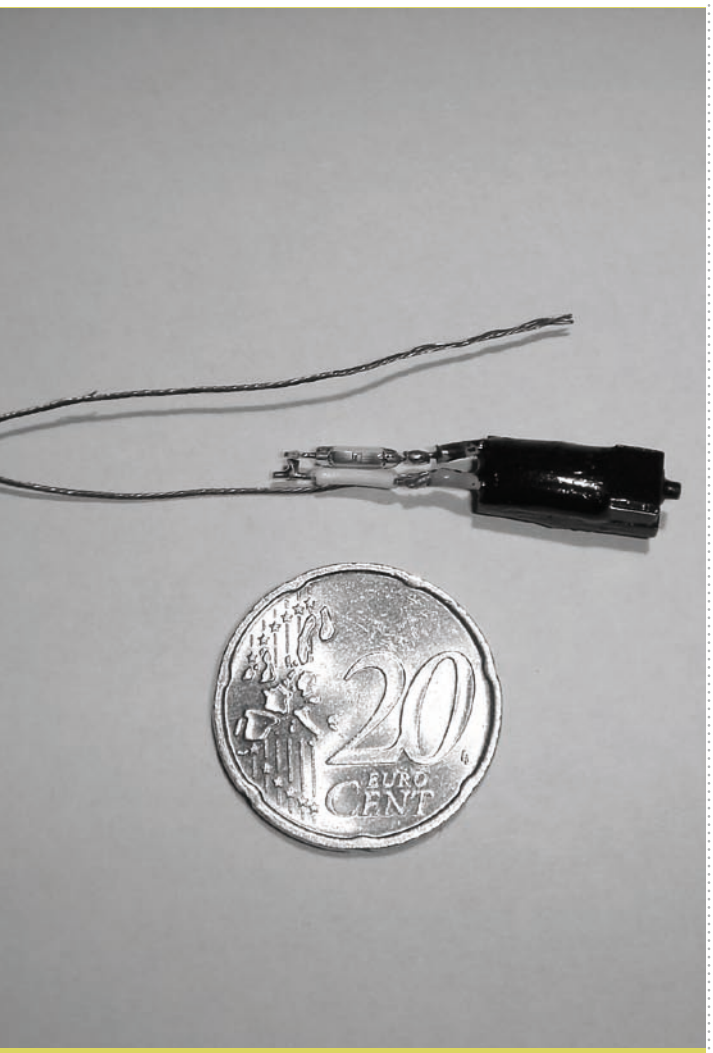
nominal price: 45,- €

LEGAL GUIDE
DEFENSE OF EAVESDROPPING AND PROTECTION OF INFORMATION

EDITOR:
RA ROBERT NIEDERMEIER,
ANSGAR ALFRED HUTH

TABLE OF CONTENTS

I. MEANING OF THE DEFENSE OF EAVESDROPPING / PROTECTION OF INFORMATION AND IT SECURITY



MINI TRANSMITTER - EAVESDROPPING BUG

The defence of eavesdropping and the protection of the information reflect an important subarea of the IT security.
Societies still extensively understand at present the IT security as the theme of the technique and organization fields. Only few professionals among the persons in charge with IT have recognized that the IT security field, besides the fields of technique and organization, is constituted also of the domain called law.
The legal position requires from a professional person in charge with the IT security the knowledge of the essentially legal contexts for his field of activity, such as a car driver has to know the traffic regulations. Without this knowledge the persons in charge with the IT security will not be able to complete their duties and thus will be bound to remain private liable amateurs of the IT security.

Information (Know how) still reflect at present the greatest and most fundamental economic unit of a company. The written or spoken word is here the target of defences of eavesdropping, as the object of communication like contract draft, offers, terms, calculations, applications, particulars and data related to the persons are conveyed here. This exchange of information occurs both internally but also externally.

1. Legal requirements for ensuring the IT security / for defence of offences of eavesdropping

Meanwhile the IT security belongs to the indispensable premises of the activity of each company. The duties of the company to guarantee the security of its data and IT systems are foreseen in the body of rules and regulations at national, European and international level.
At national level, among other principles for the organization of the trade, the law for telecommunication and the law for the data protection foresee obligations for the societies to adopt adequate technical precautions and other measures to guarantee the IT security.
The law for the control and the transparency in the society foresees a task for the creation of an internal system for the earlier identification of risks for the corporation; to the risks of a society belong also a missing IT security.

At European level the directive for the protection of data for electronic communication (directive 2002/58/ EC) is important. This one mentions that the user of a communication service with public access has to take adequate technical and organizational measures in order to guarantee the security of its services.

At international level there should be respected mainly the aggravated requests by Basel II and Sarbanes-Oxley-Law for US societies noted at the stock exchange and their outlandish subsidiaries. Basel II obliges to be taken measures because the IT security will be in future also relevant to the granting of a loan and its return payment. SOX requests from the respective societies to assure the integrity of their data. Insufficient IT security brings about claims for compensations for damages towards the society but it also causes the personal liability of the management.

CONCEALED TRANSMITTER IN THE WRITING PEN

II. WHICH ARE THE RISKS

EAVESDROPPING BUG
IN THE ONE – WAY LIGHTER

At present the greatest risk occurs in the unintentional and unseen transfer of company secrets to third parties.
Each company must think of relevant questions about the IT security in order to avoid damages (lost of money and image). The financial effects of an offence of eavesdropping can but easily threaten the existence of a company.

Each offence of eavesdropping that occurred due to defective and insufficiently adopted measures for the IT security has significant financial effects on the society, which is mostly related to often higher costs than those for a suitable IT security concept, respectively a necessary element for the offence of eavesdropping.
Who provides for a risk is able to avoid future expenses or at least to reduce them. A complete IT security policy takes always into account, beneath the technical solutions, the organizational measures and especially the legal aspects in the field of the IT security.

II.

1. Technical possibilities of the eavesdropping offence

The offences of eavesdropping can be realized e.g. by means of hidden fixed „microphones“ that are brought by employees, foreign personnel or third parties in the business areas, but also unconsciously sometimes the ones that are personally listened to. This is the case when the microphone is hidden in an advertising gift like a pen, an ash tray or sculpture and is fixed and placed by the target person, with his own hands in the room that has to be supervised.

The following eavesdropping devices are used especially at / with eavesdropping offence:

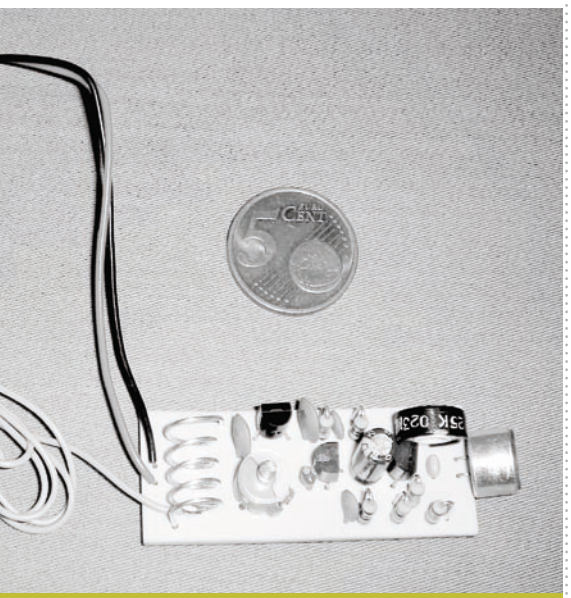
„Bugs“ Mini - transmitter

Function:

Hidden, disguised room microphones transmit discussions by radio. Reach: 20 m to 5 km. Connected to a scanner-mobile-unit: reach world wide. Supply with energy generally by battery, but also by line current and telephone network or solar cells. Passive bugs need no attached energy supply. The needed energy is simply radiated from exterior.

Hiding place:

The minor electronic parts can be placed in each hollow space, in integrated ceilings, floors, furniture, electric appliances, and room plants. What counts here are fantasy, ingenuity / resourcefulness and experience.



EAVESDROPPING BUG FOR 5 EURO

II.

1. Technical possibilities of the offence of eavesdropping

Mini – voice recorders

Function:

The small parts record language. A Dictaphone records several hours of discussions, even the smallest machine in a pen manages more hours of discussion recording. The modern cell phones have also the function for discussion recording that can realize several hours of disguised discussion documentation.

Hiding place:

Almost always do visitors carry with them recorders. These machines are attached to the body, or in briefcases, respectively to other conference tools or are hidden before the appointment into the accessories from the respective room.

PEN WITH 8 HOURS DISCUSSION RECORDING

II.

1. Technical possibilities of the offence of eavesdropping

Manipulated GSM-UMTS- cell phones

Function:

By manipulation of hardware and / or software of a cell phone these means of communication can be misused for disguised supervision of discussions and recording. The scope of performances of each cell phone can be modified at any time by remote control. Cell phones that during a sensitive discussion can realize arbitrarily and not recognizable by the owner a telephone connection to another call number overseas have been reality for years.

Hiding place:

The information point „hiding place“ does not apply to this eavesdropping tactic because the intercepted person does permanently take care that the eavesdropping technique (his own mobile) is nearby and also anytime ready, respectively accessible for operation.

STETHOSCOPE-TRANSMITTER WITH RECEIVER

Stethoscope-microphones

Function:

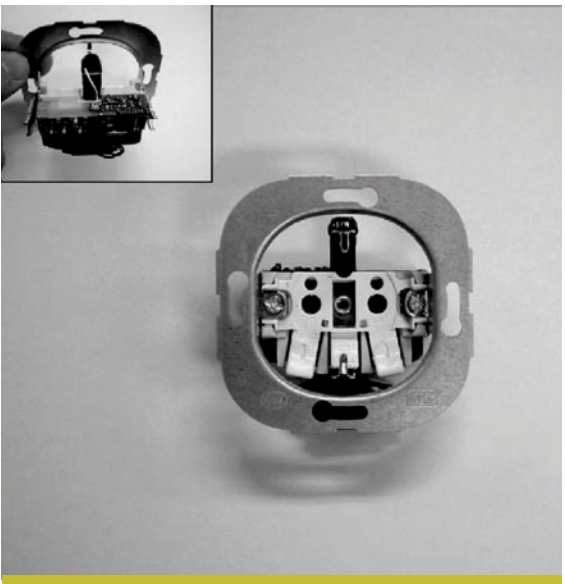
The eavesdropping person uses e.g. a heating device or the whole wall as a microphone. The sound waves displace bodies in waves that are caught, enforced, filtered and made audible by the device.

Hiding place:

The eavesdropping person sits unchecked in the neighbouring room or sends the discussions world wide by radio bug. Favoured eavesdropping places are also utility ducts that are constructed horizontally or vertically through all the levels.

II.

1. Technical possibilities for the offence of eavesdropping



IN WALL CONNECTOR / FLUSH SOCKET WITH EAVESDROPPING BUG

Wired-radio systems

Function:

Function in the building. The transmitter of long waves uses the 22- Volt –power supply line as antenna and procures power from the network. These supply line bugs need thus no battery. They do perfectly suit to a durable „data connection“.

Hiding place:

Attached to 220V- electric appliances. Often do the eavesdropping persons exchange the existing devices with prepared ones or implant the small transmitter during maintenance works or favourable upgrade. Especially preferred: attachment in commercial multiple connectors, extension cable or in wall connectors.

Fixed wired room microphones

Function:

The classical Stasi-bug is often installed even by the building construction. The discussions are overheard, evaluated and forwarded from a stable eavesdropping station in house.

Hiding place:

Room microphones can be found especially in ceiling covers and hollow spaces of the walls. This overhearing variant is used e.g. in hotels, conference centers and passenger airplanes.

II.

1. Technical possibilities of the offence of eavesdropping

DIRECTIONAL MICROPHONE

Directional microphones

Function:

The sound is captured by a parabola directional microphone or by a standard directional microphone. The sound waves are enforced, filtered and evaluated, like an evaluation of impact sound.

Hiding place:

The eavesdropping person overhears e.g. outside on a bench and orientates the top of his umbrella, unnoticed towards a person or an open office window. This top part of the umbrella, which is protected by small sleeve during walking, is the directional microphone.

Telephone bugs

Function:

Doers fix them e.g. directly to the telephone line, that also supplies the power. The transmitter is activated, when the handset is removed, supervises permanently the room in cases of sound waves or is activated from exterior.

Hiding place:

Telephone, telephone wall socket, telephone line, in the interior and exterior of the building (distribution box)

II.

1. Technical possibilities of the offence of eavesdropping

FAX MONITORING FOR RECORDING OF FAX MESSAGES

Fax-Monitoring-System

Function:

The system records all the incoming and outgoing fax messages on paper or data bases. The participants do not observe anything.

Hiding place:

The device is connected directly at the telephone line inside and outside of the building.

AIR REFRESHER WITH A HIDDEN CAMERA

Camera bug

Function:

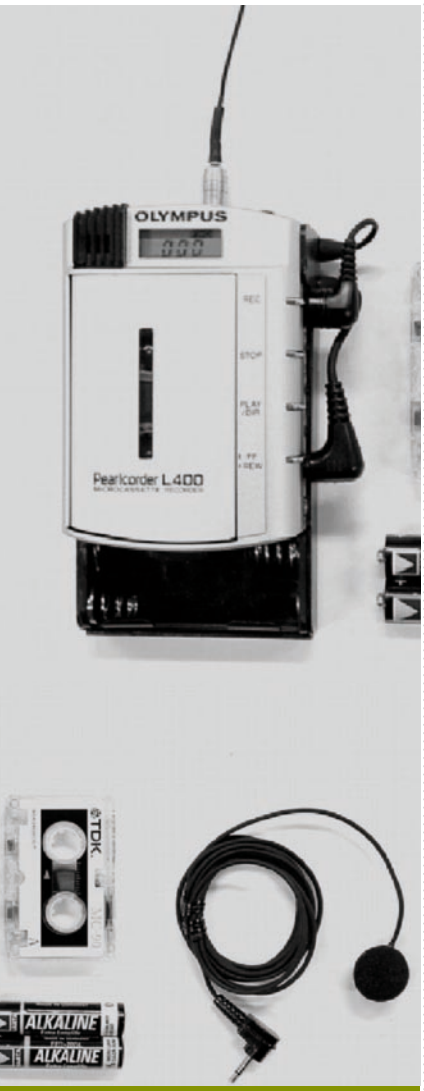
Hidden, disguised camera bugs transmit image and sound by radio connection. Coverage: 20 m - 5 km. In connection with a receiver – mobile – unit coverage: world wide. Energy supply generally by battery, but also by line current.

Hiding place:

The cameras, as big as a sugar bar, can be placed in each hollow space / cavity, e.g. in attached ceilings, pictures, mirrors, furniture, electric appliances.

III.

WHO IS RESPONSIBLE WITH THE IT SECURITY / EAVESDROPPING OFFENCE IN COMPANY



RADIO RECEIVER WITH DISCUSSION RECORDING

The top management of the company or the board or the Executive Board is legally responsible with the IT security.
The duty of the management or of the Execution Boards for the ensuring of the IT security results by now from numerous legal prescriptions. Thus was introduced for instance the KonTraG § 91 paragraph 2 Companies Act, whereby the Execution Boards of a corporation have to implement in company a system for the early identification of risks and for supervision. To the risks of a company belongs among others a lacking or defective IT security, respectively measures for the protection of the information. ***This is valid not only for the corporations, but also for all other forms of societies.***

The management can delegate decision authority to the employees of the society, especially to the managing employees, like the authorized representative or the leader of the IT department. Within the limits of their responsibility these persons can also delegate the responsibility field to administrators or other employees of the IT department. In each case should be the respective persons carefully selected and monitored, and it has to be ensured – by trainings and by putting at their disposal the necessary materials – that they fulfil their duties.

The delegation of duties for ensuring the IT security does not free the management from the liability for a missing IT security according to Companies Acts or to the limited liability company law. Also in case of delegation of adequate duties should the management monitor the appropriate fulfilment of these tasks.

The management receives support through special assigned persons who monitor the IT security and report to the management and who must submit proposals about this, without disposing of decision or instruction authority.

This one is valid, on one hand, for the operational or official person in charge with the protection of information, who has to be ordered according to the premises of the law for protection of information and, on the other hand, for the person in charge with the IT security whose appointment is ruled only with exceptions – in the telecommunication legislation or for some certain authorities, but virtually necessary for the guarantee of the IT security.

III.

VHF-SELF CONSTRUCTION KIT - EAVESDROPPING BUG

1. As person in charge with the IT security, do I sail close to the wind?

If there is identified a typical IT punishable act in the responsibility field of the person in charge with IT, then he / she personally or a representative of the company, as substitute, may incur a penalty for this act.

The unauthorized disclosure of secret information about the company (company and business secrets) or about employees (personal data) reflects an enormous risk for the company. The management of the company is thus subject to strict exigencies.

Penalty may incur also the one who (for instance because of cost reasons) contrary to duty neglects the implementation of the necessary security measures and thus assenting accepts that, for example, secret information is made accessible for third parties.

To these security measures besides email - filtering also belongs to the protection against offences of eavesdropping, respectively protection of the company - internal network, but also of the data - critical rooms in the company.

The functionality and efficiency of these security measures has to be permanently verified and revised also by the persons in charge. For the domain

III.

of eavesdropping defense this means that the controls for eavesdropping defense are effected in intervals that can be accounted for in the sensitive spaces. The shorter the intervals of time between the controls for eavesdropping defense are, more manageable and clearer it is in case of a detected eavesdropping offence to limit the caused damages, respectively the concerned business domain. A detected eavesdropping offence, that means information outflow for several weeks or even months for the company, can be but hardly limited, respectively estimated in its depth effect and impact related to the company planning and know - how loss.

2. As person in charge, do I have to be liable with my private property?

If the necessary IT security structures have not been implemented or have been but insufficient implemented and there comes up the case of an unauthorized information transmission to a third party, the IT security responsible risks the liability of the company and his / her own person. As the case may be, this means that he must pay the costs for the realized damages with his own private means. Otherwise as in the Criminal Law, in the Civil Law the IT security responsible is liable also for negligence. If the management did not name any employee (legally verifiable) as person in charge with the IT security, naturally that the first who are responsible is the management, respectively the Executive Board of the eavesdropped company, with their private means for the caused know - how loss.

Here acts negligent the one who breaches the incumbent duty of care in the business connections of a fair business man. Who omits negligently the security measures has to take into account that the damages caused by him cannot or cannot be completely replaced. Thus, the author of the damage can raise objection of the contributory negligence because the damage had been caused only in low volume. The insurance can refuse the payment if the conditions of the IT security of the insurance terms have been violated.

GPS-CAR
TRACKING SYSTEM

Also reports, expertises or recommendations for protection measures of the IT security responsible or external expert ignored by the management may lead to the liability of the whole senior management of a company.

III.

3. What are other sanctions that menace?

In case of financial losses there should be taken into account a liability with private means / personal wealth. Further, the persons in charge with the IT security are menaced by dismissal and cancellation of the employment contracts.

REMOTE CONTROLLED CIGARETTES WITH ATTACHED CONCEALED EAVESDROPPING BUG AND ACCUMULATOR PACK

IV.

LEGAL DUTY FOR DEFENSE OF EAVESDROPPING / SECURITY OF INFORMATION

The legal duty results partly from a contractual agreement, partly from the Federal Data Protection Act, but also from the obligation of secrecy in case of employees with professional secrets.

Especially the Federal Data Protection Act foresees in § 9 BDSG the duty that each responsible office must introduce appropriate technical and organizational measures in order to assure the requirements of the Federal Data Protection Act.

Beneath this aspect, there may occur, for example, a gradual access check to the personal data that should be accessible only depending on the intended use of the respective person in charge. Consequently, it should be ensured that no third party has access to the existing company – internal data and information.

A consequence of the insufficient protection of the information is the liability of the company towards the respective third party. ***If data about the customers or about the business partners become disclosed to the public because of insufficient protection, then the company has to face the claims for damages of this person.***

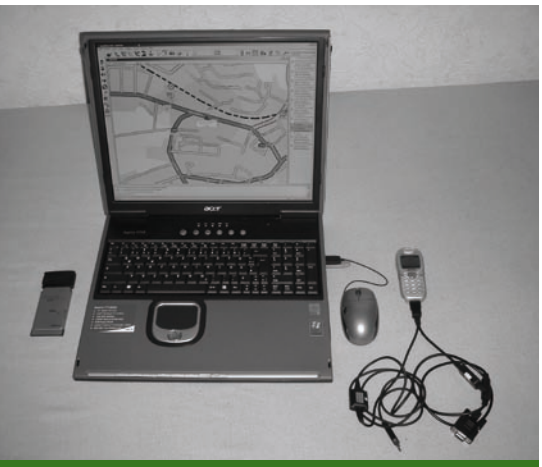
Companies that spend many resources on IT security, but do not take correspondent measures in the field of protection of information, manifest an explicit structural interruption because the domain of the protection of the own business secrets, but also the protection of the business secrets from contractual partners is but only holistically possible.

SMOKE–
DETECTOR
CAMERA

IV.

This discrepancy already questions the fulfillment of the Compliance demands and leads to the exposure of the executives/managers. This exposure can have massive negative effects because the reflected structural interruption leads regularly to deficit of or losing the protection insurance of the company and / or of the executives (D&O insurance). Insurances regularly foresee in their contract terms that only companies that are correctly structured, according to the law, enjoy coverage of the insurance.

Lately the companies have made repeated legal claims on the executives and – privately – asked them to pass by the cash office. These judgments are regularly not published because the dispute parties engage themselves to confidentiality. Evidence, like in the VW – corruption case, that the concerned D&O Insurance supports the caused damages, is the absolute exception.



GPS-CAR
SURVEILLANCE CENTRE

EQUIPMENT FOR THE SURVEILLANCE
OF THE MOBILE NETWORK

V. WHAT CAN I DO AS PERSON IN CHARGE

Each damage event, which occurred because of lacking or insufficient security measures, has a significant financial effect on each company, and it is generally related to much higher costs than those for a suitable security concept.
The one who provides against a risk can avoid future damages or losses or, at least, reduce them. A complete security policy always takes into consideration, besides the technical solutions, the organizational measures and, especially, legal aspects in the field of security of the company towards eavesdropping offence.

1. What are the technical possibilities?

Related to the use of email and internet the company has to install software for email filtering, for the detection of intrusion, firewall, etc.
The word spoken in sensitive spaces (offices of decision makers, their antechamber, conference rooms, rooms in which are taking place sensitive discussions) have to be protected by means of regular applications for the defense of eavesdropping, respectively spying technique.

VIDEO RECORDER WITH ATTACHED SPYING CAMERA

Related to the spoken word that is conveyed by telecommunication (ISDN, GSM, UMTS, VoIP, etc.) there should take place a regular check of the telephone lines, telephone system, respectively LT – appliances. Especial sensitive information and discussions may be transmitted only cryptologically encoded by telecommunication.
There can be also taken into consideration the arranging of meeting rooms protected against eavesdropping.
Gradual access controls in the whole company area, especially in sensitive rooms by means of code cards or biometrical authentication, in connection to a technically well-engineered video surveillance, illustrate the base for the protection of information.

V.

2. What are the organizational possibilities?

Technical measures must be flanked by a range of organizational measures.
The most important is to coordinate the IT security policy with regard to the eavesdropping defense / protection of information and on basis of an IT – security – guideline to develop and implement an IT security concept.
Such an intention helps to identify the weak points in the infrastructure of the IT security. Code cards or biometrical authentication, related to a technically well-engineered video surveillance illustrate the base for the protection of information.

A written IT security concept documents the organization of the IT infrastructure and its surveillance. Only this way is it trustworthy possible, in case of dispute, to present the proof (for exoneration) that the legal requirements of the IT security have been met.

After an occurred theft of information, a beforehand rendered survey of an independent expert in eavesdropping defense proves that the management has been seriously concerned with the subject of eavesdropping defense. Regularly organized verifications for the defense of eavesdropping prove the duty fulfillment of the management, respectively of the persons in charge with the security of information and know – how – protection measures.

An important part of the organizational measures is situated in the psychological field. For the implementation of the IT security concept for eavesdropping defense / protection of information the decisive factors are the consciousness of the employees for the IT security and the acceptance of the necessary measures. If there is possible an employees representation/delegation, this should be early incorporated.

TISSUE DISPENSER
WITH ATTACHED
SURVEILLANCE CAMERA

V.

As organizational measures in the frame of the IT security concepts for eavesdropping defense / security of information there come especially into consideration:

- exclusive, normally locked and specially equipped meeting rooms
- mobile interdiction (temporally and spacial clearly defined)
- verification of the adherence to the mobile interdiction by means of detectors
- discipline in the discussion behavior, even during the breaks of a meeting
- regularly checking of the sensitive rooms by means of an expert in eavesdropping defense
- control of the advertising gifts for possible microphones
- discipline when using the telecommunication appliances
- protection of information in the reception area and in public visible areas (reception counter, - visitors` book should be kept closed and the written page of the documents should be faced down, supervision monitors shouldn't be visible etc)
- reports, respectively discussions regarding the internal company aspects should not be carried in the private life
- training of the employees regarding the topic protection of information at the working place
- sensitizing the know – how responsible of the company regarding the topic industry spying
- consequent input of discussion and data coding
- consistent application of the discussions and data encoding · regular control of the network, telephone and data lines for manipulations with the help of an expert in eavesdropping defense
- remote maintenance of IT systems and LT equipments shouldn't be allowed.

V.

3. What are the legal possibilities?

The technical and organizational measures must maintain the limits of the legal permissible frames. Hence it is urgently recommended that the implementation of the eavesdropping defense / concepts of the protection of information should be legal accompanied.

A legal surveillance assures that the legally prescribed structures for the protection of information are implemented in company to a sufficient extent and in the needed depth and the company keeps relevant arguments documentation about these structures.

The main premise for the surveillance of the email / internet traffic, but also of the communication behavior related to phoning represents the fact that these media are used exclusively for company purposes. Thus the private use should be completely excluded. Otherwise the company becomes the telecommunication service provider that is liable for the secrecy of telecommunications. The storage, but also the content control of the correspondence between the employees, even if related to business, becomes thereby problematic.

If the management decides to introduce the video surveillance in company, because of security reasons, then the Federal Data Protection Act should be taken into consideration.
In case of surveillance at the working place should be paid attention that this one is not covered by § 6b BDSG. Thus there are applicable general prescriptions related to the protection of personal data. The introduction of a video surveillance of the employee requires the acceptance of the works committees according to § 87 I No. 6 BetrVG. But even after obtaining the approval of the works committees the global complete video surveillance of the employee is illegal.

For using the equipments of video surveillance for the purpose of access control there should be consulted § 31 BDSG. There is needed the notice of legitimate interests for concrete purposes. This is then the case when the situation is justified according to rational considerations. The concrete purpose of the video surveillance must be set before the implementing of the surveillance, namely it must be documented.

VI. SUMMARY

In order to assure an applicable extent of eavesdropping defense / information security, there is recommended to draft a special IT security concept for eavesdropping defense / information security, in collaboration with an independent expert. Only through this can be effectively avoided, at least reduced to a minimum extent, that the eavesdropping offences of sensitive company data shouldn't reach third parties.

Even today, when the know – how represents the most important company good, there must be clear valid regulations related to the business secrets both for the employees and for the management.
Otherwise the company is threatened by reductions, for instance in the field of company liability insurance or a relative reputation loss in the respective trade segment.

Many companies prosper and decay with increasing frequency in our days. The one who as manager does not master his perishable good „information" knowledge should delete the word future planning from his jargon. It will survive only those companies which cleverly upgrade their information knowledge and which will efficiently protect it. This is how it sounds the law of our achievement-oriented society and in the future this will intensify even more!

The managers and / or the persons in charge may incur penalty (for instance because of cost reasons) contrary to duty if they neglect the implementation of the necessary security measures (e.g. checks for eavesdropping defense) and, thus assenting, accept that secret internal information is made uncontrolledly accessible to third parties.

Lost company internal information can be neither replaced nor again acquired.

In the field of the IT security and the defense of eavesdropping there is valid prevention instead of elimination.

EDITOR:
RA ROBERT NIEDERMEIER,

Robert Niedermeier is member of the Information Communikation Technology (ICT) study group at the Heussen Advocate Company and predominantly concerned with questions of legislation technique and organization for data protection and IT-Security. With his international team he makes projects for banks, insurance and international companies of world-wide Roll-out homogeneous structure of data protection and IT-security in multicorporate enterprises and develops new designs for Compliance in the field of IT-Security. In his capacity as Executive of the European Institute for Computer Anti-Virus Research (EICAR) he discusses with the IT security domain about the legal admissibility of the so-called „Strike-Back".

ANSGAR ALFRED HUTH

Ansgar Alfred Huth is an internationally accepted expert in data protection and eavesdropping defense who has been acting in the fields of eavesdropping security and information protection for the world of industry and banking for many years. In his partially public seminars he is also training European special units, but also official representatives of countries, in the field of the defense of spying and acquisition of information.
Even VIPs trust the aspects of protection of their family and private sphere through the know-how of this specialist in eavesdropping defense. His operation in the background of numerous companies, even quoted at the stock exchange, professionally assures for the decision makers and persons in charge in these companies the vital factor „ protection of information".

RA ROBERT NIEDERMEIER

ANSGAR ALFRED HUTH

www.spionage.info