1216-2574 / USD 20.00

ACTA JURIDICA HUNGARICA
47, No. 2, pp. 183–197 (2006)

CSABA FENYVESI*

The Legal and Criminalistic Aspects of Secret Data and Information Collection

1. The typology of secret data and information collection

Bearing in mind current national, European and global crime rates as well as the globalizing tendencies of organized crime, we can state for certain that the traditional, open methods of investigation are not efficient for successful criminal prosecution. Against conspired criminal networks working with wide-scale distribution of work, using significant human and material resources, one can step up successfully only with secret methods of covering, and an extensive spectrum of human and technical devices. The detailed criminal tactical and criminal technical methodology of these devices and strategies is defined by criminalistics. Criminal procedure law provides the legal framework.

Act XIX of 1998 on Criminal Procedures (hereinafter the Criminal Procedures Law, CPL), form-fitted to Rule of Law requirements, includes the regulations for secret data and information collection. This is a novelty in Hungary, as there had been no such directions in the criminal procedure codes. The investigating authorities used to act on the basis of secret, internal commands even though their operation affected fundamental rights. The breakthrough came with Act X of the year 1990 (already annulled by Act CXXV of 1995), which–at the dawn of the political transition–was the first to regulate secret service operations. This was followed by Act XXXIV of 1994 on the Police, Act C of 1995 on Customs law, customs procedures, and customs administration, Act CXXV of 1995 on National Security Services, and Act XXXII of 1997, on the Border Guard Services, and finally the recent modification of the law on prosecutor's office, which gave a detailed authorization for secret information collection,. (Altogether, at present there are four agencies performing investiga-

* Dr. univ., Ph.D. Associate Professor, Pécs University Law School Criminal Procedure Department, H–7622 Pécs, 48-as tér 1.
e-mail: fenyvesi@ajk.pte.hu

tive tasks, including the prosecutor's office, five secret services, and the interior investigation division of the police–all entitled to collect secret information.)

Nowadays, two methods can be distinguished in a well-confined manner, namely:

- secret collection of information (memo-technically SECOLLINF), and
- secret obtainment of data (memo-technically SEOBTDAT).

Their differences can be summed up in the following table:

The taxonomic distribution of secret means and methods		
Secret collection of information		Secret obtainment of data
Requiring an authorisation from a judge or the Minister of Justice	No judicial warrant required	Requiring a court order
Can last until the investigation is ordered	Before and after the investigation is ordered (even during the investigation!)	Only after the investigation is ordered, until showing the documents
– secret search and technical recording of private apartments – surveillance and recording of private apartments – getting acquainted with and recording mail (K-check) – getting acquainted with and technically recording long-distance communications – getting acquainted with and applying the data of Internet or other computer correspondence	– the use of an informer, undercover operation (+ prosecutor's permit to person cooperating) – information collection by scouting or undercover investigator (+ prosecutor's permission) – checking data – issuing a cover document or establishing a cover organisation – surveillance of persons, premises, buildings, other objects, land and vehicles, as well as recording sound and picture – application of traps – sample shopping – infiltration into conspiracy networks	– technical surveillance of private apartments – mail – telecommunication data – data forwarded by means of computer systems

	– controlled shipping – victim role play by a policeman – establishment of information systems – tapping in addition to the cases which require a permission, recording of data discovered with technical devices – collection of information from communication devices and other data storage devices which require an official permit (+prosecutor's permission)	

First, let us review those specific secret data collection (SEOBTDAT) activities which belong under the auspices of the CPL [*a)-b)-c)* of Paragraph (1) of Section 200]. This means the following:

a) surveillance and recording of events taking place in private apartments by means of technical devices,

b) getting acquainted with the contents of letters, other postal matters, as well as communications forwarded by means of telephone cable or other communication systems, and the recording of these by means of technical devices,

c) getting acquainted with and applying data forwarded and stored by computer systems.

In the first category, the investigating authority surveys and records the events taking place in the private apartment by means of video(cameras) and listening devices ("bugs", "sound guns") secretly installed in the interior space, or used from the outside. In the second category, the "blocking" of communi-cation devices takes place, which includes the "tapping" of faxes, telegrams, and all kinds of telephones (hard wire, mobile, etc.), the–to use an old phrase–ferreting out and recording of data which will be used as evidence later. Finally, the third group contains the secret checking and disclosure of computer data, e-mails, internet data, and connections.

As they affect basic human rights (e.g. the privacy of residence or private secrets), they can only be applied with a number of restrictions, such as:

a) the existence of general basic requirements,

b) for a specific goal,

c) in relation of special crimes and special circumstances,

d) against particular individuals,
e) within time constraints,
f) according to strict formal requirements, with a judicial warrant.

Ad a) The application of SEOBTDAT has three general, basic requirements:
- necessity (there are sufficient grounds to assume that the obtainment of the evidence is hopeless in another way)
- proportionality
- the likeliness of the result.

The conditions are conjunctive: all of them need to exist for the application. If either one is absent, the secret means cannot be applied. Naturally, this only comes up at the point of approving the motion. because afterwards–provided that it was successful–it cannot be debated, the absence of any of these does not exclude or make the evidence obtained unlawful.

Ad b) Unlike the means, the aims are not very special, we could say they are general. It is not difficult to satisfy this restriction as we can list the same aims even in the case of open investigative acts;
- the establishment of the identity of the perpetrator,
- the establishment of the place of residence of the perpetrator,
- arresting the perpetrator,
- uncovering means of evidence.

Ad c) Secret devices can be applied only in relation to special (deliberate) criminal acts which pose an outstanding danger to society, or have special material or personal conditions. It is fair that the law [Paragraph (1) of Section 201] lists these;

The crimes or the attempt or the preparation for such crimes need to be
- *deliberate and to be punished with imprisonment of five years or more, furthermore*
- *related to crime spreading across the country borders,*
- *against a minor,*
- *committed serially or is performed through organised commission (including habitual commission, in conspiracy or criminal organisation as well),*
- *related to drugs or materials constituting drugs,*
- *related to forging banknotes or securities or*
- *committed while being armed.*

Ad d) The secret device cannot be applied against anybody, it can be used only in relation of a defined circle. The target person, as the criminalistics term goes, is constituted by the following:

- primarily the suspect (the comprehensive term "accused" cannot be applied here as the secret device can exist exclusively in the investigative phase of the criminal procedure)
- against the potential suspect (the person who can be suspected of the commission of the criminal act according to the data of the investigation so far but he has not been informed of this yet; that is, it can be applied in the event of the existence of the simple personal suspicion),
- it is possible against others as well, if there is information pertaining any criminal relationship with individuals of the previous two categories, or there are grounds to assume such a relationship (simple suspicion is enough for this, too).

Among "other individuals" it is a further order of limitation that the above-listed secret means can only be applied against a lawyer acting as defense counsel if there is well-founded suspicion of a criminal act against the counsel in connection with the case. This restriction–absolutely correctly–extends to the private residence, office, all the telephone lines, communication devices, postal and electronic correspondence, as well as all the mail of the attorney. Another restrictive institution that is meant to protect the client-attorney privacy is that this restriction extends to the consulting rooms of the police detention facilities and the penitentiary institutions (including the houses of correction).

As a marginal note, we would like to add that it is not necessary to use secret means in the consulting rooms of the police detention facilities which are separated with a glass-plexi wall, as the defense counsel and the accused usually need to almost shout with each other, but at least are forced to talk loudly, thus–violating thereby the defense's secret and intimacy–this can be heard within ear's reach.[1]

In connection with the tapping of the defense counsels' telephone lines, in the 1998 case of Kopp vs Switzerland the European Court of Human Rights (hereinafter ECHR).established the violation of Article 8 as the Swiss authorities violated the right to privacy and family life when they wiretapped the applicant's conversations in the attorney's office. (Bírósági Határozatok, hereinafter BH 1998/12. 955–957).

[1] For more see more in Fenyvesi, Cs.: *A védőügyvéd* (The Defense Counsel). Budapest–Pécs, 2002.

Ad e) The secret obtainment of data can only take place during the course of the investigation: it begins with the ordering of the investigation, and ends with the introduction of the documents of the investigation. Within this timeframe it can last for 90 days, with one extension for a maximum period of 180 days. With the exception of unpostponable cases (*periculum in mora*), a notice ordering investigation is needed, without which the motion for order cannot be formally accepted. In establishing the time of the introduction of the documents, it is the introduction of the documents to the first accused (if there are more than one) that is to be taken into consideration; it is the point until which the secret obtainment of data can be performed. If secret means had been used before the investigation was ordered, that could be performed lawfully only within the framework of secret collection of information (SECOLLINF). If, in the meanwhile, the investigation is ordered, the secret collection of information is kind of transformed, and only secret obtainment of data (SEOBTDAT) can be carried out according to the CPL [Paragraphs (3)–(4) of Section 200].

Ad f) The most important formal requirement is that the secret data collection can be authorised by the court, more precisely the investigator judge, upon the prosecutor's motion. In his motion, the prosecutor, as the master of the investigation (*dominus litis*) has to detail the following:

- the name of the prosecutorial body, the investigating authority,
- the date the investigation was ordered,
- the number of the case,
- if there is or has been secret information collection,, who performed it, what data has been obtained,
- the place of the planned performance of secret data collection, in the case of telephone tapping, the telephone number (either hard wire or mobile),
- the name and identification particulars of the person affected (the target person),
- the name of the means and methods,
- the starting and ending date of the planned period, with the hour and day indicated,
- the existence of the restricting conditions detailed under points *a)–b)–c)–d)–e)*,
- in case of an unpostponable (emergency) order, its reason and time,
- the documents providing grounds for the motion attached,
- upon a motion for extension the documents emerging since the earlier authorisation.

The investigating judge makes a decision about the motion within 72 hours. She/he may reject, fully or partially approve it. In case the motion is approved the judge defines what kind of secret means and methods can be used, against whom, between what time constraints [Paragraph (4) of Section 203].

In unpostponable (emergency) cases, not only the judge but also the prosecutor may order secret data collection for a period of 72 hours, however, the motion for authorisation is also to be put forward at the same time. If the court turns it down, there is no room for unpostponable order on the grounds of unchanged factual basis, and–as referred to earlier in connection with legal remedies–there lies no appeal.

If we take a look at the six restrictions listed above, we can see that apart from the first two (*a–b)* posing general specifications, the violation of the other four points *(c–d–e–f)* all make the data obtained thus unlawful (excluding it from the chain of evidence), thus they fall into the category of excluded evidence. We can conclude this, even though the law will not declare this expressis verbis in all cases.

2. The execution of secret obtainment of data, getting acquainted with and using its results

Secret data collection itself is carried out by the police and the special sub-units of the national security services, with whom–in ways specified in separate legal regulations–the telecommunication, postal, computer network service providers are obliged to cooperate with.

The prosecutor and the head of the investigating authority have several obligations in connection with secret data collection. On the one hand, he/she has to terminate secret data collection without delay if [Paragraph (3) of Section 204]

a) in the event of unpostponable order, the court rejected the motion,
b) it has fulfilled its objective determined in the permission or warrant,
c) the period of time determined in the permission or has lapsed,
d) the investigation has been terminated,
e) it is obvious that no result can be expected from its further application.

With respect to these, the law enumerates excluded evidence only in case of points *a)* and *e)*–in Paragraph (4) of Section 206–however, our opinion is that the unlawfulness prevails within the circle of all the obligations described here and below.

The same individuals also have an obligation to eliminate all data that has not importance for the goal, and data recorded in connection with individuals who are not involved in the case. An additional requirement in connection with the secret data obtained subsequently, not permitted by the judge, in an unpostponable manner, is that they are to be destroyed not within 8 days but without delay [Paragraph (4) of Section 204]. All these also belong to the category of excluded evidence.

Third, they have continuous data protection and confidentiality obligations, according to the regulations of the state secret and service secret law. Upon the request of the investigating judge authorizing secret obtainment of data, the prosecutor is obligated to present the data obtained so far. As a control of legality, she/he examines its application and should it be established that the terms of the permission have been transgressed, she/he may terminate it–with a final and binding resolution–and in the case of other violation law, may terminate the secret data collection [Paragraph (3) of Section 205].

Fourth, it is the obligation of the prosecutor to notify all parties affected by the secret data collection provided that no criminal procedure has been initiated against them and it would not endanger the success of the criminal procedure. The notification is to be made only if both conditions are satisfied. The measure often contested in the literature is a constitutional state requirement, while we can definitely expect that the person notified about the tapping of his phone will fear using the telephone all his life even though he might have only been "affected" by the case without committing or even planning anything unlawful. Thus we consider the application of the legal requirements acceptable only with very serious restrictions.

It is already the fifth obligation that the head of the prosecutorial or investigating authority is to draw up a signed report of the execution of the secret obtainment of data, which contains

- its progress,
- what means and methods were applied, for how long and where,
- who was affected by it,
- the place and time of the source of the data not destroyed
- the fact of the achievement of the goal, or the reason in case of its absence[Paragraph (5) of Section 204].

The report is unconditionally necessary for the prosecutor if she/he endeavors to use the result of secret data collection as documentary evidence in the open criminal procedure. Otherwise, it can be made evidence only if it cannot be replaced by anything else. In this case, by its application, the state secret nature of the data ceases, except if the data is a state secret regardless of the manner of

obtainment. In this case, the cancellation permission of the master of the state secret is also required.

The permission is to be attached to the documents of the investigation together with the motion for permission and the resolution of the court granting permission (the three documents) [Paragraphs (1)–(2) of Section 206].

Data obtained during the course of secret data collection, before ordering the investigation can also be made into chain of evidence if the master of the secret cancels the state secret classification and if it meets the general requirements listed under points *a–f*, and if the purpose of use is the same as the original goal of secret obtainment of data or secret collection of information [Paragraph (4) of Section 206].

Finally, here is a table about the comparison of (the execution) of secret collection of information requiring a permit (SECOLLINF) and secret data obtainment (SEOBTDAT) activity.

Secret collection of information		
	Secret collection of information (SECOLLINF)	**Secret obtainment of data** (SEOBTDAT)
Legal basis	− Police Act (XXXIV of year 1994) − State Security Services Act (CXXV of 1995) − Border Guard Act (XXXII of 1997) − Customs Law (C of − 1995) − Act on the public prosecutor (V of 1972)	CPL
Party ordering	Judge and Minister of Justice	Court (investigating judge)
Time of application	− before the investigation is ordered	− after the investigation is ordered − during the investigation − until the introduction of documents
Period of time of application	90 days that can be extended by 90 days	
Method, means	− secret search and technical recording of private residence − the surveillance and recording of a private residence	− the technical surveillance of a private residence − gathering and recording mail, telecommunication

	– mail (K-check) – gathering and digitally recording telecommunication messages – gathering and using the data of Internet or other computer technical correspondence	data, and data forwarded by computer systems
range of criminal acts	– Police Law Points a)-j) of Paragraph (3) and Paragraph (4) of Section 69 – National security interest as well	CPL Points a)-g) of Paragraph (1) of Section 201
Against whom (target person)	"potential accused"	the accused and persons in criminal relationship with the accused
General condition	Hopeless in other ways (necessary)	
		+ proportional (would propose disproportional difficulty in another way) + the result is rendered probable
Termination	Police Law Paragraph (1) of Section 73	CPL Paragraph (3) of Section 204
	the achievement of the goal the expiration of the deadline no result can be expected subsequently, the judge did not allow emergency	
	+ is unlawful for some reason	+ the investigation was terminated
Destruction of data	data without interest for the goal, and data recorded in connection with individuals not involved in the case	
Use as evidence	inclusion into report document and attachment to investigation documents	
Subsequent notification of the party affected	None	the prosecutor notifies the affected parties if no criminal procedure was launched against and is not endangering the success of the procedure

3. Secret collection of information not requiring a judge's permission

As mentioned above, to prevent, uncover, and interrupt criminal activity, to establish the identity of the perpetrator, to locate wanted criminals, to establish

their place of residence, and to obtain evidence, the police–within the constraints of Act XXXIV of 1994 on the police–can collect secret data.

During the criminal procedure, the data obtained during the course of secret information collection–which is possible–as well as the identity of the person cooperating with the police, the mere fact and technical details of information collection constitute a secret until used as means of evidence.

The aim of the application of the secret criminal-technical means is also criminal data collection, or we could say, criminal intelligence service. In a wider sense, criminal intelligence service is the information collection activity carried out under cover, in a hidden manner (conspiring), of an offensive nature, within the framework of means and methods defined by law.

In a narrower sense, criminal intelligence service is the integration of official police personnel in criminally significant positions, projects, areas, and regard to people in order to obtain data necessary for the investigation).

The types of secret information collection not requiring a judicial warrant:

a) the police may employ an informer or a fiduciary person,

b) may collect information undercover,

c) to cover the cooperating person, as well as to cover under cover operations can issue and use a cover document, can establish and maintain a cover business,

d) can survey persons who can be suspected of the commission of the criminal act as well as persons in relation with the above (so-called target persons), as well as the premises, buildings, and other projects, section of land or road, vehicles, events that can be associated with the criminal act, can collect information about it, and can record the findings with technical devices suitable for the recording of sound, picture, other signs or traces,

e) in order to uncover the perpetrator of a criminal act or in the interest of proving, is allowed to apply a trap–that does not cause damage or harm to one's health–can perform sample or fake or purchasing, may carry out controlled shipment, and can engage in victim role-play by a policeman,

f) may establish information systems,

g) apart from the cases requiring a permission, they can tap and record the findings with technical means (e.g. conversation in a park),

h) may collect information from telecommunication systems requiring official permissions and other data storage facilities.

The police can conclude secret cooperation agreements with natural persons or legal entities occurring in the above enumeration, as well as organisations

without a legal entity (in practise, most often with the informer), and can give material remuneration–even in foreign currency.

At the expense of its own budget the police can establish and maintain cover businesses indicated under point *c)* according to the legal regulations with respect to business entities or private enterprises..

A special combination of secret service devices is the so-called undercover agent and his activity. Due to its existence and human nature, it is considered a criminal tactical device rather, at the same time, as he is planning to uncover a criminal act as a flagrant *delict*, thus setting a "trap" to the real perpetrator, she/he is also in the role of an "*agent provocateur*". Nowadays, the provocateur is used mostly the fight against drug crimes. The reason the provocateur is needed in these cases is that drug-related criminal acts typically do not have a victim, there is no accuser at the police, no party filing a complaint. Thus the undercover agents pose as buyers, uncovering the drug dealers with test purchases.

Notwithstanding its use in criminalistics use, we would like to mention the theoretical, ethical and possible criminal law liability misgivings in connection with the provocateur. As we have pointed out earlier–in these cases the police practically sets a trap for the target person(s). They create a situation in which the target person thinks that the provocateur is an accomplice, that is the situation is, so to say, "ideal" for the commission of the crime. The classical example of the provocateur is the undercover policewoman who poses as a prostitute in the street, or an police officer posing as a drug dealer.

The main ethical problem in connection with the provocateur is posed by the possibility that the provocateur might even get the target person to commit a criminal act that he would not have committed by himself. In this case, the investigation did not uncover but create a criminal act, as the provocateur is able to directly influence the target person. The correct attitude is that the police should establish the situation favourable for the commission of the criminal act, but the decision needs to be made by the target person independently, without the influence of the provocateur.

4. Secret information collection requiring a judicial warrant

Secret information collection requiring a judicial warrant may have the following types:

a) searching a private residence in secret (secret house search), recording the findings by technical means,
b) surveying and recording the events taking place in a private residence with technical means,
c) reading letters, other mail, as well as the contents of communication forwarded by means of telephone wire or a telecommunication, and recording it that by means of technical devices (e.g. telephone tapping).

The police can use these special (so-called operative) means only during the persecution of crimes of outstanding dangerousness. If they
a) can be associated with international crime,
b) are aimed against an child,
c) are realized serially or by organized commission,
d) are related to drugs or materials constituting drugs,
e) are related to forging money or securities,
f) are realized by armed commission,
g) are of terrorist nature,
h) seriously disturb public safety.

5. Particular secret criminal technical devices for information collection

The different secret tapping, surveillance and search activities are carried out by the investigating authorities with special criminal technical devices as listed in the appendix of 135/1997. Government Decree 135/1997 (VII. 29.)
They are the following:
a) tapping devices;
b) secret visual surveillance devices;
c) secret entry devices;
d) other criminal technical devices.

ad a) Any electronic, mechanical or other device, method, "technology", or software can be a tapping device if used to access secret information without the knowledge of those taking part in the communication, provided that they possess one of the following features:

aa) It have been designed, or produced for the secret tapping, forwarding, or recording of direct speech, or or equipments that can be used for such purposes without significant transformation. Thus especially

- wall (contact) microphones and stethoscopes provided with electronic amplifiers
- tapping systems using laser or infra red radiation, or based on ultra sound principle,
- miniature transmitters that can be built in or may be remote controlled, and their special receivers,
- small-size transmitters built into different hiding devices or that can be hidden under clothing, the receivers and sound recording devices,
- miniature sound-recording devices with a recording capacity of over 10 hours,
- high-sensitivity parabola- and gun microphones,
- sub-miniature electret microphones and acoustic probes.

ab) Equipment that has been designed or produced for secret gathering, forwarding, or recording of data stored on digital or analogue information facilities and/or processing computers, computer or other devices, or information carriers used with them, or or equipments that can be used for such purposes without significant transformation.

ac) Equipment that has been designed or produced for secret tapping of telecommunication systems forwarding hard-line and/or wireless speech and non-speech information or equipments that can be used for such purposes without significant transformation..

ad b) Any optical, mechanical, electronic and other device or accessory, as well as a software operating these can be a secret visual surveillance devices, provided that it possesses one of the following features:

ba) Equipment that have been designed or produced for secret surveillance or recording , or for the forwarding and processing of the information obtained thereby, or equipments that can be used for such purposes without significant transformation. Thus especially:

- small-sized, high resolution and sensitivity CCD cameras and accessories,
- miniature cameras and accessories that can be hidden into hiding devices or under clothing,
- video sign forwarding devices operating in micro-wave range, and their receivers,
- video sign forwarding devices using the electric network, and their receivers,
- fibrescopes with small entry openings, and systems using glass fibre optics enabling secret surveillance, and adapters enabling connection to cameras or video cameras.

bb) Equipments that operate under restricted light conditions (i.e. do not require secondary lighting) and contain special photo-multiplying tubes or optical elements. Especially light-enhancing devices that can be used for night photography and video recording .

bc) Special night vision devices operating in infra red range.

ad c) Secret entry devices are mechanical, electronic, optical and software devices that have been produced for the purpose of secretly entering closed premises (enclosed area of land, building, vehicle, etc.), provided that they possess one of the following features:

– devices, "technologies" and accessories that aredesigned and produced for the replacement of the proper opening device of locks, padlocks, bolts, etc. operating on the basis of mechanical, electronic or other principles, for destructive and destruction-free opening,

– devices and software that is developed to penetrate electronic security systems.

ad d) Other secret service devices include:

da) coding or crypting devices,

db) communication systems that can be hidden under clothing, equipped with a wireless ear piece,

dc) miniature transmitters and special receivers that can be used for positioning.

In our opinion, the latter may have a play a significant role in combatting car thefts with the use of the so-called "beeper".[2]

The head of the investigating authority terminates the use of the special devices promptly if the its objective has been accomplished, if the time frame within the court order has been transgressed, if no result can be expected from its further application, or if the application ordered through preliminary emergency procedures was not authorised by the judicial authorities.

From all secret service expenses, probably, the largest amount is spent on Costs may reach, 15–20 billion EUR annually, primarily paid by the USA and Great Britain. It was revealed in 1999 that an American tapping system under the cover name "Echelon" was able to survey every civilian satellite, every under-sea cable, as well as Internet mail and sound communication. The American secret

[2] For more see more Gremela, Z.: A titkos információgyűjtésről (About the secret collection of information). *Rendészeti Szemle,* 1993. No. 3.

service got as far as “convincing” the largest software manufacturers, Microsoft, Lotus, and Netscape to harmonize their export Internet products with American regulations. Namely, only to use coding that can be decoded and tapped without any particular effort.

As a closing idea

It is clear both from the above-described criminal procedural legal framework, and from the criminalistics arsenal–and within that, criminal-technical and tactical means–that the possibilities for secret data collection are given for professionals. From this point on the only question is who is going to operate them and with what efficiency.