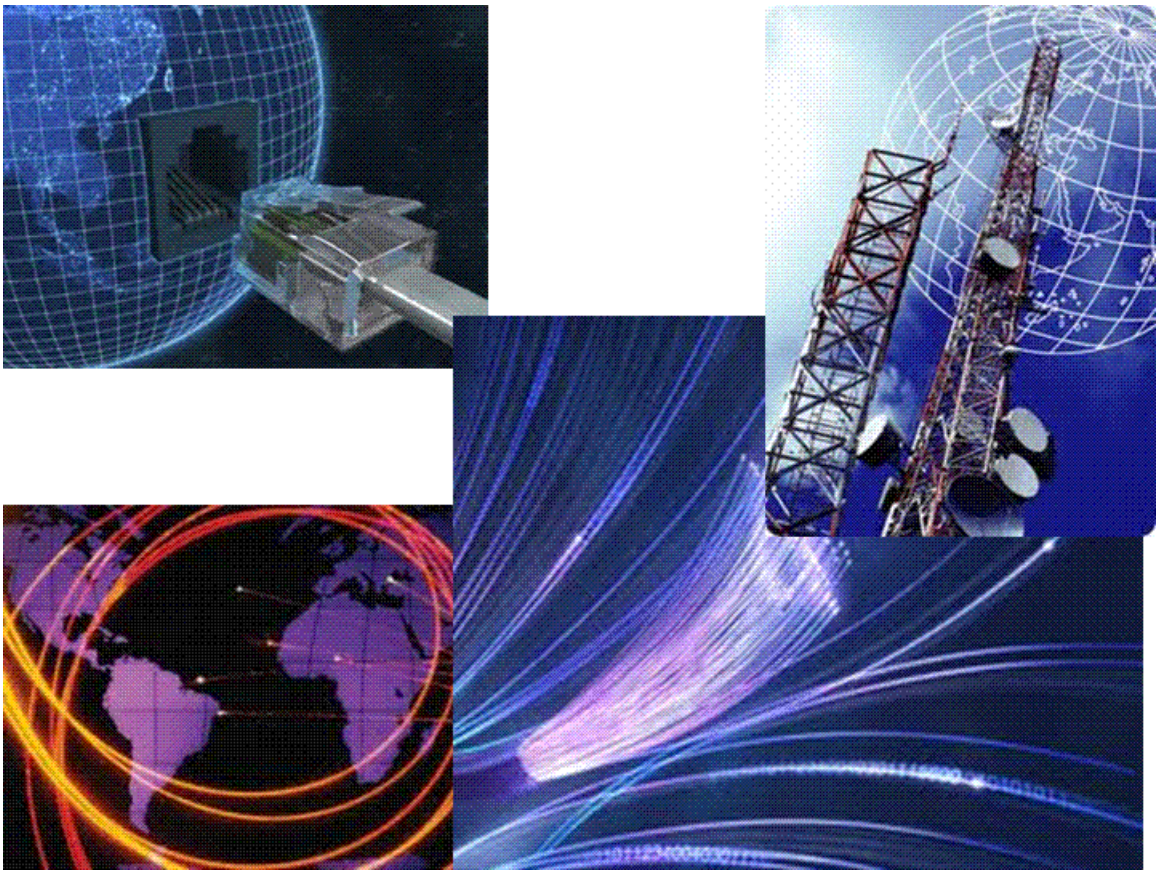
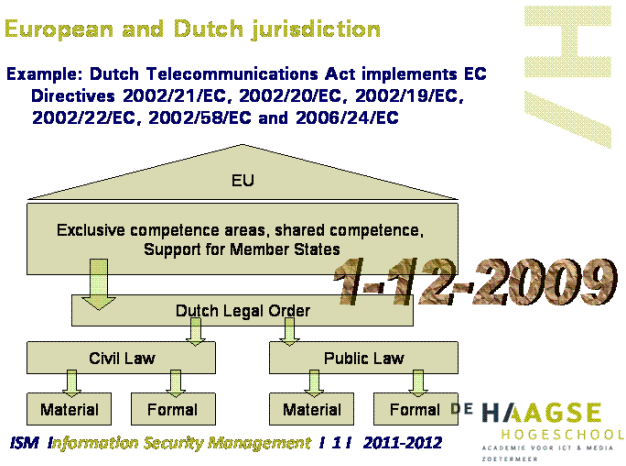
Lectures "Telecommunications Law"



This reader contains the scripts of the video colleges "Telecommunications Law". The subject will be studied in week two of period one of any given school year (September – October). You will find the scripts on the following pages.

Lecture six

This lecture covers the subject of Telecommunications Law. First, a short introduction on the European Union (EU) and the way it influences law in all it's Member States including The Netherlands. Below you see a picture of the "building" that constitutes the EU in a legal view. Prior to December 1, 2009, the EU consisted of three "pillars": the first pillar regulating economic aspects of the single market, the second pillar regulating external relations, the third pillar regulating internal security. In December 2009, the EU became a single legal entity.



As you can see, the EU has great influence on the Dutch regulatory system, especially in areas where the EU has exclusive competence, such as regulating the internal market. The EU has the right to issue mandatory directives (complete harmonisation) or *de minimis* directives (minimum harmonization). It depends on the subject whether the EU requires complete harmonisation or partial harmonisation, more on that follows in the video colleges.

The EU directives are targeted at the EU Member States (see for example article 30 of the Framework Directive that we will discuss), not natural or legal persons. Each Member State shall implement the directive in its own laws. Nonetheless, most directives are completely implemented, and a judge having to deal with a national law shall interpret that law according to the directive.

It is important that you thoroughly understand the EU system! Make sure you understand it before you study the other college materials.

Another important aspect to understand is that there are different judicial systems. One division that can be made is between civil law systems, in which the rules are explicitly coded into law and common law systems, in which the rules are determined through verdicts by the courts. Another differentiation that can be made is between the court system of judge versus jury. In the jury system, the jury comes to a verdict of "guilty" or not, not the judge. The judge then decides on the punishment following a "guilty" verdict. Research shows that well informed juries come to roughly the same judgements as judges do.

In this lecture, I will explain the regulation of the telecommunications market. In the next lecture I will elaborate on regulation to prevent crime and terrorism and the relation to

privacy. Telecommunications providers have to comply with these directives –translated into national laws– as well. Why is the EU regulating the telecommunications market? This is because it is viewed as an important part of the single market space, and differing regulations throughout the EU would hamper the free flow of goods, people, and services.

The European Commission (EC) has emphasized that one open internal market with fair competition is a very important drive for economic growth in the EU. This is for example reflected in the press release shown below, which is about EU wide consumer protection. Please read the press release of 13 November 2007 to understand the reasons why the EC has decided to introduce the "Telecoms Reform Package". Telecommunications law is by its nature very economic, which you will see throughout the texts that we will study. An example is the new regulation that was adopted in June 2011, protecting online customers by giving them a longer period to change their minds regarding an online purchase.

Let me elaborate on the Telecommunications Framework that regulates the telecommunications sector in Europe. The EU regulates a lot of aspects that concern telecommunications operators. This ranges from *ex ante* regulation by Member States, with *a priori* requirements before a party can enter the market, to the requirements on privacy to be exercised by telecommunications firms. Directives aimed at fighting

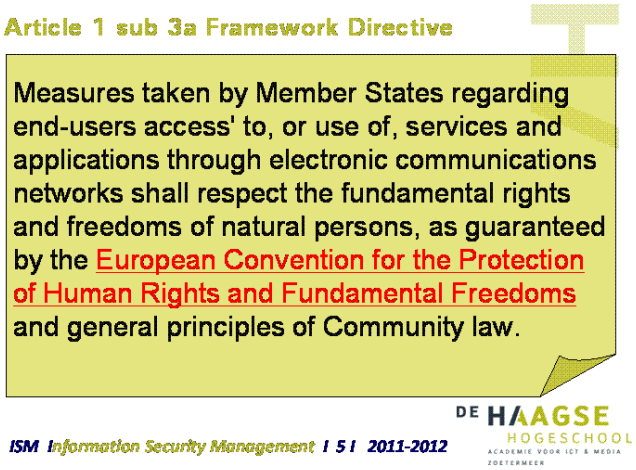
organised crime and terrorism also form an important factor in telecommunications law. The directives that regulate the telecommunications market are:

Framework Directive

I will now explain the framework of directives.[1] The framework is a consistent set of five directives that regulate different aspects of the telecommunications market. The main directive is the "Framework Directive" (directive 2002/21/EC). This directive was adopted 7 March 2002 and it was amended on 19 December 2009. It lays out the single framework that regulates the converging sectors telecommunications, media and information technology. It defines four specific directives (in article 2(l)) that regulate authorisation to operate, access and interoperability of communication networks, universal services and the right to privacy. The Framework Directive does explicitly allow Member States to take measures necessary to safeguard their critical public interests (in recital 7 of the preamble). Recital 10 of the preamble explains and article 1(1) of the directive defines what is and what is not within the scope of the directive.

The Framework Directive establishes an independent National Regulatory Authority (NRA) in each Member State (recital 11 of the preamble and article 3 of the directive). It also establishes *ex ante* regulation in certain circumstances (recital 25 of the preamble and article 8(2)(f) of the directive). The directive establishes that any measure by a Member State shall be compliant with human rights:

[1] All directives can be found in Dutch as well.



Measures shall be appropriate, proportionate and necessary. So the directive explicitly mentions these important legal principles.

The Framework Directive also defines the Specific Directives (in article 1(2)). In article 2, the terminology used in the directive and the Specific Directives is defined. The NRA is regulated in chapter 2 of the directive, and its tasks are defined in chapter 3. For the Netherlands telecommunications sector, the NRA is called OPTA ("Onafhankelijke Post en Telecommunicatie Autoriteit"). A small part of the services, the management of frequencies, is dealt with within the Ministry of Economic Affairs ("Agentschap Telecom").

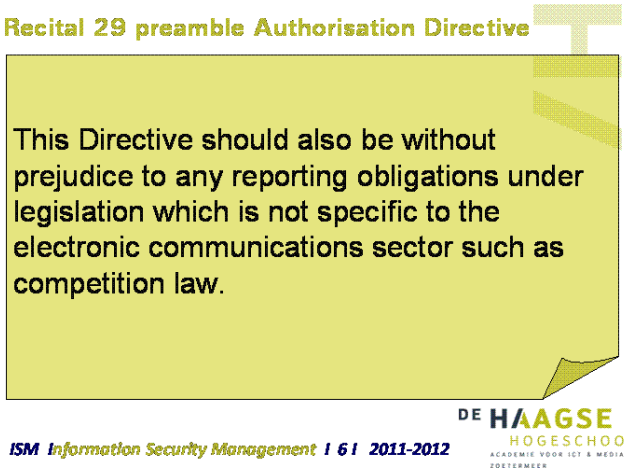
Chapter 3a regulates the security and integrity of networks and services. This chapter has been introduced in December 2009. The chapter on security requires Member States to assure that telecommunications undertakings take appropriate technical and organisational measures, with regard to the state of the art, ensure a level of security appropriate to the risk presented (article 13a(1)). In practise it means that telecommunications undertakings will have report annually to the NRA, which then assesses whether the undertaking has taken accurate measures to guarantee security and integrity of its network(s).

Apart from the above mentioned subjects, the directive regulates undertakings with significant market power, interoperability of digital interactive television services and dispute resolution.

Authorisation Directive

The "Authorisation Directive" regulates the authorisation scheme to allow the provision of electronic communications networks and services (recital 7 of the preamble). This directive is applicable to both public and private electronic communications networks (recital 4 and article 1(2))! Basically, it means that any undertaking wanting to provide a network is only subject to notification, unless special circumstances apply (article 3(3)). In other words: any party is free to provide telecommunications services, and regulation by Member States is only allowed when there is a pressing need. For example: radio frequencies can be regulated because these are available in limited quantities. Recitals 5 and 20 of the preamble and article 1(b) give the scope of this directive. Sector specific regulations shall be treated as overruling general law, as can been seen from the following statement: "*This Directive should also be without prejudice to any reporting*

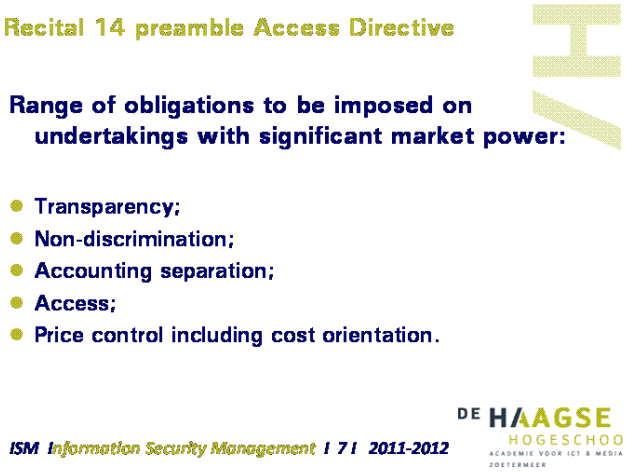
obligations under legislation which is not specific to the electronic communications sector such as competition law" (recital 29 of the preamble).



Access Directive

The "Access Directive" is primarily aimed at public networks (recital 1 of the preamble and article 1 of the directive). Content is not within the scope of this directive (recital 2 of the preamble). The aim of this directive is to provide an open and competitive market for undertakings to negotiate interconnection (recitals 5 and 6 of the preamble). Access in the scope of the directive is access of one undertaking to the network of another undertaking. The directive does not mean to regulate access to end-users (article 1(2) and article 2(a) of the directive).

The directive also regulates regulation (by Member States)! Recital 14 shows the maximum set of obligations that an NRA can impose on an undertaking:



The principles are explained in recital 17. Articles 9 to 13 of the directive define the obligations an NRA can impose. It is not permitted that an NRA imposes obligations not

mentioned in these articles. The obligations can be quite substantial, but shall[2] always be appropriate and proportionate (recital 15).

Universal Service Directive

The "Universal Service Directive" regulates a minimum set of services to all end-users at an affordable price (recital 4 and articles 1, 3). These services constitute an important part of daily life, without them life in today's information society would be very hard. An important universal service is a fixed telephony connection at an affordable price (recitals 8, 9 and article 4) and the corresponding "address" directory (recitals 11, 35 and article 5).

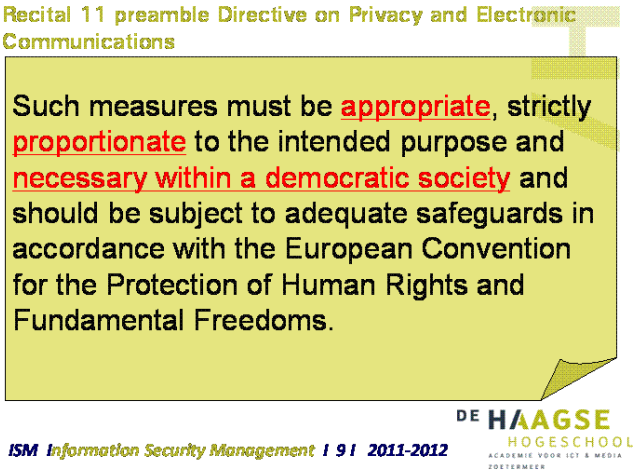
Non-discrimination (examples in recital 21, article 23a, and article 25) is an important part of all measures as well. The directive has a very distinct social inclusion philosophy: what constitutes a universal service must be periodically reviewed in order to avoid social exclusion (recitals 25, 26, articles 31, 36(3)). The directive does not implement complete harmonisation, but rather minimum harmonisation (recital 46 and article 26(4)).

Directive on privacy and electronic communications

The "Directive on privacy and electronic communications" defines the obligations of telecommunications providers with regard to the privacy of their customers. This is different regulation than the general privacy regulation in the Member States: it is sector specific regulation (recital 4 of the preamble). It overrules the general privacy regulation as laid down in Directive 95/46/EC for the telecommunications sector. Confidentiality of communications is guaranteed (recital 3 and article 5).

Member States are allowed to take measures that invade privacy in specific circumstances (recital 11 and article 15(1)), but these measures must balance all rights involved. **The test of non-discriminate, transparent, appropriate and proportional measures is a very important one that you find in many other directives and national laws. Any measure taken that is contrary to the basic philosophy of a law must be effective (appropriate) and no less intrusive measures are possible (proportionate).**

[2] Notice that this is a stricter requirement than used elsewhere. Where the word "should" is used, it means that the addressee has the freedom not to implement the proposed measure, as can be seen in for example recitals 23 and 24.



This directive also states that providers should take appropriate measures to safeguard the security of their services (recitals 20, 21 and article 4). Further, the directive restricts use of personal data to legitimate use (recitals 25, 26, 29 and article 6). Unsolicited marketing is not considered a legitimate goal, and explicitly prohibited (recitals 40, 41 and article 13).

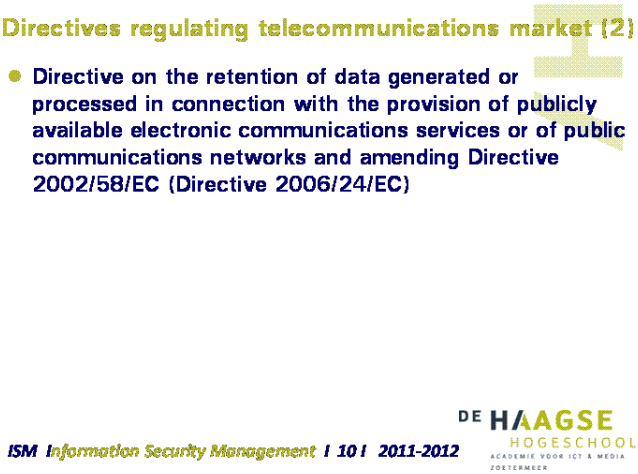
Summary

These five directives regulate the telecommunications operators establishing public networks. They have been implemented in the laws of the Member States. In the Netherlands, this has been done in the Telecommunications Law ("Tele-communicatiewet"). With regard to data retention and privacy, other directives were adopted, and that is what I will talk about in the next lecture.

Lecture seven

This lecture is about the requirements regarding protection of privacy related aspects. In general, all legal entities that automatically process personal data have to comply with the rules as detailed in Directive 95/46/EC. In The Netherlands, this directive is implemented in the Privacy Act ("Wet Bescherming Persoonsgegevens"). However, companies that provide services that are considered public telecommunications networks have to deal with a slightly different set of rules. The rules for processing personal data for public telecommunications networks are detailed in the Privacy in Electronic Communications Directive (Directive 2002/58 EC) and in the Data Retention Directive (Directive 2006/24/EC). These specific rules have been implemented in chapter 13 of the Dutch Telecommunications Act ("Telecommunicatiewet").

Telecommunications providers must provide an architecture that can be (wire) tapped in the course of a criminal investigation. In fact, The Netherlands is country where most wiretaps are placed per capita annually. In 2009 24.724 telephone numbers were tapped, an average of **2121** taps **per day**. This almost equals the total number of **2376** taps that were permitted by US courts **in the whole year**.[3]



The rules also state that telecommunications and service providers must be capable of the retention of certain data on behalf of (criminal) investigations in article 1(1) of the Data Retention Directive. Article 1(2) specifies with data must be retained: traffic and location data of both legal entities and natural persons. The contents of the communication may not be retained! Although the data is retained, access to it is restricted to the competent national authorities. This means that the usual guarantees apply. An investigating Prosecutor may issue a request for the data; this request must be reviewed by an independent judge. This judge will check the necessity and proportionality of the request. Retaining the content is subject to the provisions in the Criminal Law of each Member State.

Communications data must be retained between six months and two years. Each EU Member State may choose the length of the retention period, as long as it is between six months and two years. In The Netherlands, the government opted for a two year retention period in 2010. Naturally, the telecommunications companies were not very happy about it, as they have to provide and pay for the technical means to enable the

[3] Source: http://nos.nl/artikel/159713-fact-check-nederland-kampioen-telefoontaps.html (in Dutch)

retention. The telecommunications companies sided with human rights activists in a lobby for a shorter retention period. The lobby was successful in 2011, when the Telecommunication Act was changed in order to provide for a six month retention period for data from telecommunications networks.

A third obligation that telecommunications providers have to adhere to is providing the contents of tapped communication upon a court order to do so. The requirements for permission to tap are regulated under the Code of Criminal Procedure ("Wetboek van Strafvordering"). This Code safeguards that each request is necessary and proportional, since tapping is a severe invasion of privacy. One may wonder how serious the proportionality requirement is taken when The Netherlands is world champion in tapping telephones … In 2009 335 Internet connections were tapped. This is still a relatively low number, but the numbers are increasing rapidly:

jaar	2004	2005	2006	2007	2008	2009
deelnemers per 1-1	15	27	41	45	50	59
vorderinger	13	27	69	147	259	335
tapdagen	670	1168	2402	5468	7837	8920
gem. duur	52	43	35	37	30	27

Source: stichting Nationale Beheersorganisatie Internet Providers (NBIP), presented by Webwereld

Above you see the rising numbers (from 13 to 335 orders) from the year 2004 to the year 2009. In total the number of days that Internet connections were tapped, rose to 8920 in the year 2009. The average length of the individual tap declined to 27 days in 2009.

The Data Retention Directive also specifies the security requirements for the retained data (in article 7). The company has to provide for appropriate technical and organisational measures to ensure data protection. No one but authorised personnel may access the data. The member States have to ensure that unauthorised access is punishable (article 13(2) of the directive). In The Netherlands, data protection is regulated in chapter 11 of the Telecommunications Act.

The general rule is stated in the Privacy Act. This act states that all processing of personal data is prohibited, unless an exemption applies. And there are quite some exemptions! The most important exemptions are those of processing to execute a contract and processing on behalf of an investigation by the competent authorities. For telecommunications providers, the rules as stated in chapter 11 of the Telecommunications Act apply first. If these rules do not regulate something, the general Privacy Act applies. Both the Privacy Act and the Telecommunications Act follow the same approach: first all processing is prohibited, then a closed system of exemptions is provided.

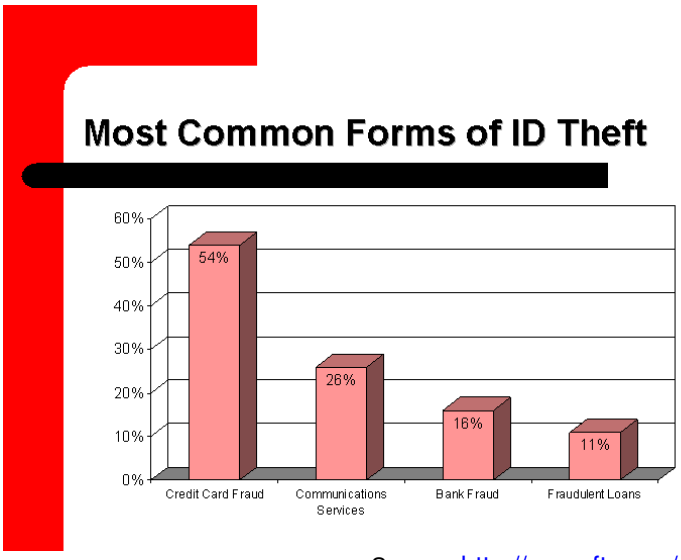
As we have seen, providers of **public** telecommunications services have to deal with a great number of regulations. It can hardly be surprising that companies will try to avoid this by maintaining that they do not provide a public network. The SURF Foundation, which provides network services to educational institutes, maintains that it is a closed community, because it is only open to legal entities that offer educational services. In

2009, the court found that SURFnet is not a public network.[4] The target customer base of SURFnet is sufficiently determined, to declare the network not accessible to the general public.

The SURFnet case shows, that not all telecommunications providers are providers of public networks that have to comply with the Telecommunications Act. The providers that do not have to comply with the Telecommunications Act still have to comply with the rules set in the general laws governing economic activities. Most notably we discussed the Privacy Act. Why this emphasis on privacy? After all, most people would argue, they have nothing to hide because they are no criminals. As the picture below shows, even the ordinary netizen (networked citizen) has to worry about his privacy.

It is therefore important that companies that provide online services do so in a sufficiently secure manner. The amount of online fraud is increasing year by year. In the US, 10 million people fell victim to identity theft in 2008.[5] For the EU, no numbers are known because there is no common legal definition of the crime in the EU, nor do all EU Member States have specific penal legislation. The European Commission proposed a new directive on attacks against information systems in 2010, building on the existing Framework Decision on attacks against information (Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems). [6] Article 13a of the Framework Directive regulates that Member States shall enforce that public network providers take appropriate organisational and technical measures to secure their networks.

[4] Source: http://www.surfnet.nl/nl/nieuws/Pages/StatusinontwikkelingenmetOPTA.aspx (in Dutch)
[5] Source: http://www.spendonlife.com/guide/identity-theft-statistics
[6] Source: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/139



Source: http://www.ftc.gov/os/2000/07/idtheft.htm

In The Netherlands, a company that does not provide for appropriate measures may be libellous under criminal law and civil law. Chapter 15 of the Dutch Telecommunications Act regulates enforcement of the rules. This may include penalties such as temporary closure of the service, or a fine of up to €450.000 for the company. Responsible employees of the company may be prosecuted under the Criminal Code. An employee who has made sensitive data public may be prosecuted under article 273 of the Criminal Code, provided the company reports a crime. Apart from that civilians can require payment of damages under article 6:162 of the Civil Code ("Burgerlijk Wetboek").

In The Netherlands, telecommunications operators are supervised by two National Regulation Authorities (NRA): OPTA ("Onafhankelijke Post en Telecommunicatie Authoriteit") and NMA ("Nederlandse Mededingings Authoriteit"). The NMA is the general authority that regulates competition. Apart from these authorities, a mediator ("Geschillencommissie Telecommunicatie") and the Consumer's Authority ("Consumentenauthoriteit") can interfere in telecommunications conflicts. And finally, the supervision with regard to processing of personal data is done by the Data Protection Authority ("College Bescherming Persoonsgegevens"). This is an impressive list of regulating bodies. It is quite possible that this leads to questions about the relative competence between those regulating bodies.

Summary

To summarise, providers of public electronic services and data networks have three obligations with regard to providing data in criminal investigations:

1. Providing a technical architecture that allows for tapping of data;
2. An obligation to provide for tapping of content of communications on request of the competent national authority (in The Netherlands this is the examining judge or "Rechter-Commissaris");
3. Finally, a general obligation for the retention of certain communications data, more specific the traffic and location data of each communication.

This concludes the seventh and final lecture.

Translation of the most important terminology

English – Dutch

Act, Code	Wet
Directive	Richtlijn
Personal Data	Persoonsgegevens
Policy making	Wetgeving
Retention	Bewaren
Undertaking	Onderneming

Dutch – English

Bewaren	Retention
Onderneming	Undertaking
Persoonsgegevens	Personal Data
Richtlijn	Directive
Wet	Act, Code
Wetgeving	Policy making