as this is necessary for solving a crime due to which the mobile station or a subscription used therewith is unlawfully in the possession of another.

Notwithstanding the provisions of paragraph 1 and an agreement between a user and a telecommunications operator on the secrecy of identification information regarding the telecommunications subscription of the user, the telecommunications operator shall have the right to disclose to the police, or rescue authority who has received an emergency call or to other authorities who receive emergency calls identification information regarding the subscription from which an emergency call has been made.

The identification information to be disclosed may, in addition to the subscription number, include also information on the installation address and holder of the subscription as well as on the location of the support station through which the emergency call from a mobile station has been routed to the public telecommunications network.

The right of an authority to obtain identification information of a message transmitted through telecommunications in other cases for the pre-trial investigation of a crime shall be governed by the Coercive Criminal Investigation Means Act. Coercive Measures Act § 5a: 9 obliges telecommunications operators to provide the connections, personnel and information necessary for tapping and monitoring telecommunications lines. Operators should be compensated out of governement funds for cost arising from this obligation.

No one who, in connection with performing his tasks referred to in the Telecommunications Market Act or in provisions or orders issued thereunder, has learned of a business or professional secret may disclose it to a third party or use it for his own benefit.

In addition to this, § 29 of the Telecommunications Act and § § 9- 10 of the Telecommunications Decree[11] prohibit present and past employees of telecommunications operators from unlawfully disclosing the contents of communications or information by which the parties to the communications may be identified. Violations of this provision are punishable under Criminal Code § 38:1.

2. EXPLICIT PERMISSION: PROPER FUNCTIONING OF THE NETWORK

A second category of legislation gives telecommunications network operators and/or service providers the permission to register call data but only insofar as it necessary for the "proper functioning of the network. Typical examples of this kind of legislation can be found in the Netherlands, Belgium and Sweden.

The confidentiality or secrecy of communications in **the Netherlands** with regard to telephone and telegraph is laid down in article 13 subsection 2 of the Dutch Constitution:

"The right to telephone and telegraph secrecy is inviolable, except in the circumstances prescribed by law with permission of those appointed by law to give this permission."

Article 6 of the current Telecommunications Act states that only authorised personnel of the Network Operators is entitled to take note of communications and only to guarantee the proper functioning of the service.

The same principle can be found in article 139c. Criminal Code:

[11] Decree 1996/374.

"1. Any person intentionally using a technical device to tap or record data transmitted using the telecommunications infrastructure, a telecommunications facility used for public service or terminal equipment connected thereto, which data is not intended for him alone, for him as well as others or for the person on whose orders he is acting, shall be liable to a term of imprisonment not exceeding one year or a fine of 25,000 guilders.

2. Paragraph 1 shall not apply to tapping or recording:

a. data received via a radio-electric receiver, unless a special effort has been made or a prohibited receiver has been used in order to make reception possible;

b. by or on the orders of the person entitled to use the telecommunications connection, except in instances of obvious abuse;

c. in the interests of the proper operation of the telecommunications infrastructure or of a telecommunications facility used for public service, in the interests of criminal procedure or, on the special joint orders of the Prime Minister, the Minister of Justice, the Minister for Home Affairs and the Minister of Transport and Public Works, to be given to the Head of the Internal Security Office for a period of no more than three months at a time, in cases in which such action is required in the interests of the security of the state.

The Dutch Telecom Act imposes a duty on licensed mobile telecom-operators to take such measures that they can respond to an order by the competent authorities to intercept certain communications over their infrastructure.

The relevant regulations in this area are art. 64 and 64a Telecommunications Act and the Decree Tapping Mobile Telecommunication GSM.[12] The latter contains all kinds of obligations for mobile telecom operators with respect to technical features and information about the mobile equipment used by the subscribers. On the basis of art. 64 Telecommunications Act telecommunication providers and mobile telecom operators are obliged to co-operate with the law in order to tap or record telecommunications messages.

The Netherlands is presently also implementing the Resolution of the Council of the European Union with respect to the international specific provisions concerning the legal interception of telecommunication of January 17, 1995 in its new Telecommunications Bill.[13]

Under Dutch criminal law, a wiretapping warrant can only be issued by an examining judge, on demand of the public prosecutor and in the context of a criminal inquiry into an offence for which pre-trial detention is possible. The prosecutor must provide convincing indications that the suspect takes part in the communications on the line to be tapped.

In 1993 and 1994, 3,619 and 3,284 telephone lines respectively were tapped on behalf of Dutch justice. Compared to other countries these are very large numbers. In 35 of the 95 cases in the WODC study, the most severe offence involved was drug trafficking. Fraud theft and receiving stolen goods accounted for 12, 11 and 9 cases respectively; arson, homicide and robbery for 8 cases each.[14]

As in every other E.U. Member State, the law in **Belgium** protects very strictly the confidential character of private telecommunications. The relevant provisions can be found in the law of 21 March 1991 regulating the telecommunications market and in the Criminal Code.

The central provision is article 109terD of the law of 21 March 1991:

---

[12] August 18, 1994, Stcrt. 162 and with respect to art. 2 (2) of the Decree: February 26, 1996, Stcrt. 43.

[13] See TK II 25 533 1996-1997, especially Chapter 13. Brussels, August 28 1995 (06.09) (OR.f) 9529/95 ENFOPOL 90; TK 24679, 1995-1996.

[14] Reijne e.a., Tappen in Nederland, Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC),Gouda Quint, 1996, p. 53

"Unless the consent has been obtained of all the persons directly or indirectly involved in the information, identification or data mentioned hereafter, it is forbidden for anyone

1. with fraudulent intention to take knowledge of the existence of signs, signals, writings, images, sounds or data of any kind exchanged by means of telecommunications, originating from and destined to other persons;
2. with fraudulent intention to register or eliminate the information sub 1° with technical means of any kind or to identify the other persons;
3. to intentionally take knowledge of data with regard to telecommunications relating to other persons;
4. to communicate, to use, to modify or to delete the information, identification and data sub 1, 2 and 3."

As such, the confidential character of private telecommunications, including telephone calls, is consequently very strictly protected in Belgium. Notice that the article doesn't protect the confidential character of the content of the messages. The protection of the confidential character of the content of the messages is regulated in the Belgian Criminal Code. The provision of the law of 21 March 1991 envisages explicitly the protection of all other aspects of the message, such as the identity of the correspondents, the time and the duration of the call, etc.

Of course there have to be some exceptions to the general principle of the confidentiality of private telecommunications. These exceptions are enumerated in article 109terE of the Belgian law of 21 March 1991. This article mentions three exceptions:

1. when the law permits of imposes the activities mentioned in the former article;
2. when the activities mentioned are exclusively aimed at monitoring the good functioning of the network and the good provision of the telecommunications service;
3. when the activities are aimed at making possible the intervention of emergency and help services when they receive emergency calls directed to them

The first exception points principally to the articles in the Code of Criminal Procedure concerning wiretapping of telephone calls on the request of a judge.

The second exception is relevant for network operators or service providers planning to use call data for fraud detection purposes. It allows the monitoring of the calls on the network under the condition that it is done "exclusively for the good functioning of the network or the good provision of the telecommunications service".

In **Sweden,** the confidentiality of communications is regulated in the Penal Code (Brottsbalken), chapter 4 section 8 and 9a, and in the Data Protection Act 1973:289 (Datalagen), section 21.

The same issue is as well regulated in section 25 of the Telecommunications Act 1993:597 (Telelagen).

Two sections of chapter 4 of the Swedish Penal Code[15] deal with the confidentiality of telecommunications. In the context of this report, section 24 is the most important one.

In Sweden network operators are excluded from the legal provisions protecting the confidentiality of telecommunications. The Swedish Telecommunications Act, section 24, states that "a telecommunications message may be monitored in the telecommunications activity only to the extent that this is necessary in order to carry on the activity". This provision gives the network operators a right to monitor telecommunications messages from a technical point of view, for the purpose of technical control.

[15] The translation was made by the Ministry of Justice, National Council for Crime Prevention, Sweden, in 1990.

3. EXPLICIT BUT CONDITIONAL PERMISSION FOR FRAUD DETECTION

Specific rules permitting network operators and service providers to process call data for fraud detection purposes are rather seldom. One of the rare examples is Section 7 of the German Telecommunications Services Data Protection Regulation[16] of 7 June 1996:

"(1) As far as necessary in a specific case

1. the company is allowed to register, to process and to use data concerning the subscription and concerning the individual calls of their customers to detect, limit and eliminate errors and breakdowns on the network;

2. if there are written and filed authentic indications, the company and the service provider may collect, process and use standard and communications processing data necessary to investigate and preclude surreptitious use of services and other unlawful use of public telecommunications networks and its facilities used to provide telecommunications services.

(2) As far as necessary to prevent and to investigate fraudulent use of public telecommunications networks, a network operator or a service provider may process and use call data collected in such networks by extraction out of all call data of one month where there is a good reason to believe in a suspicion for illegal fraud or other faulty use of the telecommunications service. Data concerning other communications have to be deleted immediately.

(3) The Ministry of Postal Service and Telecommunications as well as the data protection supervisory authority in charge have to be informed instantly about measures taken based on subsection 2 first sentence together with a notice about the background allegation. The data subject has to be informed when it is not incompatible with the purpose of the measure taken.

(4) In the case of subsection 1 no. 2 the company may collect, process and use in a specific case the content of a transmission as far as essential to investigate and preclude the specified acts and if no other reasonable and proportional measure is available to reach the objective. Subsection 3 applies

The conclusion is that Germany has specific legal rules concerning the possibility for network operators and service providers to process call data for fraud detection purposes. There are severe limits on the amount of data that can be processed, the ministry and the data protection supervisory authority have to be informed. The data subject has to be informed as soon as this is no longer incompatible with the purpose of the measure, for instance once certainty has been obtained that there is no question of fraud.

[16] Telekommunikationsdienstunternehmen-Datenschutzverordnung - TDSV.

III. PERSONAL DATA PROTECTION

Fraud detection is essentially based on the analysis of call data. From a legal point of view call data have to be considered as "personal data" falling under the scope of the personal data protection legislation. Personal data is, indeed, all kinds of data relating to a natural person who is, or can be, identified.

Processing of individual call data is unlawful if the provisions of the national data protection laws are not respected. Basic principles such as the right of the individual to be kept informed of the purposes for which data concerning him are being processed, or to have a right of access to the personal data which concern him/her, have therefore to be taken into account.

Why is a correct application of personal data protection legislation so vital in case of mobile communications fraud detection?

The reason is that evidence collected in an unlawful manner, for instance using methods contrary to the principles of personal data protection, will not be accepted in court proceedings.

A. HISTORICAL BACKGROUND

The origin of the legislation with regard to the protection of individuals in case of the processing of personal data concerning them, at least in Western Europe, goes back to the early seventies. One of first European national laws on this issue was enacted in Sweden in 1973.

1. CONVENTION 108 OF THE COUNCIL OF EUROPE

At the same period, discussions were started in the Council of Europe with the aim to prepare a European Convention in this domain. The discussions were successful and led to the approval of Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data. It was opened for signature on 28 January 1981. Convention 108 is an important legal instrument in the data protection field, not only because of the early date in which it was enacted but also because of the generality of the principles, which are set out in a manner which allows adaptation to evolving situations.[17]

The purpose of the Convention, as stated on its article 1, is "to secure in the territory of each Party for every individual, respect for his rights and fundamental freedoms, and, in particular, his right to privacy, with regard to automatic processing of personal data relating to him". Data protection is considered a fundamental human right, intimately linked to the right of privacy (article 8 of the European Convention on Human Rights and Fundamental Freedoms).

The key-idea on which the Convention is based is that uniform principles for privacy protection which are applicable throughout different States provide a legal safety net for individuals and help to resolve international conflicts[18]. The Convention is, however, of a non-self-executing character, what in practice means that individuals may not directly invoke the Convention before their national Courts. The Convention holds mainly obligations for the States themselves. The principal obligation for them, resulting from the Convention, is the obligation to enact a national data protection law. The existence of such a law is a prerequisite for the ratification of the Convention.

Article 12 deals with transborder flows of personal data. The aim of this article is to reconcile the requirements of effective data protection with the principle of free flow of information, regardless of

---

[17] Council of Europe, New technologies: a challenge to privacy protection? Study prepared by the Committee of experts on data protection under the authority of the European Community on Legal Co-operation, Strasbourg 1989.

[18] Rostoker, M.D. and Rines, R.H., Computer jurisprudence: legal responses to the information revolution, Oceana publications, INC, USA, 1986, chapter VII.

frontiers, enshrined in article 10 of the European Convention for Human Rights[19]. This principle of free flow of personal data inside Europe could be very important in the area of mobile communications fraud detection.

The Convention has been ratified by all Member States of the European Union. The text of the Convention has also served as inspiration for most of the national data protection laws in Europe and recently also for the Directive 95/46/EC of the Council and the European Parliament, which will be the basic legal text in this domain in Europe for the forthcoming years.

2. NATIONAL DATA PROTECTION LAWS IN EUROPE

In a time span of more than two decades, from 1973 – the enactment of the data protection act in Sweden – till 1996 – the year of the enactment of the last data protection law in the European Union, in Italy – every Member State of the European Union has adopted its own data protection law.

Table 1 gives an overview of these national laws

19 Explanatory chapter on the Convention for the protection of individuals with regard to automatic processing of personal data, Convention opened for signature on 28 January 1981, Strasbourg 1981.

Table 1: National Data Protection Laws in the E.U[20].

Member State	Title	Enactment
Austria	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG)	1978
Belgium	Loi relative à la protection de la vie privée à l ĕgard du traitement de données à caractère personnel	1992
Denmark	Lov nr. 293 om private registers Lov nr. 294 om offentlige myndigheders registers	1978
Finland	Personal Data Files Act Law nr. 471/87 (Laki Henkilörekisterilaki)	1987
France	Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés	1978
Germany	Bundesdatenschutzgesetz	1990
Greece	Law on the Protection of Individuals with regard to the Processing of Personal Data	1996
Ireland	Data Protection Act	1988
Italy	Legge n. 675. - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali	1996
Luxembourg	Loi réglementant l'utilisation des données nominatives dans les traitements informatiques	1979.
Portugal	Lei da Protecção de Dados Pessoais face à Informática	1991
Spain	Ley orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal (LORTAD)	1992
Sweden	Datalagen	193
The Netherlands	Wet houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties	1988
United Kingdom	Data Protection Act 1998[21]	

[20] Before the transposition of Directive 95/46/EC

[21] http://www.hmso.gov.uk/acts/acts1998/19980029.htm;

3. PRESENT STATUS

It is evident that the data protection laws of the E.U. Member States, enacted over a period of more than twenty years, contain a wide variety of solutions. In 1973, when the first law was enacted in Sweden, the IT landscape was dramatically different from the one in the nineties. Mainframe computing was still predominant and limited to large organisations. This explains for instance why the first laws still started from the belief that individuals could be protected ideally by requiring a state license for every single processing of personal data. For the legislator acting in 1992, when personal computing had conquered the world, such a licensing regime didn't seem practicable.

Because the Convention 108 of the Council of Europe was formulated in extremely general wordings, it allowed a wide variety. It is precisely on this point that the European Commission took the initiative to propose a draft Directive in this field. This Directive – 95/46/EC – was enacted on 24 October 1995. All Member States of the E.U. have to transpose the provisions of this Directive in their national law by 24 October 1998 at the latest.

At the time of writing these pages, all the Member States are changing their data protection law in order to make it compatible with the provisions of the European Directive.

For the ASPECT-project it doesn't seem useful to describe the current law of every single E.U. Member State in this area, because it will be subject to considerable changes on a very short term. Because every national law has to be the transposition of provisions of the European Directive, it is primordial to analyse the text of the Directive and examine the practical consequences for the processing of personal data in the context of mobile communications fraud detection.

B. THE EUROPEAN DATA PROTECTION DIRECTIVE

1. OBJECTIVE: FREE FLOW OF PERSONAL DATA

The European Directive is based on the fact that differences in the level of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State. This difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law.

Art. 1.2 of the Directive clearly and unambiguously establishes the basic principle that within the EU, there shall be no prohibitions or restrictions in the free flow of personal data between the Member States for reasons connected with the protection of the right of privacy. This text is substantially different of the one of the Council of Europe Convention 108 under which it was possible for a Member State to forbid the export of data to EC countries with a low level of protection.

The Directive thereby fulfils one of its two basic aims, to ensure such free transfer of data within the European Union, considered as vital for the functioning of the Single Market, which will not be anymore restricted by the existence of different national laws with different provisions regarding the trans-border flows of information. Differing requirements originated at national level naturally affect the overall design and operation of any intended international network or database arrangement[22].

As far as non-EC countries are concerned, the transmission of personal data is restricted if the country in question lacks an adequate level of data protection (article 25). The adequacy of the level of protection afforded by a third country must be interpreted in such a way to ensure that privacy of

22 Hoyle, Chris, Trans-border data flows: many barriers stand in the way for users, The international computer lawyer, Volume 1, Number 1, November-December 1992.

the citizens is not endangered by the export. It shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of transfer operations.

The text of the Directive attaches special importance to the existence of an independent supervisory authority in each Member State, that is seen as an essential component of the protection of individuals with regard to the processing of personal data and to which very relevant functions should be entrusted.

2. SCOPE OF THE DIRECTIVE

The scope of application of the data protection Directive is defined in its article 3, saying that it will apply to *the processing of personal data wholly or partly by automatic means and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.* Two elements need therefore to be defined: personal data and processing.

a) Personal data

The Directive defines *personal data* in article 2 (a) as

"any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or identifiable, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

This means that, if the data subject is not identifiable, the principles of the Directive will not apply any longer.

Call data processed for fraud detection will not be considered as personal data if not linked to individual natural persons. Anonymous data is not considered to be personal data and do not fall under the scope of personal data protection legislation. In case of absolute anonymity, i.e. if there is absolutely no possibility to return back to the individual from whom the data originated, there is no question of personal data and the data protection rules don t consequently apply.

As long, however, as, starting from the data, ANYONE is able to identify the person concerned, the data remain under the scope of personal data protection. Personal data encrypted or encoded, are therefore to be considered as personal data.

As it can clearly be deduced from the above-mentioned definition, data on legal persons – companies, societies, associations, public bodies, etc. - are not covered by the Directive but they might be covered by the national data protection legislation (for instance, in Luxembourg[23]).

Personal data concerning natural persons linked to a legal person (for example, the name of the contact person in a company) are however covered by the Directive.

b) Processing

A second important concept is the one of *processing*, which is defined in article 2 (b) of the Directive:

"processing of personal data" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

---

[23] Article 1 of the Luxembourger Data Protection Act of 31 March 1979 reads: Natural and legal persons shall be protected against the improper use of nominal data...

The material scope of application of the Directive is very comprehensive as it covers not only automated data but also data in filing systems, as well as temporary collections of data such as copies to be transmitted in the context of disclosure, back-up copies and scratch files[24].

c) Controller and Processor

Article 2 of the Directive contains the definitions of controller and processor. It is worded as follows:

(d) "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller and the specific criteria for his nomination may be designated by national or Community law.

(e) "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

It is fundamental to know who is the controller in each case since the law applicable to a processing is determined by the place of establishment of the controller and the Directive imposes very relevant obligations and responsibilities to the controller:

- with regard to the rights of the data subjects,
- with regard to the adequacy of the data, , security, liability in front of any person who has suffered damages...
- with regard to the notification to the supervisory authorities

Although the tasks of the processor are less important than those of the controller, he still has certain important obligations to fulfil, with regard to the security and confidentiality of the processing[25]

It is very important to know exactly who is the controller in case of processing of personal data for fraud detection purposes. Is it the network operator or the service provider? Who is the controller when fraud detection isn't performed at the level of the single national companies of an international network operator but centralised at the level of the headquarters? In this case the international headquarters will be considered as the controller of the processing of personal data.

---

[24] See chapter 6 (Payment systems, data protection and cross-border data flows, by Jan Berkvens) of the book of Norton, J., Reeds, C. and Walden, I., Cross-border electronic banking, Challenges and opportunities, Lloyds of London Press Ltd, 1995

[25] Article 17 of the Directive, paragraph 1, reads as follows:

"Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and the organisational measures governing the processing to be carried out, and must ensure compliance with these measures."

3. BASIC DATA PROTECTION RULES

a) The "finality" principle

Article 6 of the Directive, included in the section entitled *Principles relating to data quality*, reads as follows:

1. Member States shall provide that personal data must be:

(b) collected for specified, explicit and legitimate purposes[26] *and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that the Member States provide adequate safeguards.*

2. It shall be for the controller to ensure that paragraph 1 is complied with.

This principle is generally known as the finality principle and it means that data should always be collected and processed for a given purpose, they can not just be collected and processed at random.

The purpose of the collection can moreover not be a very general one, such as *"for business purposes"*, but has to be more specific. Each processing operation should have expressly specified purposes. Wide formulations of purposes or objectives should be avoided. When the processing operations refer to a concrete article or clause of a legal text, this should be clearly identified by the controller

If not, one should make sure that the precise purpose of each concrete operation is specified.

When call data are processed for fraud detection purposes the finality principle is very important. According to the data protection rules call data are collected for a specific purpose, namely billing. This purpose has to be communicated to the person concerned. If call data collected for billing purposes, are used for other purposes, for instance for fraud detection, this purpose should be specified from the start. This could be done in a clause to insert in the subscription agreement.

b) Necessity of the processing of personal data

Personal data should only be collected and processed when this is strictly necessary for the purpose of the processing.

It should therefore be examined in every single case whether the identification of a person is truly required for each processing operation taking place, step by step in the whole chain of processing

---

[26] Basing ourselves on the text of the explanatory chapter concerning the amended draft Directive (COM (92) 422 final - SYN 287), we can make the following comments concerning the terms used in article 6. 1 b) , when referring to the purpose of collection of personal data:

- "Specified": The aim of the collection and use of data has to be defined in a way as concrete as possible. A vague or general definition would not satisfy this requirement.

The purpose has to be specified before the data are collected and any subsequent change in the purpose of a processing operation will be lawful to the extent it is compatible with the initial purpose.

- "Explicit": This term was not contained in the text of the Council of Europe Convention. It relates to registration with the data protection authorities; in such a case, the purpose of the collection and use of the data should be clearly stated in the registration.

- "Legitimate": The potential purposes of processing personal data are therefore limited: a processing operation may only be designed and performed for a purpose permitted by the Directive and by the domestic legislation in the Member States.

of personal data for fraud detection purposes. For the areas where the identification of the persons is not necessarily required, two possibilities exist:

1. to restrict the use of information which could lead to the identification of persons, or

2. in certain circumstances, to make use of techniques to prevent identification, such as, for instance, identity protectors, whose effect is to cordon off certain areas of the processing system which do not require access to true identity[27].

c) Lawfulness of the processing of personal data

Article 7 of the Directive enumerates the cases in which the processing of personal data will be considered legitimate by the Member States:

Member States shall provide that personal data may be processed only if:

(a) the data subject has given his consent unambiguously; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interest of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed; or

(f) processing is necessary for the purpose of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection pursuant to Article 1 (1).

Only in the above-mentioned cases the processing of personal data can be allowed by the Member States. Within these limits, they can define in a more precise way the conditions but they may not change or broaden them[28].

The consequence of this in the ASPECT context is that one has to make sure that the processing activities taking place for fraud detection fulfil the requirements of one or more of the letters of article 7 of the Directive. When reading this article, it is important to realise that some of the notions mentioned, such as *public interest*[29], are explained in other parts of the Directive and can not be interpreted in a broad way.

For the processing of call data for fraud detection purposes, it should be examined whether the processing activities carried out in this context fulfil one or more of the conditions imposed in article 7 of the Directive. Only in these cases a processing can be considered as lawful and legitimate! To obtain absolute legal certainty that processing of call data for fraud detection purposes will be considered compatible with article 7 of the Directive, it is advisable to ask the consent of the data subject. This can, for example, be inserted as a clause in the subscription agreement.

---

27 For more information about identity protectors and privacy-enhancing technologies see the chapters of the Dutch Registratiekamer in co-operation with the Information and Privacy Commissioner of Ontario: Privacy-enhancing technologies: the path to anonymity, volume I and II, Achtergrondstudies en verkenningen 5a, August 1995.

28 See article 5 of the Directive.

29 For instance, recital 34 of the preamble mentions a number of cases in which grounds of important public interest are involved.

d) The applicable law

Article 4 of the Directive determines which national law is applicable to a given processing operation. The rationale of this provision is to make sure that there should always be one -and only one- law that will govern the way in which data is collected and processed.

The criterion established by this article is that the law of the Member State where the controller has his establishment will apply to his/her data processing activities carried out in the context of the activities of this establishment.

When call data is being processed for mobile communications fraud detection, the data will probably be collected from calls all over the world. Nevertheless, if the operator who processes these data for fraud detection purposes, is established in a European Union Member State, the applicable data protection law will be the law of that Member State.

For operators having establishments in different E.U. Member States, the question will be: which is the establishment in charge of fraud detection? If one establishment is in charge of fraud detection, the applicable data protection law will be the local law of this establishment.

If each establishment of one operator is in charge of its own fraud detection, each one will have to apply its local data protection law to its own activities.

If each establishment of an international operator is in charge of its own fraud detection but transfers its call data to one central point for being processed and receive the results, each establishment will still have to apply its local data protection law. The central service will be considered as the processor for each of the establishments.

e) The data processed: are there any sensitive data involved?

It is important to analyse in detail the various categories of data supposed to be processed or exchanged in this context. By determining the nature of the data involved we will be able to assess whether the data in question are under the scope of application of the (whole or certain parts of the) Directive or not.

The Directive refers to special categories of data in its article 8, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, for which special guarantees are foreseen.

The processing of these data is in principle prohibited by article 8 of the Directive and it is only allowed in special circumstances. These circumstances are different for each Member State.

In the context of mobile communications fraud detection, there will normally no sensitive data involved, such as data concerning race, political opinion, religion, health, sexual behaviour or trade union membership. If one of these types of personal data is involved in the course of a fraud detection process, they should be eliminated unless they are strictly necessary. If they are strictly necessary, it should be carefully examined whether of not the provisions of the applicable national law permits the processing of these data.

f) Adequacy and quality of the data

The purpose of the processing will have to be communicated to the data subjects and it is also very important to determine the adequacy of the data.

Three letters of paragraph 1 of article 6 of the Directive refer to data adequacy and quality principles:

Member States shall provide that personal data must be:

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they are further processed, are erased or rectified.

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which data were collected or for which they were further processed.

The key-question one must start with is: how much personal data is truly required for the proper functioning of the information? This question should be asked prior to the design and development of any new system, for each single step foreseen in the processing operations.

As it has already been mentioned, the adequacy of the data has to be judged in relation to the concrete purpose of the processing operations in question. Knowing this purpose, the controller has to examine in each case if the data to be processed are really necessary and relevant and make sure that no superfluous data is processed or exchanged.

The controllers of the processing operations have to make sure that all the data provided are adequate and relevant on the basis of the very specific purpose for which they are collected. Especially when dealing with sensitive data, all measures should be taken to ensure that these data are only processed when this is strictly necessary. This has to be assessed on a one by one basis.

In order to guarantee that no superfluous data is provided a good idea would be to determine (when possible) sets of minimal data necessary for each situation

Data should also never be kept for longer than necessary. Once again, the specific purpose of a processing operation has to guide us in assessing the period of time for which certain data have to be kept.

Reasonable time delays have to be fixed , data can not be kept for unlimited periods of time without concrete reasons.

Personal data can not be kept for unlimited periods of times. Specific limits have to be established on the basis of the concrete purpose of the processing operations. The more particular the purpose of the processing is, the easiest this time delay will be possible to fix.

For the cases where the processing operations can last for a very long time, it will be good to re-evaluate the necessity of each processing operation after a certain period of time and see if the reason for the processing still exists.

4. RIGHTS OF THE DATA SUBJECTS

Article 10 to 14 of the Directive deal with the rights of the data subject, in particular the right to be informed, to have access to the data and to object to the processing of data.

a) Information right

Articles 10 and 11 of the Directive are dedicated to the information right of the data subjects. Two different cases are dealt with: when the data is collected from the data subject and when the data have not been obtained from the data subject.

In the first of these instances, the controller should give the following information to the data subject, unless he already has it: identity of the controller, purpose of the processing and some further information if necessary.

When the data is not obtained from the data subject, the controller should make sure that, before the data is first disclosed to a third party, the person concerned gets to know (unless he already knows) who is the controller, the purposes of the processing and, if necessary, some additional information.

It might however happen that data that are collected for a very clear purpose, known by the citizen, are also or at a later stage used for other secondary purpose that is not so obvious to the

data subject. This secondary purpose can be perfectly legal (for instance, call data can be used for fraud detection) but only if it is clearly specified and explicit at the moment of the collection.

b) Access right

Article 12 of the Directive deals with the access right of the data subjects. Three different elements should be distinguished in this article:

- The right to obtain from the controller, regularly and without excessive cost, information as to the data relating to him being processed, the purposes of the processing, the categories of data, the potential recipients, etc.
- The right of rectification, erasure or blocking of data, the processing of which does not comply with the provisions of the Directive.
- The notification to third parties to which data have been disclosed of any rectification, erasure or blocking carried out.

National legislation provides exemptions from such subject access in respect of certain data if held for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders. This exemption only applies if allowing subject access to the personal data would be likely to prejudice such a purpose[30].

5. DUTIES OF THE CONTROLLER

a) Notification to the data protection supervisory authority

As a general rule, the controllers have to notify the supervisory authority of the country whose law is applicable to the envisaged processing operations before starting any processing operations.

One should not forget that the specific procedures for notification are determined in each national law and they present visible differences, even after the transposition of the Directive.

The U.K. Data Protection Act 1984 , for instance, governs the processing of personal data and requires that anyone processing personal data must register with the Data Protection Registrar and must only process personal data in accordance with the principles set out in the Act.

There are exceptions to the obligations to register and comply with the principles relating to fraud prevention measures. In particular, the Act requires companies to describe the people to whom it intends or may wish to disclose personal data. However, the Act permits the disclosure of personal data in certain circumstances, without committing a criminal offence, even though the data user is not registered to make such disclosure;

One of these exceptions is in respect of disclosures made for the purposes of the prevention or the detection of crime or the apprehension or prosecution of offenders. This exemption only applies where failure to make the disclosure would be likely to prejudice such a purpose[31].

---

[30] Section 28(1) Data Protection Act of 1984.

[31] Section 28(3) of the Data Protection Act of 1984.

b) Transfer of personal data to countries outside the E.U.

The Directive is quite restrictive with regard to the transfers of personal data to third countries. Article 25, which establishes the principles for the transmission of personal data to third countries, prescribes that they will only take place *if the third country in question ensures an adequate level of protection.*

In the same sense it is stated in its preamble[32] that *the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited.*

Adequacy is thus the main criterion for deciding on a concrete data transfer but determining what is adequate or not, is not easy. Therefore, the second paragraph of article 25 provides some guidelines:

The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations. Particular attention should be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security matters that are complied with in those countries.

It is however not self-evident whether a country offers and adequate or inadequate level of protection. In order to facilitate and make uniform the evaluation of the adequacy of the protection offered in third countries, it would be desirable that all the Member States and the European institutions would use the same evaluation methods and criteria.

One of the criteria to be considered, from our point of view, could be the ratification of the Council of Europe Convention n° 108. This convention is open to ratification to any country, not only to members of the Council of Europe, which has a data protection law.

This convention imposes more concrete obligations than the guidelines of the OCDE or the UN. Therefore, a certain level of protection can be expected from countries which have signed and ratified this convention.

There are, fortunately, important exceptions to the general principle in article 26 of the Directive:

- When the data subject gives his consent to the transfer.
- When the transfer is necessary for a contract concluded in the interest of the data subject.
- When reasons of important public interest exist or for the establishment, exercise or defence of legal claims.
- When it is necessary to protect vital interests of the data subject;
- When the transfer is made from a register of public consultation.
- When adequate safeguards (which may result from adequate contractual clauses) exist and the transfer is authorised by a Member State.

In the cases where a problem of adequacy exist, the Commission may as well enter into negotiations[33] with the country in question in order to take measures to remedy the situation, as it is established in article 31 of the Directive.

---

[32] See recital n° 57.

[33] See article 25, paragraphs 5 and 6, of the Directive.

When an operator decides to transfer call data to countries outside the European Union, he should be extremely careful. It is at present still impossible to predict which countries will be considered to have an "adequate level of personal data protection". Therefore it is advisable to ask the consent of the data subject before transferring call data outside the European Union.

In cases where it is not possible or very difficult to ask the explicit consent of the data subjects, the transfer to third countries should be regulated in a contract between the sender and the recipient.

c) Security measures

Security is certainly a matter closely related to data protection. Therefore it is not strange to see that article 17 of the Directive considers this issue:

"Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

It is therefore for the controllers to implement adequate security measures. Without entering in the description of concrete security measures we want to affirm the strict necessity of taking solid security measures.

The question whether the security measures implemented by an operator handling call data for fraud detection purposes fulfil the requirements of article 17 of the Data Protection Directive has to be answered with regard to four criteria:

- the state of the art: this includes, for example, the use of strong encryption;
- the cost of implementation: a large company will be considered to be able to bear higher security investments than an individual person;
- the potential risks: when data is transferred over public networks, the risks are considerably higher;
- the nature of the data: because call data is considered to be very sensitive personal data, they need high security

IV. ADMISSIBILITY OF ELECTRONIC EVIDENCE

A. INTRODUCTION

The third chapter of our chapter covers the issues of whether electronic data is admissible as evidence in the courts of selected Member States of the EU and in which forms such evidence may be adduced in courts. Important issues such as relevant legislation, general court practice and requirements concerning witnesses are covered in this chapter.

1. OBJECTIVE

The need for this chapter arises from the fact that mobile telecommunications operators use call data records for fraud detection purposes. These data records are called toll tickets. They contain details relating to every mobile phone call attempt. Toll tickets are transmitted to the network operator by the cells or switches that the mobile phone was communicating with. They are used to determine the charge to the subscriber, but they also provide information about customer usage and thus facilitate the detection of any possible fraudulent use. Such data would be relied on as evidence where a case is brought against a suspected cellular fraudster.

Call data, being electronic in nature, differs from the usual paper-based evidence submitted in court. This raises two questions: Firstly, is electronic evidence adducible in domestic courts in the E.U. and secondly, if so, in which form should it be presented.

Generally speaking, electronic data is admissible as evidence in all EU Member States. Specific legislation allows for this in the EU's two common law jurisdictions, namely Ireland and the UK (except for Scotland, which has a civil law system) while the EU's civil law jurisdictions permit this type of evidence under their general freedom of proof principle. While electronic data is admissible as evidence in domestic courts, it should also be borne in mind that the legal profession is conservative by nature and certain members of the judiciary may not feel entirely comfortable dealing with this type of evidence. Another factor to consider is the disparities that exist between Member States in terms of how much they have embraced the IT revolution. Attitudinal differences become reflected in IT facilities in courtrooms and in the approach of judges.

Naturally, the rules of evidence differ from Member State to Member State. This is also true of the rules of court regulating the format in which such evidence must be adduced at trial.

The aim of this chapter is to paint a clear picture of the evidential situation prevailing in the Member States covered by this chapter. This will be beneficial for mobile operators as they will be able to determine, using the information in this chapter, the relevant legislation or legal principle governing the area of cellular fraud in the Member State concerned. This chapter also helps establish the differences and similarities that exist between Member States when it comes to admitting electronic data as evidence.

2. METHODOLOGY

The following five questions relating to presenting evidence in court were asked:

1. In which form(s) can fraud data associated with this type of fraud be presented as evidence in Court? For example, does the data have to be contained on a diskette or a CD Rom or does it have to be presented in paper form?
2. What legislation/Rules of Court/jurisprudence exist in your country which may be relevant to the way and form in which fraud data (associated with this type of fraud) may be submitted as evidence in Court? Please give a reference and include a copy (preferably in English or French) of the text(s).

3. In practice, do the Courts in your country admit fraud data (associated with this type of fraud) as evidence in forms other than those specified in legislation/Rules of Court/Jurisprudence? If so, please specify the acceptable forms.
4. Does the Court require the intervention of an independent expert to confirm that the evidence being presented to Court is the same as that generated on the computer or to decide what evidential value should be given to the data?
5. Does the operator of the computer (which contains the fraud data) have to comply with any legal requirements before the fraud data can be admissible as evidence?

The object of the questions was to place emphasis on the form in which the data should be presented as evidence. Any relevant legislation was also required as was information on possible intervention by an expert in the proceedings.

3. THE LAW OF EVIDENCE

The law of evidence is a particularly complex and difficult subject to deal with. The principal reason for this is that it relates to the innermost concepts and traditions of a country's legal system.

The term "evidence" is defined in the Oxford Concise English dictionary (ninth edition) as:

> *"information given personally or drawn from a document etc. and tending to prove a fact or proposition"*

while it is defined in Curzon's "A dictionary of Law" (second edition) as

> *"Testimony and production of documents and things relating to the facts into which the court enquires and the methods and rules relating to the establishing of those facts before the court".*

The rules of evidence differ significantly between the common law systems and civil law systems. The two common law jurisdictions in the EU, Ireland and the UK (apart from Scotland which has a civil law system) have specific legislation providing for the adducibility of electronic data (or computer-generated documents) as evidence. In some civil law jurisdictions, the principle of freedom of evidence applies i.e. all means of evidence may be produced and have free evidentiary value. In that case, the only problem that the court faces when evaluating computer-generated evidence is the weight to attach to it.

In other civil law systems, the law sets out an exhaustive list of admissible evidence. This limits the types of proof which are admissible in court to those explicitly mentioned in the list. Even if the country in question does not include electronic data in the list, the courts there may, however, have a discretion in the matter.

B. ADMISSIBILITY OF ELECTRONIC DATA AS EVIDENCE IN COURT

1. OVERVIEW

The two common law jurisdictions covered, namely, England & Wales and Ireland have specific legislation concerning the admissibility of electronic data as evidence.

Civil law jurisdictions, on the other hand, generally apply the freedom of proof principle. This means that electronic data is admissible in criminal proceedings. Examples of the freedom of proof principle at work can be seen by briefly examining the situation that prevails in the following countries:

The Netherlands: Criminal evidence rules allow for the adducibility of computer-generated evidence. It may be presented to the court in the most suitable format.

Sweden: Sweden has a system of free submission of evidence and the courts apply the principle of free evaluation of evidence. Every kind of evidence is allowed.

Finland: Finnish courts have considerable discretion as regards what data they admit as evidence. In addition, expert testimony is usually admitted in proceedings.

Germany: Electronic data is admissible as evidence in German courts. It may be adduced in court in electronic or paper format.

Austria: There are no written rules except the general rule that every kind of evidence may be presented in court.

Portugal: A diskette or CD-ROM are both acceptable as evidence in Portuguese courts. Evidential issues are determined on a case-by-case basis subject to the general law on the admissibility of evidence.

Spain: There is no jurisprudence touching on this issue. However, Spanish courts generally admit evidence in forms other than those set out in the rules of court procedure.

Italy: Acts, data and documents created by public agencies and private persons by means of computer-based or telematic systems are legally valid and may be used for any purpose of law.

2. COUNTRY REPORTS

a) AUSTRIA

There is no legislation in Austria covering the form in which fraud data should be presented in court. In practice, evidence in this type of case is presented to court as a printout and is generally dealt with as "urkunde" (documentary evidence). However, it must be pointed out that many commentators do not consider machine readable data to be evidence.

An expert often appears in these type of cases in Austria but it seems that the participation of an independent expert is not required by the court.

The operator of the computer (which contains the fraud data) does not have to comply with any legal requirements before the fraud data can be admissible as evidence.

b) ENGLAND & WALES

(a) Police and Criminal Evidence Act

The Police and Criminal Evidence Act 1984 provides for the admissibiltiy of computer generated evidence in criminal proceedings. Section 69 of the Act is framed in a negative way but essentially states that a computer-produced document may be admissible as evidence provided:

1. There are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer

2. That at all material times the computer was operating properly, or if not, any respect in which it was out of operation was not such as to affect the production of the document or the accuracy of its content.

This provision facilitates the adducibility of telecommunications data as evidence.

The aim of Section 69 is to impose a duty on anyone who wishes to submit computer-generated evidence to demonstrate that it is safe to rely on that document. There is no definition of computer in the 1984 Act, as the legislators believed that any definition would soon become redundant due to the swift rate of advance in computer technology. This deliberate decision not to include a definition of 'computer' means that the courts have to give the term its ordinary meaning rather than to apply, by analogy, the definition used in Section 5 (6) of the Civil Evidence Act 1968 i.e. 'any device for storing and processing information'.

Paragraph 8 of Schedule 3 of the PACE provides for the possibility of a certificate being tendered as evidence of any of the matters referred to in the preceding paragraph. The certificate would be evidence of "anything stated within it". It would :

1. Identify the document containing the statement and describe the manner in which it was produced

2. Give such particulars of any device employed in the production of that document as may be appropriate for the purpose of showing that the document qwas produced by a computer

3. Be signed by a person occupying a responsible position in relation to the operation of the computer.

If a certificate is submitted to court, it should be evident on its face that it is signed by a person who can give reliable evidence about the computer's operation. This allows the other side to decide whether to accept the certificate, or ask the judge to require oral evidence which can be challenged in cross-examination. Paragraph 9 of Schedule 3 recognises the higher standard of proof required for a conviction in criminal proceedings. It provides therefore that the court may require oral evidence to be given of anything which could have been given by certificate under Paragraph 8.

Paragraph 9 of Schedule 3 recognises the higher standard of proof required for a conviction in criminal proceedings. It provides therefore that the court may require oral evidence to be given of anything which could have been given by certificate under Paragraph 8.

Section 69 can be satisfied by the oral evidence of someone who is familiar with the operation of the computer and who can give evidence of its reliability. That person need not be a computer expert. This was stated in R v Shepherd,[34] where the House of Lords held that it will very rarely be necessary to call an expert to prove that the computer is reliable. Lord Griffiths said in R v Shepherd:

Computers vary immensely in their complexity and in the operations they perform. The nature of the evidence to discharge the burden of showing that there has been no improper use of the computer and that it was operating properly will inevitably vary from case to case. I suspect that it will very rarely be necessary to call an expert and that in the vast majority of cases it will be possible to discharge the burden by calling a witness who is *familiar* with the operation of the computer in the sense of knowing what the computer is required to do and who can say that it is doing it properly '

Paragraphs 11 and 12 of Schedule 3 to the 1984 Act provide guidance as to what weight if any should be attached to a statement admissible under Section 69.

In estimating the weight, if any, to be attached to a statement regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement and, in particular-

- to the question whether or not the information which the information contained in the statement reproduces or is derived from was supplied to the relevant computer, or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information; and
- to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced by it, had any incentive to conceal or misrepresent the facts.

For the purposes of paragraph 11 above information shall be taken to be supplied to a computer whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment.

---

[34] (1993)1 all ER 225

When deciding whether a statement contained in a computer-produced document is admissible in accordance with Section 69, the court may draw reasonable inferences from the circumstances in which the statement was made and from any other circumstances, including the form and contents of the document in question.[35]

(b) Jurisprudence in England & Wales:

The general course of development in English law to date had been towards permitting electronic data as evidence. It is indicative of the Law's greater willingness to meet the challenge posed by information technology to legal principles and theories. An example of this development can be seen in the recent case of Regina v Governor of Brixton Prison and Another, ex parte Levin.[36] In Regina it was held by the Court of Appeal and upheld by the House of Lords that computer printouts would be admissible as evidence in UK extradition proceedings against a Russian who allegedly committed electronic fraud (bank or wire fraud) from Russia against banks in the US. The Russian was arrested in Stansted airport on foot of an arrest warrant issued by a New York court.[37]

c) BELGIUM

The law of evidence is often divided into two systems, that of non regulated-evidence and that of regulated-evidence. In the former, all types of evidence are admissible and the judge decides on its evidential value according to his "intimate conviction". In the latter, the admissible evidence is pre-determined with a certain evidential value attached to it. Most laws of evidence are a combination of both.

Generally speaking, Belgium has a regulated-evidence system in civil law and a non regulated-evidence system in penal law. However, there are a number of exceptions to those principles. So for instance, in civil law, all mere facts (not being legal acts) can be freely proved and evaluated. While evidence in penal law is generally not regulated, evidence obtained by illegally tapping a telephone-line or by performing a house-search without a valid search warrant will not be admissible as evidence.

d) FINLAND

Cellular fraud data is usually presented as evidence in court in the form of personal testimony or in paper form. The Common regulations on the Code of Judicial Procedure govern the way and form in which fraud data may be submitted as evidence in court.

Finnish courts have considerable discretion as regards what data they admit as evidence. In addition, expert testimony is usually admitted in proceedings.

e) GERMANY

Fraud data may be presented in court in paper format (for example, an application form), personal evidence (shop staff or consumers) or electronic data. Electronic data may be presented in four forms:

1. By a witness

---

[35] Schedule 3, paragraph 14

[36] 1996 3 W.L.R. 657

[37] See for example Regina v Governor of Brixton Prison and Another, ex parte Levin (1996) 3 W.L.R. 657 where computer printouts from US banks relating to alleged electronic fraud (wire/bank fraud) committed online from Russia were admitted as evidence in extradition proceedings in an English Court.

2. By an expert-witness who has accessed the data

3. In paper form

4. In electronic format

Evidence presented in all four forms is admissible.

The admissibility of evidence adduced in a cellular-fraud case may be affected by one or more of the following points:

- Possible illegal obtainment of data which is protected by telecommunications secrecy legislation
- The principle of direct evidence (Unmittelbarkeitsgrundsatz)
- Truthfulness and likelihood of error (section 261 StPO)

The court has to reject an application for evidence to be admitted if the evidence is inadmissible and the court might reject evidence which is irrelevant. (section 244 Abs. 3 StPO)

The principle of telecommunications secrecy restricts access to telecommunications data by investigation authorities.

The court does not require the intervention of an independent expert to confirm that

- the evidence being presented to Court is the same as that generated on the computer or
- to decide what evidential value should be given to the data. However, the judge, the public prosecutor or the defendant may request the participation of an independent expert. The decision would be made by the court. The court may reject the application if the court has sufficient knowledge of the subject (section 244 subsection 4 StPO). In computer-related cases, judges often request an expert witness to analyse the evidence.

There are no specific legal obligations with which the operator of the computer (which contains the fraud data) has to comply before the fraud data can become admissible as evidence. However, the judge may rule that the evidence is not admissible if there is no proof that the system was working correctly at the relevant time or if there was a possibility of the computer data having been manipulated. All criteria which can be used to measure the reliability of the evidence can be taken into account.

f) IRELAND

Much will depend on whether fraudulent cellular calls have been recorded by the service provider on computer (in terms of distance and length of time) for billing purposes. A printout of these computer records or that information stored "on microfilm, microfiche, magnetic tape or disk" would constitute a "document" for the purposes of the Criminal Evidence Act of 1992 (section 2).

The admissibility of this type of evidence is governed by Part II of the Criminal Evidence Act of 1992. This Act states at section 5 (1) that:

> "information contained in a document shall be admissible in any criminal proceedings as evidence of any fact therein of which direct oral evidence would be admissible if the information:
>
> a) was compiled in the ordinary course of business,
>
> b) was supplied by a person... . who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with, and
>
> c) in the case of information in non-legible form that has been reproduced in permanent legible form [i.e. in this case, computer record printouts], was reproduced in the course of the normal operation of the reproduction system concerned".

Section 1, does not, however, apply to information that is privileged from disclosure in criminal proceedings or information supplied by a person who could not be compelled to give evidence at the instance of the party wishing to give the information in evidence. Nor does it apply to documents containing information compiled for the purposes or in contemplation of any criminal investigation(s) or inquiries carried out under any enactment, or to documents containing information compiled for the purposes or in contemplation of civil or criminal proceedings or proceedings of a disciplinary nature. (s.5(3)). This type of evidence is however admissible where the document concerned is a deposition made on oath in the District Court by a person who is alleged to have committed an offence and who is ordinarily resident abroad, or where Section14 of the Criminal Procedure Act 1967 (which deals with taking of depositions) could not be involved or where the accused has died or fled the jurisdiction.

Independent Expert: There is no requirement under Irish Law for an independent expert to confirm that the evidence being adduced is the same as that produced on the computer. Section. 8(2) of the Criminal Evidence Act 1992, merely requires the Courts to consider whether or not it is a "reasonable inference" that the information which is to be admitted is "reliable".

Where a party to the proceedings wishes to submit a 'document' within the meaning of section 5, a copy of the document must be served on the accused pursuant to s.6(1) of the Criminal Procedure Act, 1967 or notice of intention to give the information in evidence, together with a copy of the document, must be served on each of the other parties, at least 21 days before trial.

g) THE NETHERLANDS

Not all court evidence must be presented in written form. The Supreme Court tends to consider all objects used to commit a criminal act as pieces of evidence ('corpus delicti'). This means that those exhibits can form part of the evidence through the own observation of the judge, when they have been exhibited and discussed during the investigation in court (see article 297 paragraph 5 Sv. below).[38]

Legislation governing the adducibility of fraud data as evidence in courts:

Article 339 Sv (Penal Code) is relevant in this regard. Paragraph 1 of this article states that only the following may be considered as proof in court proceedings:

1. The judge's personal observations

2. Statements of the suspect

3. Statements of a witness

4. Statements of an expert

5. Written documents

Article 297, paragraph 5, provides that documents will not be used unless read aloud during the trial or when the defendant is informed of its content.

An investigating judge is entitled to order that an object in the possession of a third person be handed over to him provided it may legally be seized (see art. 98 Sv). In the field of computerised information, the investigating judge has the power to order the handing over of (a copy) of computer data on the basis of art. 125i Sv. The subject of this power are data in a computer system which could serve as evidence in a computer system. The data must relate to the defendant and may be more precisely described as:

- input in the system by the suspect;
- addressed to the suspect;

---

[38] J.F. Nijboer, Inleiding tot het strafrechtelijk bewijs, Ars Aequi Libri, Nijmegen 1992, p. 129

- under the suspect's control;
- served to commit the investigated crime or being the object of the investigated crime.

In addition, a system operator can be ordered to hand over the whole or part of the system log-file. The background of the specified restrictions is that the order relates only to existing stored data. Orders that involve processing or matching of computer data cannot lawfully be given.[39] The person to whom the order applies is not free to deliver the data in the form he prefers - it is up to the judge to decide - in order to prevent data from being handed over in encoded or encrypted form and/or in a medium that cannot be processed by the judge. The suspect is exempted from this judicial order (art. 125m (1) Sv) as well as other persons who have a legal excuse not to testify (art. 125m (2) Sv). If a search of the premises results in the recording of data from a computer system there, the administrator of the computer system must be informed about the data recorded by means of an official (written) statement.

In practice, computerised data can easily be manipulated without leaving a trail. Special procedures for the collection and storage of it are developed by the CRI and, internationally, by Interpol. Moreover, official written statements will show how access to the data was made, at what time and under which circumstances, in what format the data was seized, etc. The present rules on criminal evidence facilitate computer-generated evidence. It can be presented to court in the most suitable format. An official statement concerning its seizure and analysis will be contained in the file. If necessary, law enforcement personnel can be called to the witness stand.

A print-out of a computer record or file can be considered as writing and can be presented in court. Art. 297 Sv provides that data on a floppy or a CD-rom must be visualised in court (the judge will inspect it) or it can be printed out and read in open court. The official statements about the collection, conservation and visualisation of this kind of data become extremely important as regards the reliability of this type of evidence. As a consequence, data filed on a floppy disk or CD-rom must be printed out first.

The court does not require that an independent expert confirm that the evidence being presented to court is the same as that generated on the computer or to decide what evidentiary value should be given to the data. The judge decides independently what evidence he considers reliable to use. As long as nobody contests this there is no obligation for him to explain his decision.[40]

h) SWEDEN

Sweden applies the principles of verbality, immediacy and concentration. The principle of verbality means that the parties 'claims, answers and pleadings must be presented verbally. [41] The principle of immediacy means that the court must base its decision exclusively on what has been presented to it during the trial.[42] The judge shall base his determination only on what he has observed during the trial. The principle of concentration is necessary so that the principle of immediacy may be applied. The evidence must be presented to the court in one continuous series of meetings.[43] This means that the fraud data should be presented in the form in which it can be best viewed and evaluated by the court.

---

[39] TK 1989-1990, 21551, no. 3, p. 26.

[40] A. Minkenhof, De Nederlandse Strafvordering, Gouda Quint B.V., Arnhem, 1990, p. 236

[41] The Code of Judicial Procedure 1942:740 (rättegangsbalken) chapter 43 sec 5 and chapter 46 sec 5.

[42] The Code of Judicial Procedure chapter 17 sec 2 and chapter 30 section 2.

[43] If for some reason this is not possible, there are strict rules concerning adjournments (the Code of Judicial Procedure chapter 43 section 11 to 13 and chapter 46 section 11 to 13).

Sweden has a system of free submission of evidence and the courts apply the principle of free evaluation of evidence.[44] Every kind of evidence is allowed. The weaknesses and shortcomings in the evidence presented shall be taken into account when the evidence is evaluated. The proceedings before the courts are adversarial in nature. Use of the adversarial procedure means that the parties are responsible for the presentation of the evidence in court. In criminal cases however, the court carries responsibility for the investigation and may request the parties to submit additional information.[45] The court may, even on its own initiative, arrange for the presentation of certain evidence although this seldom happens.[46]

Swedish courts do not require the intervention of an independent expert to confirm that the evidence being presented to Court is the same as that generated on the computer or to decide what evidential value should be given to the data.

C. CONCLUSION

Electronic data is adducible as evidence in all the EU Member States covered by this chapter. Legislation enacted in 1984 (UK) and 1992 (Ireland) ensure the admissibility of such evidence in the common law jurisdictions covered by this chapter while the principle of free proof is used in the civil law jurisdictions to guarantee the admissibility of data as evidence. In addition, civil law courts sometimes have a broad discretion regarding what they will accept as evidence.

---

[44] The Code of Judicial Procedure, chapter 35 section 1.

[45] The Code of Judicial Procedure, chapter 45, section 11.

[46] The Code of Judicial Procedure, chapter 35, section 6

V. LEGAL QUALIFICATION OF MOBILE COMMUNICATIONS FRAUD

The last chapter of this report will focus on the issue of how one legally qualifies various types of mobile telecommunications fraud. Does the law of the E.U. Member States contain a legal qualification of "telecommunications fraud" as a specific incrimination. Is there a specific criminal treatment of telecommunications fraud. Or do we have to fall back on traditional criminal categories such as theft, deceit, forgery, etc.

The task of qualifying different types of cellular fraud does not fit neatly into one particular field of law. In addition to qualifying the different types of cellular fraud, this chapter also contains the relevant legislation used to prosecute cellular fraud and the possible legal remedies available to counteract mobile fraud in the relevant member states.

To tackle the question of the legal qualification of mobile telecommunications fraud, we used the twelve fraud types defined in the technical ASPeCT reports. These twelve types are:

1. direct call selling
2. pabx fraud
3. freefone fraud
4. premium rate line fraud
5. mobile to mobile fraud
6. provision of data that may be used to impersonate another subscriber's identity
7. agreeing to a subscription for a suspect subscriber
8. fictitious subscriber details
9. dealer/subscriber making a gain
10. subscription fraud
11. roaming fraud
12. handset fraud

For each type of fraud we examined the law of selected E.U. Member States.

A. FRAUD TYPE 1 - DIRECT CALL SELLING

This involves X fraudulently selling GSM airtime to people at discounted rates relative to those of the Service Providers. X obtains a subscription from a Service Provider, sells the airtime but has no intention of paying the bill. X will collect a flat rate for each call made.

In **Ireland,** the fraudulent sale of airtime (often at rates far lower than those offered by the national telecommunications operator) constitutes a breach of the 'exclusive privilege' granted to Telecom Eireann (the national telecommunications operator) under the 1983 Postal and Telecommunications Services Act (PTSA). Telecom services may be provided only on foot of a licence granted by either Telecom Eireann or the Minister holding the telecommunications portfolio (currently, the Minister for Public Enterprise). Where the cellular fraudster has no intention of paying his bill, he may be prosecuted under the PTSA[47] for wilfully causing the company (Telecom Eireann) or its licensee to suffer loss in respect of any rental, fee or charge properly payable or for attempting to avoid payment of any such rental fee or charge.

[47] Section 87 (4)

In **England & Wales**, offering a telecommunications service without a valid licence is an offence under the 1984 Telecommunications Act.[48] The Secretary of State for Trade and Industry is responsible for issuing licences. In addition, a person who dishonestly obtains a telecommunications service with intent to avoid payment shall be guilty of an offence under Section 42 of the Telecommunications Act 1984 and may be subject to a period of either six months (summary conviction) or five years[49] (conviction on indictment) imprisonment.

Selling airtime at discounted rates in **the Netherlands** without the intention of paying the service provider's invoice is legally qualified as deceit under Article 326 of the Penal Code. However, the onus is on the public prosecutor to prove that the alleged fraudster never had the intention of paying the invoice. This type of cellular fraud is also covered by the crime of deception in Sweden.[50] The minimum penalty in Sweden is a fine (calculated taking the defendant's daily income into consideration) and the maximum penalty is six years' imprisonment.

In **Austria**, direct call selling is legally qualified as fraud and deceit. It may be caught by Section 146 of the Strafgesetzbuch (StGB) "Betrug (fraud, deceit), Schwerer Betrug, Gewerbsmässiger Betrug". The sanctions that may be imposed will depend on the level of financial loss suffered. If the financial loss is between 0 and 25,000 DM, a term of imprisonment of up to six months may be imposed. A daily financial penalty may also be imposed. There are up to three hundred and sixty daily rates provided for under Section 146 of the StGB. If the fraud is carried out on a commercial basis ("gewerbsmässig), a prison sentence ranging from six months to five years may be imposed under Section 147 StGB.

Under **Finnish** law, direct call selling is simply qualified as fraud. Sanctions may be applied under Chapter 36 of the Penal Code (Fraud and dishonesty). Section 1 of this chapter provides that a person who, "in order to obtain unlawful financial benefit for himself or another... .deceives another... .and in this way causes financial loss to the deceived person... .shall be sentenced for fraud to a fine or to imprisonment for a maximum of two years".

This type of cellular fraud is deemed "common" fraud under **Italy**'s Penal Code.[51] The penalty can range from a minimum of six months imprisonment to a maximum of three years while the minimum fine is 100 thousand lire and the maximum 2 million lire.

B. FRAUD TYPE 2 –PABX FRAUD

This type of fraud involves breaking the password of a corporate switchboard system. It involves a trial and error attack (usually outside office hours) on the system until the password is broken. The dial-on-service is then used by the fraudster, usually for international call selling purposes. This type of fraud is usually carried out by fraudsters carrying fraudulent mobiles not possessing international access as a means of making international calls.

In **the Netherlands**, this form of fraud is considered as hacking and is actionable under Article 138a of the Penal Code. The definition of "hacking" is deliberately broad so as to catch this type of fraud. The use of a dial-on-service is caught by Article 138a, a provision that is primarily meant for computer systems but which is applicable to this fraud type. The maximum penalty for an offence under Article 138a is four years' imprisonment or a fine of up to Fl. 25,000. The prosecution has to prove that the hackers purposely and by illegitimate means gained access to the PABX and broke a security measure. The prosecutor must also prove that the alleged fraudster made unauthorised use of the PABX and the network.

---

[48] Section 4 (3)

[49] The maximum penalty of five years was introduced by the Telecommunications (Fraud) Act 1997.

[50] It would be prosecuted under the Penal Code, chapter 9 sections 1-3.

[51] Article 640, para. 1

In **Ireland**, PABX fraud would be viewed as stealing time on someone else's system. It may be governed by Section 99 (1) of the PTSA. Unauthorised use of a password in a PABX system may also be caught by Section 1 of the Forgery Act 1913 since the password may be deemed a "false document" under that Act as it is something which gives information.[52] The term "document" itself is not defined in the Act.

Currently, there is no specific legislation in **Belgium** relating to unauthorised access to a computer system/corporate switchboard system. However, it is possible that the fraudster who accesses the PABX may be prosecuted for stealing electrical energy under Article 461 of the Criminal Code (Theft). There is judicial precedent on this point, the latest case being Iuvis (1994). The Belgian Supreme Court (Hof van Cassatie) has held that electricity may be considered a "good" from a legal point of view and therefore is capable of being stolen.

In **England & Wales**, this form of fraud would be actionable under Section 42 of the Telecommunications Act 1984 since it involves someone dishonestly obtaining a telecommunications service with intent to avoid payment of any applicable charge. Interesting, it may also be caught by Section 1 of the Computer Misuse Act 1990 which covers unauthorised access to a computer where the person accessing the computer knows this to be the case. Section 15 of the Computer Misuse Act provides that a person resident in the UK may be extradited to another country where it is alleged that he has engaged in conduct which would, in the UK, constitute an offence under Scts. 2 or 3 of the Computer Misuse Act. This type of fraud when committed in Sweden, is viewed as unlawfully affecting the result of automatic information processing, or a similar automatic process, involving gain for the fraudster and loss for others. It would be prosecuted under Chapter 9 (sections 1-3) of the Penal Code. The minimum penalty is a fine and the maximum is six years 'imprisonment if the crime is considered as grave.

PABX fraud is prosecutable in Austria under Section 49 of the Datenschutzgesetz and Section 148a of the Strafgesetzbuch (StGB). However, the prosecution must prove unlawful appropriation of data and damage to another person's rights if invoking Section 49 and unlawful tampering with the data processing procedure (in this case, tampering with the central switching and authorisation system) if invoking Section 148a. The German legal system views PABX fraud as computer related fraud (actionable under section 263a StGB) and service fraud (actionable under section 265a StGB).

C. FRAUD TYPE 3 – FREEFONE FRAUD

The abuse in this instance is similar in nature to PABX fraud. It may feature a large number of calls to (or a long duration spent on) a mobile calling a single freefone number in an attempt to break the freefone password. A charge card may be used by the fraudster.

Under **Swedish law**, this fraud type is qualified in the same way as PABX fraud i.e. unlawfully affecting the result of automatic information processing, or a similar automatic process, which involves gain for the fraudster and loss for others. Like PABX fraud it is prosecuted under Chapter 9 (sections 1-3) of the Penal Code.

In **Ireland**, Section 99 (1) of the PTSA may be invoked where the fraudster has wilfully caused Telecom Eireann or one of its licensees to suffer loss. Once again, the Forgery Act 1913 may be applicable where a password is entered in a computer by someone who is not entitled to use it. A password, when used in the way just described, may constitute a false document being used as a genuine under the provisions of the Forgery Act.

Breaching a freefone number is actionable under Article 138a of the Dutch Penal Code. Subsequent use of the network with an intention not to pay for services received constitutes the crime of deceit of electronic services under Article 326c of the Penal Code. Where both provisions apply, the judge in **the Netherlands** is required not to award damages which are

---

[52] Per Kenny J. in McCarthy v. O 'Flynn (1979) IR 127

higher than the highest damages awardable under either of the two provisions.[53] The maximum penalty for the offence under Article 326c of the Penal Code is three years 'imprisonment or a fine of Fl. 100,000.

Italian law holds that freefone fraud is dealt with under Article 615–ter of the Criminal Code. This provision of the Criminal Code provides as follows:

> "Whomsoever fraudulently gains access to a computer or telecommunications system protected by a security system, or continues to access it against the express or tacit will of whoever has the right to deny access, shall be punished by being imprisoned for a minimum of 15 days and a maximum of three years"

In **Spain**, freefone fraud is simply regarded as computer fraud and is prosecuted under Article 248.2 of the Penal Code while in Austria and Germany the legal provisions invoked to prosecute PABX fraud are also used against freefone fraud.

D. FRAUD TYPE 4 – PREMIUM-RATE LINE FRAUD

A premium rate service is a service offered for telephone access where a premium rate charge is levied which is significantly higher than the standard call tariffs. A premium rate service may be offered in relation to information lines (e.g. weather service), advice lines or competition lines. Charges may be in the form of a price-per-minute.

This type of fraud can take two forms.

Firstly, a fraudster may establish a premium-rate-line with an unsuspecting public telecommunications carrier and make calls from one or more fraudulent mobiles to that line. The fraudster, in its capacity as operator of the premium rate line claims revenue from the carrier for these calls.

The second category is a type of direct call selling fraud. X pays the fraudster in advance for a connection to a premium rate line and then later calls the fraudulent mobile to be forwarded on to the premium rate line while paying only mobile and not premium tariffs

Section 42 of the Telecommunications Act 1984 is applicable to this type of fraud in **England & Wales** since it involves a person dishonestly obtaining a telecommunications service with intent to avoid payment of any charge applicable to the provision of that service. Under amendments introduced by the Telecommunications (Fraud) Act 1997, the penalty has been increased to a maximum of five years 'imprisonment.

In **Ireland**, Section 99 (1) of the PTSA is used to prosecute premium-rate line fraud. This section applies when the action (fraud) causes the telecommunications operator to "suffer loss in respect of any rental, fee, or charge properly payable".

Dutch law would qualify this type of fraud as the crime of deceit under Article 326 of the Penal Code if all elements can be proven, including the intention of the fraudster to use fraudulent handsets to produce higher revenues. Where the fraudster offers third parties discount rate connections to a premium-rate line and the calls are forwarded through his fraudulent handset, the offences committed are hacking[54] and deceit of electronic services[55]. The offences are considered to have been committed both by the fraudster and the third party. The financial loss of the service provider is determined by calculating the revenue the service provider would normally have received from the calls to the premium-rate line.

---

[53] Article 55 of the Penal Code

[54] Under Article 138a of the Penal Code

[55] Under Article 326c of the Penal Code

In **Germany**, premium-rate line fraud is viewed simply as ordinary fraud (actionable under Section 263 StGB) committed against the public telecommunications carriers and mobile phone company if at the time of opening the premium-rate account/mobile account, the person deceived the public telecommunications carrier about his intention not to pay.

Spain applies its ordinary fraud law to this type of fraud. It is covered by Article 248 of the Penal Code. Similarly, the second category of premium-rate line fraud is dealt with under the "common" fraud provisions of Italy's Criminal Code (Art. 640, paragraph 1), thereby excluding the possibility of computer-based crime provisions applying.

In **Sweden**, this type of fraud would be qualified as a type of deception whereby the public telecommunications carrier is induced into entering a contract which the fraudster plans to misuse in such a way as will result in gain for himself and loss for the telecommunications carrier. It is prosecuted under Chapter 9 of the Penal Code, sections 1-3.

The maximum penalty is six years 'imprisonment (if the crime is considered grave). The fine is calculated taking the offender's daily income into consideration and fines representing from thirty to one hundred and fifty days of income may be imposed.

E. FRAUD TYPE 5 – MOBILE TO MOBILE FRAUD

X uses a fraudulent mobile without international access in conjunction with another mobile with international call forwarding capabilities so as to make international calls.

Section 99 (2) of the PTSA may be invoked to prosecute this fraud type in **Ireland**. This provision makes a person guilty if he connects any apparatus or device to, or places or causes to be placed any apparatus or device in association or conjunction with, the telecommunications system operated by Telecom Eireann or one of its licensees where the effect is the provision by Telecom Eireann of a service to any person without payment of the appropriate rental, fee or charge.

In **the Netherlands**, the use of a fraudulent handset of itself dose not constitute a criminal act. However, pursuant to the Dutch telecommunications law (WTV),[56] it is an offence to keep a device which does not meet the technical requirements specified therein, connected to a public network.[57] If the fraudulent part of the handset (the manipulated SIM card) is not part of the peripheral equipment of the network, special criminal provisions will apply. They are contained in Article 29f (subsection 3) WTV and Article 50 (subsection 4 c) which provide that the maximum penalty be six months imprisonment or a fine of Fl. 10,000.

In **Sweden**, where this type of fraud involves the fraudster unlawfully using a handset belonging to another person and causing damage or inconvenience with same, it will be legally qualified as unlawful use. It is prosecuted under Chapter 10, section 7 of the Penal Code. The minimum penalty is a fine and the maximum penalty is six years 'imprisonment (if the crime is considered grave).

Under **Finnish law** mobile-to-mobile fraud is simply qualified as fraud. A fine or a prison sentence (maximum–two years) may be imposed for this type of fraud. Cases of aggravated fraud may attract prison sentences ranging from four months to four years. Cases of petty fraud attract a fine only. The sanctions are imposed under the Penal Code, chapter 36 (fraud and other dishonesty), sections 1-3.

In **Italy**, mobile to mobile fraud would be caught by Article 640-ter of the criminal code.[58] This Article relates generally to computer fraud but also contains a provision covering the falsifying in

---

[56] Wet op de Telecommunicatievoorzieningen (WTV) – it came into force on 1 January 1989. Significant changes were made since then.

[57] Articles 29e, 29f and 50 of the WTV.

[58] As provided by paragraph 10 , law no. 547, 23 December 1993.

any way of a computer network or telecommunications system so as to gain an unfair advantage. The penalties that may be imposed are imprisonment for a minimum of six months and a maximum of three years. The minimum fine is 100,000 Lire and the maximum fine is two million Lire. The penalty may be increased if the crime is committed with the intent of damaging the quality of the operator's telecommunications system. The increased penalty is imprisonment for a minimum of one year and a maximum of five years and a minimum fine of 600,000 Lire and maximum of three million Lire.

Spain qualifies this type of fraud simply as telecommunications fraud and it is prosecuted under Article 255 of the Penal Code while in England & Wales, Section 42 of the Telecommunications Act 1984 is applicable since this type of fraud involves the obtaining of a telecommunications services by dishonest means. In addition, the fraudulent handset may be prosecuted under the Forgery and Counterfeiting Act 1981.[59]

F. FRAUD TYPE 6 – PROVISION OF DATA THAT MAY BE USED TO IMPERSONATE ANOTHER SUBSCRIBER'S IDENTITY

This would involve, for instance, an employee of the Service Provider providing authentication data to a fraudster which in conjunction with cloned or simulated SIMs can be used to reproduce a legitimate subscriber's identity and result in the latter being billed for the calls made. The situation may also involve the presence of a SIM simulator in a PC being fed stolen data or data being provided intentionally from within the Network Operator

In **the Netherlands**, the cloning or simulation of a SIM card and its use is considered a forgery and dealt with under Article 225 of the Criminal Code. The maximum penalty for an offence under Article 225 of the Criminal Code is six years' imprisonment or a fine of Fl.100,000. The public prosecutor has to prove that the alleged fraudster forged a document (SIM card) with the object of using it or intending that others use it.

Under **Italian law**, Article 615–quater of the Criminal Code is the relevant legal provision for prosecuting this fraud type.[60] It relates to the withholding or dissemination of passwords to computer networks or telecommunication systems. It provides as follows:

> "whosoever, in order to gain for himself or others an unfair advantage or to cause loss to others, illegally obtains, reproduces, disseminates or delivers codes, passwords or other means suitable for access to a computer network or telecommunications system protected by security measures, or provides information or instructions suitable for said purpose, shall be punished by imprisonment (minimum – fifteen days/ maximum - one year) and fined (minimum – 10,000 Lire/maximum – 10 million Lire)."

The penalty may be more severe if circumstances provided under Article 617- quarter of the Criminal Code prevail. The latter Article relates to illegal interception, interference or interruption of a computer or telecommunications system. The more severe penalties are terms of imprisonment ranging from one year to two years and a minimum and maximum fine of 10 million and 20 million Lire respectively.

In **Ireland**, Section 99 (1) of the PTSA is relevant. It provides that a person shall be guilty of an offence if he, by "false statement or misrepresentation or otherwise" attempts to "avoid payment or any ... rental, fee or charge". There may also be implications under the Data Protection Act 198861 since it provides that personal data may not be disclosed by a data processor or by an

---

[59] Cloning of handsets may constitute an offence of forgery contrary to Section 1 of the Forgery and Counterfeiting Act 1981.

[60] It was introduced by Article 4 of law no. 547 of 23 December 1993.

[61] This Act is intended to give effect to Ireland's obligations under the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 28 January 1981. It regulates the collection, processing, keeping, use and disclosure of personal data that is processed automatically.

agent/employee of his without the prior authority of the data controller on behalf of whom the data are processed. The Act also states that it is an offence for a person who obtains access to personal data or obtains any information constituting such data, to disclose such data/information to another person without the prior authority of the data controller or data processor by whom the data are kept.

Generally speaking, employment law in **Belgium** considers that the employer is responsible for losses suffered by a third party which are caused by his employee.[62] However, in this case the employer will not be deemed responsible for his employee's actions as the provision of authentication data and/or cloned/simulated SIMs to a fraudster cannot be regarded as an act falling within the normal scope of the employee's employment. The legitimate subscriber, whose identity has been fraudulently reproduced may have a claim against his service provider (based on contract law) or possibly against the dishonest employee on the basis of an unlawful deed having been carried out. [63]

This type of fraud would fall foul of the provisions of the **UK**'s Data Protection Act 1984 as one of the eight data protection principles contained in the Act stipulates that personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes. In addition, the dishonest employee breaches the common law obligation of rendering loyal service to the employer and may have to account for any secret profits he earned while performing his work services. The employee's duty to account extends to profits arising out of criminal acts. In Reading v. AG,[64] Lord Oaksey stated that:

> "an agent is accountable for profits made in the course of his agency without the knowledge and consent of his principal and no less accountable if the profits arise out of corrupt transactions".

G. FRAUD TYPE 7 – AGREEING TO A SUBSCRIPTION FOR A SUSPECT SUBSCRIBER

In this case the Service Provider provides a subscription to a suspect subscriber without subjecting the latter to any credit check. The Service Provider may be reimbursed by the Network Operator for any loss suffered due to fraud

In **Ireland**, this type of fraud may be governed by the second part of Section 99 (1) of the PTSA if the provision of the subscription is deemed 'wilful' or 'with intent to defraud'. If not, it may just fall under general tort (negligence) law.

Under **Dutch law**, no criminal offence is committed. It is more a contractual matter between the service provider and the network operator. The service provider is free to sell subscriptions to high risk subscribers although it is not likely that the subsequent loss suffered (arising from fraud) will be reimbursed by the network operator.

In **England & Wales**, it is possible that the network operator and service provider would have entered into a contract regulating the issuing of subscriptions. If that is the case, there may be contractual provisions stipulating how the service provider should screen prospective subscribers. If so, much will depend on whether the service provider satisfied all the contractual provisions when deciding to grant a subscription. If it did not, it may be subject to a breach of contract claim by the network operator. It may also be possible for the network operator to sue the service provider in negligence if the two have a close working relationship and the network operator's profit margins are affected by the professional standards applied by the service provider in its business dealings. If the service provider fails to meet the professional standards

---

[62] Article 18 Employment Contract Law 1978.

[63] Onrechtmatige daad, Article 1382 Civil Code

[64] 1951 AC 507

normally expected of an entity occupying its position, it may be sued by the network operator in negligence.

Negligence has been defined in jurisprudence as:

> "the omission to do something which a reasonable man, guided upon those considerations which ordinarily regulate the conduct of human affairs would do or do something which a prudent and reasonable man would not do".65

In **Belgium**, if the contract between the network operator and its authorised agent stipulates that the latter should conduct a pre-subscription credit check and it fails to do this, the network operator could claim for breach of contract. It would however, have to prove the agent's failure to carry out the credit check.

Under **Italian law**, this type of fraud would result in a non-criminal prosecution whilst in Sweden agreeing to a subscription for a suspect subscriber does not give rise to an illegal action.

In **Austria**, this type of fraud can be qualified as fraud/deceit under Section 146 ff StGB Betrug. An additional element is present here as the perpetrator of the fraud is usually an employee of the service provider. The penalty is imposed under Section 12 StGB.

In **Germany**, standard fraud provisions (contained in Section 263 StGB) would apply if the service provider acts with the intention of causing financial loss to the network operator and makes a profit from its activities. Computer-related fraud may also be invoked under Section 263a StGB if there is a type of electronic sign up procedure.

H. FRAUD TYPE 8 – FICTITIOUS SUBSCRIBER DETAILS

This type of fraud features an intermediary submitting fictitious subscriber details to the Service Provider so that he can collect commission payments. Another form of fraud occurs where the dishonest dealer adds a number of 'imaginary telephones' to a genuine contract.

In **Belgium**, there is no specific legislation covering this type of fraud. However, the general principles of contract and criminal law are relevant. Article 193 of the Criminal Code which covers forgeries ("valsheid in geschrifte") may be relevant especially where a hand-written document exists. The term "written" ("geschrift") has been interpreted broadly by the Belgium courts. In addition, Article 496 of the Criminal Code may apply. It relates to the crime of deception ("oplichting") and could be important as the fraudulent dealer/intermediary obtains benefits (commissions) from his deception. The constituent elements of deception under Belgian law are: misappropriation of another person's goods, the use of false names, fraudulent acts and the handing over of a good.

Under **Irish law**, the Forgery Act 1913 may be used to prosecute this type of fraud. Section 1 of the Act makes it an offence to make a false document in order that it be used as genuine. In addition, the offence of false pretences may be relevant as obtaining money or other property by false pretence is an offence under Section 32 of the Larceny Act 1916. This provides that a person is guilty of an offence, where by any false pretence, with intent to defraud, he obtains from any other person any chattel, money or valuable security or causes or procures any money to be paid, or any chattel or valuable security to be delivered to himself or to any other person for the use or benefit or on account of himself or any other person.

The Theft Act 1968 may be relevant in **England & Wales** as section 15 (1) provides as follows:

> "a person who by deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it, shall on conviction on indictment be liable to imprisonment for a term not exceeding ten years"

---

65 Munnings v. Hydro-Electric Commission (1971) A.L.R. 609, p. 622 per Windeyer J.

Section 4 of the same Act defines the term "property" as including "money and all other property, real or personal, including things in action and other intangible property".

Deception is defined as follows in Section 15 (4) of the Act:

> "any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person".

In the **Netherlands** this type of fraud can be qualified as forgery and deceit under Articles 225 and 326 respectively of the Penal Code. It is usually caught by a combination of articles 225 and 326 of the Penal Code. The financial loss of the service provider consists of the commission paid for the "imaginary telephones".

Swedish law holds that this fraud type is legally qualified as a situation where the intermediary by deception, induces the service provider to pay him a commission for having found a customer who in reality, does not exist. The fraud can be prosecuted under chapter 9 of the Penal Code (sections 1-3). The minimum penalty is a fine and the maximum penalty is six years 'imprisonment (if the crime is considered grave).

Under **German law**, this type of fraud is viewed as standard fraud (Section 263 StGB) while computer-related fraud (Section 263a StGB) may also be relevant where there is an electronic sign-up procedure. Austrian law treats fictitious subscriber fraud as fraud/deceit under Section 146 ff StGB Betrug. The use of a forged document ensures that the action is deemed "Schwerer Betrug" under Section 147 StGB. The use of a forgery also means that the very shortest sentence that can be imposed is three years 'imprisonment.

I. FRAUD TYPE 9 - DEALER/SUBSCRIBER MAKING A GAIN

This is similar to Fraud type 8 in that the subscriber obtains a subscription through the collusion of a dealer. The dealer helps the subscriber to get around the credit control check. Both the dealer and subscriber benefit as the latter gets a subscription that he would not ordinarily get and the dealer is paid a commission for getting the subscription.

In **the Netherlands**, this fraud type is legally qualified as forgery and deceit perpetrated by both the dealer and the service provider. Articles 225 and 326 of the Penal Code are applicable. The financial losses of the service provider arising from the unpaid calls of the subscriber can be recovered from the dealer. If the subscriber makes illegal use of his subscription, the service provider cannot claim damages against the dealer, instead, he must file an action against the subscriber. The maximum penalty for an offence caught by Article 225 of the Penal Code is six years 'imprisonment or a fine of Fl. 100,000.

In **Belgium**, the dealer could probably be prosecuted as an accomplice or perpetrator (Articles 66 to 69 of the Criminal Code). In addition, the legal provisions mentioned under Fraud Type 8 could also be invoked.

Under **Irish law**, if the subscriber does not intend to pay for his calls, both parties would probably be liable under Section 99 (1) PTSA either under the broad heading of 'causing the company to suffer loss 'or under the 'false statement or misrepresentation 'section. Both parties may also be liable under the common law offence of conspiracy to defraud. The offence of false pretences may apply if airtime is interpreted to mean a 'valuable security'. Obtaining money or other property by false pretence is made an offence under Section 32 of the Larceny Act 1916. This provides that a person is guilty of an offence, where by any false pretence:

> "with intent to defraud , (he) obtains from any other person any chattel, money, or valuable security, or causes or procures any money to be paid, or any chattel or valuable security to be delivered to himself or to any other person for the use or benefit or on account of himself or any other person"

In **Sweden**, this type of fraud is legally qualified as the first type of fraud (that which involves deception) under the Penal Code, chapter 9, sections 1-3 if the dealer by deception, induces the

service provider to give the subscriber a subscription that the latter would not ordinarily have obtained and it involves loss for the service provider and gain for the dealer. The minimum penalty is a fine and the maximum penalty is six years 'imprisonment (if the crime is considered as grave). The smallest fine is 450 Krona and the maximum is 150,000 Krona. These penalties are applied under the Penal Code, chapters 25 to 38.

In **England & Wales**, the agreement between the dealer and the subscriber may amount to a conspiracy to do an unlawful act. The crime of conspiracy exists as both a statutory66 and common law offence.67 The crime of conspiracy has been defined in the past as an agreement to do an unlawful act or a lawful act by unlawful means. The onus of proof, where conspiracy is alleged, is on the prosecution. The maximum penalty under common law conspiracy is ten years ' imprisonment while a person convicted of statutory conspiracy is liable to be sentenced to a term of imprisonment not exceeding the maximum provided for the offence which he has conspired to commit.[68]

Italian law holds that this type of fraud be legally qualified simply as fraud and dealt with under Article 640, paragraph 1 of the Criminal Code (non computer-based fraud). The penalties for this type of fraud ranges from a minimum period of imprisonment of six months to a maximum period of imprisonment of three years. The minimum fine is 100,000 Lire and the maximum is two million Lire.

J. FRAUD TYPE 10 – SUBSCRIPTION FRAUD

Fraudulent users use false identities, stolen ID and other similar personal documents to obtain a mobile subscription. Such fraudulent mobiles may be used personally by the fraudsters or sold on to others for personal use.

In **England & Wales**, the use of false IDs is probably caught by the Forgery and Counterfeiting Act 1981. Section 1 of the Act states that :

> "a person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice".

The term "instrument" is defined in Section 8 of the Act as meaning:

> "Any document, whether of a formal or informal character".

Section 6 of the Act allows for the offence to be tried either on summary conviction or by way of trial on indictment. Stolen ID s are covered by the Theft Act 1968. Section 1 (1) of this Act defines the offence of theft as follows:

> "A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it... "

Under **Irish law**, if the fraudulent users obtained the subscription using false information for the purposes of avoiding some charge, the fraud will be covered by the "false statement or misrepresentation" heading of Section 99 (1) of the PTSA. Subscription fraud may also be governed by Section 1 of the Forgery Act 1913 which makes it an offence to make a false document in order that it may be used as a genuine.

Dutch law qualifies this type of fraud as forgery under Article 225 of the Penal Code. Under Article 225 (1) of the Penal Code, the intention/objective to use a forged document as real

---

66 Section 1 (1) and Section 1 (2) of the Criminal Law Act 1977 (as amended by Section 5 of the Criminal Attempts Act 1981)

67Section 12 of the Criminal Justice Act 1987

68 Section 3(3) of the Criminal Law Act 1977

suffices to ground a conviction. This is sometimes called the pre-stage provision. Where a forged document is actually used, Article 225 (2) of the Penal Code applies. For Articles 326 or 326c of the Penal Code to apply, the perpetrator should already have obtained an illegal profit from the scheme. Subscription fraud is usually caught by a combination of Articles 225 and 326 of the Penal Code. The maximum penalty under Article 225 is higher, i.e. six years 'imprisonment or Fl. 100, 000 and it is usually easier to prove.

Under **Swedish law**, subscription fraud is legally qualified as the first type of fraud (involving deception) under the Swedish Penal Code if the fraudster uses the false document to induce the service provider to sign a contract with him and this involves gain for the fraudster and a loss for the service provider. The fraud can be prosecuted under the Penal Code, Chapter 9, sections 1-3.

In **Austria**, this type of fraud is qualified as fraud/deceit under Section 146 St GB Betrug. The use of a forged document means that the crime will be deemed at least "Schwerer Betrug" under Section 147 StGB. The minimum prison sentence that may be imposed is three years.

Under **Italian law**, subscription fraud is qualified as larceny where the piece of ID is a tangible document.

K. FRAUD TYPE 11 – ROAMING FRAUD

Here the fraudster uses his subscription (SIM CARD) from a foreign network to commit the fraud. He takes advantage of the fact that time elapses before the home network operator receives the roaming call records from the foreign network operator. This type of fraud can also be carried out by subscribers to the home network who make a large number of calls from abroad at the weekend.

1. GENERAL INTRODUCTION

Roaming fraud has the capacity to throw up difficult and complex legal questions relating to criminal jurisdiction. Roaming fraud, by its very nature, involves a transborder element. This fact, in turn, raises the question of which country's courts have criminal jurisdiction. Criminal law is territorial in nature.

This means that a court will assume criminal jurisdiction when the criminal act occurs on its national territory. A problem may arise as roaming fraud may involve the commission of criminal acts in a number of EU Member States.

The possibility of different national courts claiming jurisdiction arises. This may spell bad news for the home network operator as it reduces the possibility of a court in its territory gaining jurisdiction in the case. This, in turn, lessens the degree of judicial predictability for the home network operator.

Roaming fraud presents a problem for the home territory operator where no fraud is perpetrated against the network operators in the roamed countries. As a consequence, they will have no vested interest in commencing proceedings against the fraudster. If the financial loss has been significant, the network operator will wish, ideally, to see the fraudster imprisoned and "out of harm's way", thereby reducing the possibility of further fraud being committed. However, a "jurisdictional lacuna" exists which the fraudster may exploit.

What options are available to the home network operator?:

- hand over the evidence to the police who take criminal proceedings with a view to co-operating with the police of the country in which the fraudster is currently based.
- seek extradition of the fraudster. However, much will depend on whether the two relevant countries have entered into a bilateral extradition treaty or are both signatories of the Council of Europe's Convention on Extradition. Even if an extradition framework is in place, it must then be determined if the offence is an extraditable offence (much may depend on the gravity (financial losses) of the alleged crime).

The issue of roaming fraud also raises the issue of localisation. In essence, this issue relates to determining where the crime took place. Lawyers must attempt to localise the crime. The entity which is ultimately defrauded is the home network operator. However, important elements of the fraud (the actual calls made) take place outside the home network operator's territory! The issue of localisation may be answered by referring to the calling records – these will, at least, permit us to determine in which countries calls were made. The issue of jurisdiction is strongly interlinked with that of localisation. In fact, jurisdiction is predicated on localisation.

2. LEGAL QUALIFICATION OF ROAMING FRAUD

In **Ireland**, this type of mobile fraud is probably governed by the first part of Section 99 (1) PTSA which makes it an offence for a person to:

> "wilfully cause the company to suffer loss in respect of any rental, fee or charge properly payable for use of the telecommunications system".

Under **Dutch law**, if the subscriber entered into the contract with the intention not to pay the bill, the crime of deceit under Article 326 of the Penal Code will be committed. A loss, if incurred, will consist of calls made that are not paid for. The evidence can take the form of call records produced by the service provider or other telephone companies with whom roaming agreements exist.

German law considers roaming fraud to be standard fraud as described in Section 263 StGB if there is intention to defraud at the time when the subscription is first taken out while Austrian law qualifies it as fraud/deceit under Section 146 ff StGB.

Under **Italian law**, roaming fraud would be caught by Article 615 –ter of the Criminal Code (Illegal access to computer or telecommunications systems). This provision was introduced by Article 4 of the law of 23 December 1993 n 547. It provides as follows:

> "Whomsoever fraudulently gains access to a computer or telecommunications system protected by a security system, or maintains access against the express or tacit will of whomsoever has the right to deny said access, shall be punishable by imprisonment for a minimum of 15 days and a maximum of three years.

L. FRAUD TYPE 12- HANDSET FRAUD

Here the fraudulent user has a number of phones and uses them with legitimate or stolen SIMs. A threat may also occur where stolen or lost SIM cards are not automatically withdrawn from the network.

Under **Irish law**, the theft of handsets and/or SIM cards is governed by Section 1 of the Larceny Act 1916 (simple larceny) since they are, unlike airtime, tangible objects and therefore 'capable of being stolen' for the purpose of that Act. A person steals, who without the consent of the owner, fraudulently and without a claim of right made in good faith, takes and carries away anything capable of being stolen with intent, at the time of such taking, permanently to deprive the owner thereof. It is also possible that the Wireless Telegraphy Acts 1926-1988 might apply. Under these Acts, it is prohibited to keep or have in one's possession anywhere in the State any apparatus for wireless telegraphy without a licence.

In **the Netherlands**, the use of a fraudulent SIM card is actionable under Article 225 of the Penal Code which covers the crime of forgery. The user may also have impersonated someone else so as to obtain the services of the telecommunications provider – in that case, article 326 of the Penal Code applies. The public prosecutor has to prove that the fraudster forged a document (SIM card) or deliberately used a forged document (SIM card).

In **England & Wales**, handset fraud is probably actionable under Section 1 (1) of the Theft Act 1968 as it involves stolen SIMs. The offence was originally punished by ten years' imprisonment but the maximum was reduced to seven years by Section 26 of the Criminal Justice Act 1991.

Under **Swedish law**, it is possible that this type of fraud be legally qualified as the second type of fraud under the Swedish Penal Code (no deception required) if the fraudster affects the result of automatic information processing, or a similar automatic process, which involves gain for himself and loss for any other person. Illegal use may also arise if the fraudster unlawfully uses SIM cards belonging to another person and thereby causes damage or inconvenience. This fraud type may be prosecuted under the Penal Code, chapter 9, sections 1-3 or chapter 10, section 7. If the fraudster is found guilty of both fraud and unlawful use, he will only be sentenced for fraud.

It is interesting to note, that under **Austrian law**, the term 'stealing' only applies to objects which have an independent value – it does not apply to items such as saving books, eurocheques, credit cards etc.This poses a problem as under Austrian law, a SIM card cannot be deemed to be stolen. It has been argued by some academics that use of a stolen SIM card may be deemed Computerbetrug under Section 148 a or Section 49 DSG (where it is not an anonymous SIM). However, this view is not accepted by everyone.

In, handset fraud is caught by the larceny provisions as the (stolen) SIM is a tangible object. Where the fraud involves stolen SIMs, the fraudster may, if found guilty, be imprisoned for a minimum period of fifteen days and a maximum period of three years. The minimum fine is 600,000 Lire and the maximum is one million Lire.

Jos Dumortier

Mark Hyland

Diana Alonso Blas

15 December 1998