Summary

The use of telephone and Internet taps in criminal investigations

The study: cause, research questions and data collection

Cause and research questions
In the Netherlands, the use of telephone and Internet taps often makes the news. These news articles are not based, however, on recent research about the use of the tap. The tone of these articles is often set in by the lack of information on this subject. Annually, the Ministry of Security and Justice publishes the number of telephone taps which have been used by Dutch investigative services. In response to questions posed by the Dutch Lower House about these tapping statistics in 2009, the then Minister of Justice promised to commission a study on the use of the telephone tap (*Kamerstukken II* 2009/10, 30 517, number 16). The aim of this study is to provide insight into the actual use of telephone and Internet taps in criminal investigations. This report consists of several parts. In part I, after the introduction, we will discuss the telephone and Internet market; in part II, we will give a broad description of the use of telephone and Internet taps in the Dutch investigative practice; part III of this report will focus on the question how criminal investigators use the tap in some of the West European countries surrounding us (England and Wales, Sweden and Germany); and in part IV, we will discuss the findings of this study in our final conclusions. The starting point of this research has been an indirect presentation of the question:

1. In what ways are telephone and Internet taps used in the Netherlands during the criminal investigation process?
2. How do some other West European countries handle this means of criminal investigation?
3. Is it possible to explain (big) differences in the use of this means of criminal investigation between these countries?

The various research questions can be summarized as follows: how often, why and when do criminal investigators use the telephone and Internet tap, how long does the tapping last, and what kind of information does it yield?

Data collection
Answers to the above research questions are gathered by studying legislation and regulations, by literature research and by conducting interviews. To be able to give a broad description of the use of taps in the investigative practice, and of the considerations on which this use is based, for the Dutch part of our study we have conducted interviews with 55 people who deal with taps professionally. The people involved were criminal investigators, public prosecutors, examining judges and lawyers, among others. This study was conducted on a national level and in two regional police districts that differ from one

another with regard to the number of committed crimes, staffing, and the way in which activities are organized that involve the use of special powers of investigation. These regional police districts are not chosen for the purpose of comparison, but to be able to present a good description of how the tap is used. For the parts of this study dealing with other countries, we have conducted interviews in the selected countries with in total 14 experts and 3 academics specialized in the field of (data collection on) the tapping of telephone and Internet communications.

The telephone and Internet market
In the past decades, telecommunications traffic has grown explosively. Beside the increase in telecommunications, which is partly caused by the enormous expansion of the use of the mobile phone, the way in which telephones are used has changed as well. An ever growing number of mobile phones is connected to the Internet, and a growing share of communications take place via the Internet. Communication gets increasingly fragmentised because of the possibilities and channels that are available (VoIP, mail, chatting, forums, games, social media, etc.). This has major consequences for the way in which the telephone tap can be used in the practice of criminal investigation. It is expected that in the future, more and more often Internet taps will be used to intercept communication. Although at this moment, the main part of telecommunications can still be intercepted with a telephone tap, the rapidly changing supply of communication services on the Internet makes it necessary to review the possibilities for tapping on a regular basis (Stratix Consulting, 2009).

The regulation of tapping in the Netherlands

The Special Investigative Powers Act
Tapping telephone and Internet communications is an infringement on the right to privacy, a basic right guaranteed by the European Convention on Human Rights (article 8 ECHR). The public authorities are allowed to infringe (see paragraph 2), however, only when this infringement congregates the requirement. In the context of the more detailed interpretation of article 8 paragraph 2 ECHR, the use of a telephone and Internet tap requires a definition of the categories of people who can be subjected to this investigative means, how long and with regard to which crimes this investigation tool can be used, and which procedures should be observed while working up the tapped communication. In the Netherlands, the tapping of telephone and Internet communications has been provided with a legal base in the Special Investigative Powers Act ('BOB' in Dutch).
Placing a telephone or Internet tap (article 126m Code of Criminal Procedure) constitutes a special power of investigation. It has been laid down in

the Special Investigative Powers Act that special powers of investigation may be used based on three titles: 1) on the suspicion that a crime has been committed (title VIa); 2) based on a reasonable suspicion that crimes as circumscribed in article 67 paragraph 1 Code of Criminal Procedure are being plotted or committed within an organized association, which in view of their nature or their connection to other crimes plotted or committed within that organized association will result in a serious violation of the legal order (title V); 3) on indications that a terrorist crime is being committed (title Vb).
A number of special investigative powers has been regulated for specific application, others only as far as they are systematically applied. The legal conditions stipulated for the special powers of investigation provide some insight into the extent to which they are perceived as being far-reaching. Thus, the degree of suspicion, the person against whom a special power of investigation may be used, the duration of that use, the procedure to get permission, and the grounds on which the use of a special power of investigation is based, may all tell us something about the extent to which the means used are perceived as being extreme.
When the Special Investigative Powers Act came into being, the legislator assessed the tap as being one of the most extreme powers of investigation. Its use must answer the requirements of proportionality and subsidiarity. The tap can be used only in case of crimes like those circumscribed in article 67, first paragraph Code of Criminal Procedure. In addition, the nature of the crime must result in a serious infringement on the legal order. To conclude, the investigation must be in urgent need of the use of the telephone tap. The tap may only be used if it is impossible to achieve the same result with lighter powers of investigation.

Professionals pledged to confidentiality
To some occupational groups (for instance judicial and medical occupations) the right of non-disclosure applies. This means that it is not allowed to listen in on or record conversations suspects have with these professionals pledged to confidentiality. It has happened in the past that worked-up conversations between suspects and professionals pledged to confidentiality had ended up in the process file. A well-known example of this is the criminal case against members of the Hells Angels in the Netherlands. Meanwhile, action has been taken to avoid blunders like these in the future. These measures consist of an instruction on the way in which investigators are to deal with intercepted communications with professionals pledged to confidentiality and a caller display system. This system has been put into use on 1 September 2011. It holds the telephone and fax numbers handed in by lawyers and associated people to whom the right of non-disclosure applies in a filter registered with the National Interception Unit (ULI). When a telephone number is tapped, the traffic data (telephone numbers, point in time, etc.) are routed to a filter. When the system recognizes a telephone number, the recording is ended

automatically. In case there is a delay in the relaying of traffic data, the communication already recorded is wiped. In this new system, the investigation team only has access to the traffic data pertaining to the conversations with professionals pledged to confidentiality who are registered in the system. It is mandatory for all lawyers to take part in the new system. It is expected that, with the introduction of this system, the problems with regard to the recording of conversations with professionals pledged to confidentiality included in this caller display system have been overcome. Yet, conversations with other professionals pledged to confidentiality, such as doctors or clergymen, are not automatically filtered. To such conversations, the older arrangement still applies.

Notification, destruction and use for another purpose
Suspects against whom a special power of investigation has been used must be informed about this as soon as the investigation's interest allows it. There are a few exceptions to this rule. A suspect does not need to be notified if he/she already has been granted access to his/her file, if that notification is in fairness impossible, for instance because the authorities have been unable to find out the identity or residence of the person involved, or when a security risk is involved in the notification. The postponement of the notification of those involved is bound to terms. Two months after the notification, all information gathered by means of a telephone or Internet tap must be destroyed. Sometimes destruction can be postponed because the public prosecutor wants to use the data in another investigation, or because the public prosecutor wants to store the data in the so-called 'serious crime register'.

What is a tap and how does it come about?

A telephone tap is used to tap the communication from or to a specific telephone number or telephone. Tapping communication means that the content (article 126m Code of Criminal Procedure) and traffic data (article 126n Code of Criminal Procedure) of conversations are passed on by the provider to the National Interception Unit (ULI) of the National Corps Police Services (KLPD). By means of an Internet tap, all Internet traffic (or if an e-mail tap is involved, just the e-mail communications) on a specific Internet line are intercepted.

Traffic data
It is also possible to ask for traffic data only. In that case, an investigation team only obtains information on the telephone numbers of the caller and the person called, the data, the point in time and length of the conversation, and information about the transmitting mast. It is possible to ask for two kinds of traffic data: past and future traffic data.

Past traffic data provide insight into a person's calling behaviour over a period in the past, while future traffic data provide information on someone's calling behaviour during the criminal investigation. Traffic data can be of value for mapping social networks and may play a role in considerations about whether or not particular phone numbers should be tapped. Asking for traffic data constitutes a lighter special power of investigation than the telephone tap and can be demanded by a public prosecutor without authorization by an examining judge. Asking for traffic data with regard to Internet communication provides insight into, among other things, the time of logging on, the IP address, information about e-mail adress contacts of both sender and receiver and the protocol used.

Procedure

It is the public prosecutor who, after authorization by the examining judge, issues a tapping order to the criminal investigator. When a tap is requested, there are two checking moments. Firstly, the public prosecutor checks whether the legal requirements have been met, such as the presence of suspicion; whether there is the threat of a serious infringement on the legal order; and to what extent the investigation urgently requires the use of the tap, taking into account the requirements of proportionality and subsidiarity. Secondly, the examining judge checks whether the public prosecutor could have come to a reasonable decision to start using the tap and checks a second time whether all requirements have been met.

In urgent situations, it is possible to request an 'emergency tap'. In that case, the public prosecutor and the examining judge confer by phone, and the tap can be installed on very short notice if the examining judge issues an authorization. After this, the tap request needs to be confirmed in writing. A tap authorization can be issued for a maximum period of four weeks, but the examining judge can also decide to allow the tap only for a shorter period. This is often done in case of an emergency tap. A tap may be ended prematurely, but when it is considered necessary to continue a tap, the public prosecutor first needs to present the examining judge with a request for continuation.

Notification and destruction

In practice, the notification of people who have been tapped is left to the 'Special Investigative Powers chamber' (people working at the Public Prosecution Service who take care of the administrative settlement of requests and of continuations of special powers of investigation, notifications and the destruction of data). They register names and addresses, collect signatures from the public prosecutor and finally send the letters of notification. A record must be destroyed two months after notification. This is also coordinated by the Special Investigative Powers chamber.

Central Information Desk Telecommunication Research (CIOT)
Before a request for a tap is submitted, investigators need to make sure that the telephone number or IP address involved is still being used. This can be checked by asking the CIOT. The Central Information Desk Telecommunication Research is the link between investigative services and telecom companies and takes care of the storage and use of identifying data. Identifying data are the name, address and place of residence connected to telephone numbers, e-mail addresses and IP addresses. Providers of telephone and Internet services are obliged to refresh such data every 24 hours. Authorized investigative services can ask the CIOT for these data. Such requests may only be made on the basis of articles 126n, 126na, 126u, 126ua, 126zh, 126zi, 126ii Code of Criminal Procedure, article 29 Intelligence and Security Services Act and article 10.10 Telecommunication Act, in the context of a specific criminal investigation.

Statistics

Annually, the Ministry of Security and Justice publishes the number of telephone taps deployed by the Dutch investigative services. The statistics are based on the numbers of tapping orders issued by the examining judge. For each separate telephone number, IMEI number, IP or e-mail address, a separate tapping order needs to be drawn up. When the tapping statistics are compared to the total number of telephone numbers in use in the Netherlands, it turns out that annually, a tapping order has been issued for approximately one in every thousand telephones in use. The number of taps on landlines has remained stable throughout the years. The increase in the number of telephone taps since 1998 can be attributed mainly to the rise of mobile telephony. In 2010, the number of taps amounted to 22,006. In the Netherlands the number of taps has decreased over the last years, both in an absolute sense (with almost 17 per cent in 2010 in comparison to 2008) and in relation to the total number of telephone connections in use.
For the year 2010, the number of Internet taps was published (1,704) for the first time; during the second half of 2010, investigators submitted requests for historic data pertaining to both historic traffic data and identifying data 24,012 times.
An account is kept of the number of requests made of the CIOT as well. This number has steeply increased throughout the years. Regularly, the number of requests at the CIOT is criticized because the disclosure of identifying data of all kinds of people, connected to particular telephone numbers or IP addresses, means a violation of privacy. This large number is mainly attributable to requests pertaining to transmitting mast data (identifying data of all numbers from which calls have been made at a particular time via a particular mast) and pertaining to contra numbers (numbers or IP addresses that are

in contact with a number or address that is tapped or of which the traffic data have been requested).
To be able to use the information from mast data or about contra numbers for the investigation, investigators try to find the identity of the users of these numbers or IP addresses. However, this is difficult because the CIOT often does not have any identifying data in its database of the large numbers of pre-paid mobile phones that are in use.

Telephone taps in practice

Crimes
This study shows that tapping is used in different ways and with many different goals. In case of calamities the tap is used rapidly and widely, for the sake of a quick determination of the direction the investigation should take. The tap is also regularly used in case of more frequently occurring crimes, such as violent robbery of a mobile phone. Because a stolen phone is usually quickly resold, in such cases the use of the tap is focused, quick and short. In case of an investigation of serious crime, on the other hand, the telephone tap is used frequently and for longer periods of time. This type of cases often involves continuous criminal activities such as drug trafficking or human trafficking about which suspects communicate with each other (over the phone). In this kind of investigations, the yield of tapped conversations as regards content is mainly supporting. In these cases, direct evidence is seldom established by means of a tap. Seasoned criminals are well aware of the fact that they are being tapped and have adjusted the way in which they communicate by phone accordingly. To map networks and organizations, investigators make use in particular of traffic data.

Goals and considerations
The objectives of tapping often are: to obtain directional information by collecting background information about a person or network, to obtain evidence, to obtain data about the location of a tapped person by analyzing the content of conversations and traffic data, or a combination of both. The tap may also be used in support of other means of investigation.
Various considerations play a part in the decision to start tapping someone. First of all, it must be certain that the proportionality and subsidiarity request are met. Is the use of the means proportionate to the nature of the crime, is it necessary, and is there no lighter investigative power with which the needed information can be secured? Furthermore, the capacity of the investigation team also plays a role. The team must be adequately staffed to be able to process the conversations. The personal preference of the team leader and the ease with which a tap can be realized play a role as well in the decision to use a tap or not.

Not only suspects may be tapped, but also other people involved. Examining judges, public prosecutors and also several police officers indicated that they are more restrained to start with tapping an involved person than they are with tapping a suspect. The number of taps per investigation differs strongly and depends on the considerations described above. Of course the number of suspects involved in a case and the number of telephones and SIM cards which are used play a role in this as well.

Request for traffic data
Traffic data provide important insights in investigations into various kinds of crime. They may provide insight, for instance, into the contacts or the network with which suspects and/or victims communicate or have communicated in the past. Historic traffic data may play a part in the considerations whether or not to tap a particular phone number. The data show how many calls are made, how long, with whom or with which specific number. Based on this, investigators can estimate the capacity needed to listen in on and process a tap. In addition, sometimes historic traffic data are requested when a public prosecutor does not consider a crime serious enough to place a tap. With the aid of traffic data, investigators can then gain insight into the communication streams used by a suspect all the same.
An important advantage of historic and future traffic data in comparison to a tap is that investigators do not need to listen in on conversations and process them afterwards. For the examining judge, the request for traffic data submitted beforehand is not a precondition for allowing or rejecting the use of a tap. Deciding whether it is necessary to gain insight into the ways in which particular phone numbers are used, is the responsibility of the public prosecutor.

Asking for data from the CIOT
A disadvantage of using traffic data is that it is not always possible to obtain the identifying data of the numbers that have attracted attention as a result of the request. Respondents indicated that requesting identifying data for these numbers at the CIOT often remains without result, since much use is made of prepaid telephone numbers of which no identifying data are known at the CIOT. In such cases, a tap makes it easier to find out the identity of the user of a specific phone through the information revealed by the conversations conducted and contacts maintained by the caller.
Police forces can only ask for information at the CIOT according to a legally established procedure. If forces do not meet these legal requirements, they are not allowed to submit requests for information. At this moment, all investigative services are able to ask for information at the CIOT according to the established rules.

Listening and processing
To listen to all intercepted telephone calls and to process the conversations is labour-intensive and asks a lot from the investigation team. It is specialist work: experience with the elaboration and interpretation of telephone taps is crucial for the quality of the result. Besides experience, staff continuity is also important. Investigators must get an opportunity to familiarize themselves with the voices they hear on the lines to be able to acquire voice recognition. The respondents from the legal profession consider the quality of elaborated conversations to be variable. Whenever a conversation has somehow been elaborated in a one-sided way, perceived as biased by the suspect, the lawyer may request to listen to the conversation in question him- or herself.

Interpreters
During the tapping of phone calls, the language spoken is in many cases different from Dutch. In cases, an interpreter is called upon. In the regions and public prosecutor's offices we studied, the procedures with regard to contact and working with interpreters were interpreted locally; they therefore differed in several respects. According to the respondents, working with interpreters has the advantage of getting additional staff. A disadvantage, on the other hand, is the dependency on an interpreter – translations often are unverifiable for the team. When in doubt, the investigation team may let a second interpreter listen to the content of conversations, which actually is standard procedure when conversations are considered of great importance to a case. The majority of the respondents had a positive opinion of the work turned out by interpreters. For some languages, however, interpreters are hard to find; as a result, investigation teams sometimes have to wait until an interpreter is available, which may delay the investigation.

Continuation or conclusion
The considerations about either ending or continuing a tap depend on the ratio between the information yielded by that tap and the capacity needed to obtain that information. Respondents indicated that they usually abort a tap that does not yield any relevant information. Yet, a lack of capacity to listen in on the lines and to process the results may be a reason to put a premature end to a tap as well. It also happens that a tapped line turns out to be 'dead'. This means that the telephone number is not in use and thus will not yield any information. When a case is closed, the taps are closed as well. The examining judges indicated to us that the longer a tap is used, the more critical they are when they have to assess a request for continuation. According to the respondents, the extent to which a tap infringes on persons' privacy is part of the considerations to either continue or conclude a tap.

Privacy

Since the law has been amended on 1 February 2000, tapping no longer only covers communication in which the suspect participates. Involved people, people who maintain a relationship with the suspect in one way or another, or people who may know something about the crime committed may now be tapped as well. The decision to use a tap is taken after weighing the interests at stake and the results that might be expected. One of those interests is the right to privacy, which regularly clashes with the interests of an investigation. According to the respondents, they are more strict when the person to be tapped is just someone involved. Then the investigation team needs to motivate even more convincingly why they want to tap this person and what this might yield to benefit the investigation. In addition, the term for which the examining judge issues permission is often also shorter in case the tap concerns someone involved, in comparison to terms for tapping suspects. Nevertheless, putting a tap on someone involved can sometimes be more important than putting a tap on a suspect, because people involved may be less aware of the possibility of being tapped.

It is certain that the telephone tap constitutes an infringement on privacy, according to the respondents. The respondents themselves thought that they should deal with taps very carefully, using them only if something big is at stake and it is expected to really yield a result. When the use of the telephone tap is compared to the use of the Internet tap, opinions differed on the question which of the two powers of investigation constitutes more of an infringement on privacy. The use of the Internet and the telephone increasingly merge, also because of the Smartphone, making the discussion about the seriousness of privacy violations by either kind of tap obsolete in the long run, as a respondent argued.

Professionals pledged to confidentiality

Information obtained from conversations with people who fall under the right of non-disclosure is not allowed to be included in the investigative process. As mentioned earlier, to prevent this from happening, a caller display system has been set up for conversations with lawyers. Upon inquiry at the beginning of January 2012, it appeared that although the caller display system has officially come into effect, it does not yet function optimally. This is due to the fact that not yet all lawyers haven been able to get registered in the new system, due to a problem with registration. When this problem will be solved is as yet unclear. Although the caller display system has come into effect, the 'old' method of working[216]for conversations with professionals pledged to confidentiality must still be observed.

In the new situation, too, the police and the Public Prosecution Service remain responsible for the correct destruction of conversations with professionals pledged to confidentiality.

216 Instruction on the destruction of intercepted conversations with professionals pledged to confidentiality.

Results

Telephone taps mainly yield directional information and information with which it is possible to trace suspects or victims. Regularly, a tap generates information that can be used to determine the direction of the investigation, to start using specific other means of investigation, or to establish the location of specific people.

In addition, the tap provides the investigators with evidence, although this happens less and less often, according to our respondents. They indicated that the main importance of tapped conversations is that they yield circumstantial evidence, that is, information that supports other evidence. They supply 'another piece of the puzzle'. Although this is not a goal in itself, taps also often yield other information, about other crimes or persons. Whether the investigators respond to this, and in which way they do, depends on the nature of the information and the seriousness of the crime to which this information is related, the capacity of the investigation team and the importance of the original investigation, which may be thwarted by this new information.

According to our respondents, compared to twenty years ago, an increasing effort must be made to obtain the same results from a tap. Suspects are more and more aware that the police tap their telephones and that they must not communicate over the phone. The result of tapping depends strongly on a number of factors: the offence committed or to be committed; the target group to which the suspect belongs; how much of a stir or arousal is caused by the police in a group of involved people which stimulates communication; whether or not an analyst is involved in the investigation; the decrease in the use of speech telephony; and just coincidence as well.

Notification and destruction

In contrast to what the research results from 2004 show, in the public prosecutor's offices we have studied, tapped people were usually notified in 2011. Although the legal regulation is clear[217], each of these offices has its own interpretation of it. In one of the studied regions (region A), several respondents stated that notification has had a low priority for years, but that the Ministry of Justice exerts pressure for the regulation to be observed. At the moment, a catch-up effort is being made to notify people and to issue destruction orders to the police.

Respondents from another studied region (region B) indicated that the rules for notification are strictly observed. According to this employee of the Special Investigative Powers chamber, this region succeeds in being 'up-to-date' with notifications and is not behind. This is due to the fact that funds and time have been earmarked for notification and destruction. The smaller number of cases this region annually deals with probably also contributes to this.

217 Instruction on powers of investigation (2011A002), 14 February 2011, *Staatscourant* 2011, 3240.

In the studied regions, the notification is coordinated by the Special Investigative Powers Chamber. In region A, the arrangement is as follows: a year after the start of an investigation, the administration asks the public prosecutor involved about the state of affairs in that investigation, and whether a notification can be sent. In region B, the decision to notify is taken two months after an investigation has been closed, at the initiative of the Special Investigative Powers Chamber and in consultation with the public prosecutor. The majority of the respondents, both at the national and the regional level, considered the obligation to notify a nonsensical rule. The fear is that criminal investigation tactics will be up for grabs. Furthermore, respondents often had the impression that receiving a letter of notification raises more questions than it answers. Although the respondents all had a negative opinion about the obligation to notify, the notifications are actually carried out, however with low priority.

When someone wants to file a complaint about the letter of notification, approaching the Public Prosecution Service has no purpose. Tapped persons do not receive more detailed information in response to the letter they have received. In the letters of notification sent within the studied regions, no reference is made to a regulation or organization were the receiver can turn to with questions or complaints. Regarding the complaints procedure, there is room for improvement.

Beside the tapped person himself, who gets notified afterwards, there are more people who have communicated with the tapped person and whose privacy has thus been violated. Yet, these people are not notified. One respondent argued that the obligation to notify should be extended to people who have frequently been in contact with a 'tapped person'.

Two months after the letter of notification has been sent, the Public Prosecution Service must issue a destruction order to the police. This means that the police get the order to destroy all information collected by means of special powers of investigation. The interviews show that systematic destruction has only recently been taking place in region A. Only recently someone has been appointed within the police force to coordinate the destruction of records. Region B indicated that they have already been preparing the notification and destruction for a couple of years. By securing these matters in a standardized way at the front end, the actual destruction at the back end only takes a minute. In a standard way, in recent years a so-called 'zero file' has been added to all criminal files, in which all special powers of investigation used have been noted down; thanks to this method, it is not longer necessary to go through the entire file looking for the special powers of investigation used.

Destruction can be postponed for two reasons. When data obtained by recording telecommunication can be used for another criminal investigation, these data do not need to be destroyed until the other investigation has been ended. Furthermore, data may be retained when they relate to persons involved in serious crime in the way defined by the Police Registers Act.

Inquiry proved that both at the national public prosecutor's office and the district public prosecutor's offices information obtained by means of a tap is quite regularly stored on the basis of this Act.

Bottlenecks of tapping
Respondents mentioned the following bottlenecks and/or points for improvement regarding working with telephone and/or Internet taps: 1) the fact that criminals are very knowledgeable about the investigative techniques used by the police; 2) the fact that online telecommunication is often encrypted with specialized software, which makes it harder to tap; 3) the extensive administrative process involved in tapping. According to some of the respondents, the investigative methods used by the police are exposed too much to publicity. The result is that criminals bear in mind that covert means of investigation are used against them, and that they anticipate it. This puts the possibility of tapping communication in danger. Criminals search for alternative ways of communicating and for ways to evade a tap. It turns out, for example, that seasoned criminals make use of technological possibilities to encrypt their communication. The great majority of the observations made about bottlenecks with regard to tapping related to the bureaucracy and the mass of paperwork involved in submitting a request for a tap.

The Internet tap

The number of Internet taps installed annually during criminal investigations is very modest in comparison to the number of telephone taps used. Yet, Internet experts expect that the application of this investigative means will increase considerably. Respondents especially mentioned the increase in the number of Smartphones as an important motive for innovations regarding the Internet tap. As a result, several respondents expected that a tap on a Smartphone will, as a matter of course, be an Internet tap in the future. However, in practice this is not yet how things stand. The use of an Internet tap often takes place in response to information obtained by means of a telephone tap. Our interviewees indicated that they proceed to use an Internet tap when an 'ordinary' telephone tap on a Smartphone proves to yield too few results and the investigators feel they are missing part of the communication.
With regard to the use of the Internet tap, three groups of respondents can be distinguished. First, there is a group of respondents who until now have never used an Internet tap and do not feel they are missing it as a means of investigation, for instance because it does not fit in with the target group. Secondly, there is a group of respondents that uses the Internet tap regularly. These respondents were enthusiastic about its use. The third and largest group of respondents has had to deal with the Internet tap in the past, but

tries to avoid using the Internet tap as much as possible due to bad experiences. These bad experiences with the Internet tap have negatively influenced this group of respondents in their assessment of this means of investigation. Meanwhile, the software has greatly improved, certainly compared to some years ago, but according to several respondents there is more room for improvement. Beside the not too user-friendly applications, respondents also mentioned the extensive staff that is needed for elaborating the results, a lack of digital expertise within the teams and the large amount of data an Internet tap may yield. The interviews also show that there are no clear guidelines for elaborating and verbalizing the Internet tap, even though the respondents really need them. The police do not have enough knowledge of high-quality analytical techniques to search large amounts of data quickly and thoroughly, as an expert on Internet tapping told us. In addition, with an Internet tap it is not possible to choose beforehand which information should be intercepted and stored and which information should be kept out of the data stream. This possibility might make the Internet tap more focused and efficient. Such an improvement was also mentioned as an opportunity to make the violation of the tapped person's privacy less serious.

Professionals pledged to confidentiality and the Internet tap
In contrast to the situation regarding tapped telephonic communications with professionals pledged to confidentiality, there are no protocols or procedures for communications with professionals pledged to confidentiality intercepted by means of an Internet tap. Digital specialists are aware that this is a problem that will not be easily fixed.
Fundamental basics of the law prescribe that investigative services have to remove communication with professionals pledged to confidentiality from tapped data. However, this is unfeasible in case of an Internet tap. The amount of intercepted data can be gigantic. This makes a thorough search for confidential information time consuming and difficult. Besides that, it is not very logical to force investigators to thoroughly go through these data in order to find confidential information they are not alowed to see. Furthermore, the removal of bits of information from the intercepted data is technically difficult to achieve. At the moment, a lot of thought is given to the possibilities of filtering professionals pledged to confidentiality from Internet taps. At the ULI, protocols are being developed to make it possible to automatize scanning for professionals pledged to confidentiality.

Accessibility for taps
The rise of encryption makes it increasingly more difficult to intercept the content of online communication. Several respondents saw encryption as a tool used by people who have something to hide. However, improved security during Internet use is important for the security of people, their money and their property. To guarantee that criminal investigators will keep having

access to the content of communications via Internet, they are suggested to listen or look in before the encryption or screening-off takes place. A technique that makes this possible is to hack a computer or Smartphone from a distance. The Public Prosecution Service has recommended the Minister to study the possibilities of hacking computers.

Alternatives

Usually, several means of investigation are used during a criminal investigation. The choice of a particular means of investigation is determined by the kind of crime (requirement of proportionality), the available capacity, personal preference, knowledge and experience, the throughput time of the investigation, and administrative hurdles and procedures. Two teams – one at the national level and one in a studied region – are conducting criminal investigations without the (large-scale) use of taps. These respondents indicated that because taps can be used relatively easily, this may be of influence on the creativity with which investigators look for other ways to find out the investigative information they need. These teams, which are still in their infancy, are less focused on solving individual criminal cases than traditional investigation teams are. These teams make use of a more programmatic or thematic approach, and solving a criminal case has been subordinated to solving a more encompassing social problem, which may not just be dealt with by criminal law but also by means of preventive or administrative measures.

Beside taps, respondents make use of other covert means of investigation, yet in the Netherlands there is no really equivalent alternative to the tap. When other special means of investigation are used, tapping is often necessary to get the input needed to adequately deploy such an investigative power. Furthermore, the objectives of the use of these means of investigation are often different from those connected to taps, and the team also starts to use them in another investigative stage. However, the use of these special means of investigation may actually shorten the use of the tap. The telephone tap is a means of investigation with which investigators can come close to the suspect unseen. In particular when suspects are highly prepared for police attention, it is difficult to use certain other means of investigation because the risk of being discovered, and with it the risk of damaging the investigation, is very real. The choice to use the telephone tap is mainly inspired by the speed with which this means of investigation can be put into operation and by the fact that there is little risk to the use of a tap. Other special powers of investigation require time to prepare, with the risk that costly investigative information will get lost in the meantime. In addition, as we have said before, these methods have a greater risk of putting the investigation in jeopardy.

Since there are no alternatives to the telephone tap, the requirement of subsidiarity is in fact a formality, a legal requirement of which the outcome is a foregone conclusion.

Legislation and regulations in the compared countries

In this study, we have compared the way in which taps are used in the Netherlands to that of three other European countries: England and Wales, Sweden and Germany. Since the use of the tap constitutes an infringement on the right to privacy, a basic right guaranteed by the European Convention on Human Rights, the use of taps is couched in safeguards. Similar to the Dutch situation, in England and Wales, Sweden and Germany, the use of telephone and Internet taps has also acquired a legal base. We will now discuss in more detail some of the aspects laid down in these laws.
In the Netherlands, Germany and Sweden, the judicial review is the final piece of the authorization process that should lead to a tapping order. In this process, the public prosecutor always submits a request for the use of the telephone or Internet tap to the (examining) judge. In England and Wales, the public prosecutor has no part in the authorization process; the use of any telephone or Internet tap is authorized by the Secretary of State instead of the judge. For this reason, England and Wales seem not to meet the requirements of treaty law regarding the judicial review. Nevertheless, in the case of *Kennedy against the United Kingdom* (18 May 2010), the ECHR has decided that the British regulation is not at fault on this point.
Whether the use of a telephone or Internet tap is authorized, depends in all studied countries on the assessment of the seriousness of the crime – during which it is examined whether the infringement on privacy outweighs the seriousness of the offence to be investigated. Another relevant question is whether the information that may be uncovered by means of the tap is necessary for the investigation's progress and cannot be obtained in another way that constitutes less of a violation of a citizen's privacy (requirements of proportionality and subsidiarity). For which crimes the tap can be used is determined in a legal regulation in all studied countries. Although these regulations differ per country, the crimes involved are always serious. In addition, in all studied countries the tap can not only be used against suspects, but also against people who maintain a relation with the suspect in one way or another.
The maximum term during which a tapping order (and its possible extension) may be applied differs among the studied countries. In the Netherlands, the maximum term is four weeks, in Sweden it is a month. In England and Wales, a tap can be applied for a maximum of three months, the same as the maximum term in Germany. In Sweden and Germany, intercept may be used as evidence in a criminal case, similar to the Dutch situation. This is prohibi-

ted in England and Wales if the information has been obtained on the basis of an English tapping order. In 2008, however, a commission installed by the British government, the *Privy Council*, has come to the conclusion that information obtained through the use of a telephone or Internet tap should in principle be used as evidence in a criminal case. For the time being, this recommendation has not been adopted by the British government. If the intercept comes from abroad, for instance from the Netherlands, and it has been obtained legally according to Dutch standards, it may actually be admitted in an English court, to be used as evidence. In the context of further safeguards against the violation of privacy (for instance article 8 ECHR), a regulation has come into effect in the Netherlands, Germany and Sweden, which requires that a citizen who has been subjected to a telephone or Internet tap must be notified afterwards about the use of this covert means of investigation. Such a regulation does not exist in England and Wales. In response to a notification, a citizen can subsequently file a complaint about, for example, a possible violation of his or her privacy. Although a notification is obviously not a constitutive requirement for (possibly later on) filing a complaint, it can actually be instrumental to a citizen's legal protection. In Sweden, England and Wales, there are independent bodies for dealing with complaints. In addition, Sweden has the figure of the Public Ombudsman (*Offentliga Ombud*), whose task it is to watch over the rights and integrity interests of individuals in criminal investigations in general. This Ombudsman must also see to the protection of the integrity of third parties.

Use of the tap in compared countries

Statistics

The statistics of these countries are not easily comparable because of their different ways of administrating. The number of taps in Sweden, England and Wales, for instance, are registered on an individual level, while in the Netherlands and Germany, each tapped telephone number or extension number is counted. Furthermore, the periods to which the figures on tapping apply, are different for each compared country. Nevertheless, we can conclude from the statistics that in recent years an increase has taken place in the number of issued tapping orders in all countries under study (England and Wales, Sweden and Germany).

In England and Wales, the telephone tap is not used very frequently; the (modest) increase during the 2008-2010 period is attributed to an increase in the number of cases of serious crime and threats to the national security of the United Kingdom. In Sweden, too, taps are not frequently used in an absolute sense; a small number of big criminal investigations strongly influences the annual figures. The increase in the number of tapping orders in Sweden during the 1999-2008 period has been steady, while it was even very substan-

tial in 2009 – with an increase of 67 per cent compared to the previous year. Yet, the average duration of taps, measured in days, decreased in 2009 with 34 per cent in comparison to the year before. The increase in the number of taps is explained by the use of this means in the national campaign against serious organized crime, which started in 2009. This resulted in a rise in the number of criminal investigations in which telecommunication was tapped. Although the reported figures show that the Germans make less use of taps than the Dutch do, the German situation is comparable to that of the Netherlands. The number of tapping orders for landlines issued during the 1998-2007 period shows a modest increase. During the same period, the number of issued tapping orders pertaining to mobile phones, however, increased exponentially. An explanation for the strong increase in issued tapping orders for mobile phones for the 1998-2007 period may be the exponential growth of the use of mobile phones in recent years. This can be observed in more detail in the group of tapped persons, who frequently change their telephone cards or mobile phones. The figures with regard to Internet taps of the countries under study are unknown.

The use of traffic data (subscriber data included) also shows an increase for all compared countries. In England and Wales, for example, there has been a limited growth (of about 5 per cent) of the number of requests for access to traffic data during the 2008-2010 period. In Sweden, the number of authorizations issued for intercepting traffic data has increased in 2009 with 47 per cent in comparison to 2008; yet, the average number of days during which traffic data were intercepted has decreased in 2009 with 35 per cent compared to the previous year. The growth of the interception of traffic data is closely related to the increase in the number of authorizations issued for tapping telecommunication. In Germany, the number of requests submitted for permission to use subscriber data has increased exponentially during the 2001-2010 period. This seems to be related to the rise in the use of mobile phones and the increase in the number of tapping orders for mobile phones, or to the interception of traffic data. Although for the time being there are no specific and current figures on this, the use of traffic data (subscriber data included) seems to grow in importance for the German practice of criminal investigation.

Where the Dutch chiefly make use of telephone taps as a covert means of investigation, the figures on England and Wales for the 2006-2010 period make clear that police investigators make more use of *Covert Human Intelligence Sources* (CHIS) than of telephone or Internet taps. This ratio is different in Sweden, since approximately 75 per cent of all issued authorizations related to covert means of investigation pertained to telephone or Internet taps. This means that no less than 25 per cent of all authorizations in 2009 per-

tained to other covert investigation methods. We have not found any figures on Germany with regard to this point.

Use in practice

In the fight against and investigation of serious and organized crime, in all the countries we studied the use of telephone and Internet taps and of traffic data is well-thought-of. In England and Wales, often the first means of investigation is to ask for traffic data, enabling investigators to get an impression of (the behaviour of) the person involved before a telephone or Internet tap is used. In Germany, too, asking for access to traffic data proves to be a means of investigation all by itself. Furthermore, the combined use of the telephone tap and other means of investigation, such as informers and/or monitoring equipment, turns out to be a productive method in all compared countries. Because people suspected of serious and/or organized crime divulge little about their doings and dealing related to their (assumed) criminal activities over the phone, investigation services use other means of investigation in addition to the telephone tap. Moreover, the tapping of telecommunication has excess value where gathering information as the basis for further investigation is concerned. In England and Wales, this is the logical consequence of the fact that intercepts are (usually) not allowed in court to be used as evidence. It seems that in Germany, intercepts are often not used in court as direct evidence, either. The reason is that the reliability and/or completeness of intercepts are quite regularly questioned in court. In those countries in which intercepts actually can be used as evidence, our respondents pointed out that writing a report about it is a time-consuming task.