COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

REVIEW REPORT

on

the processing of telecommunications data
by GISS and DISS

CTIVD NO. 38

[5 FEBRUARY 2014]

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 38

REVIEW REPORT

on the processing of telecommunications data by GISS and DISS

Table of Contents

REVIEW COMMITTEE
for
THE INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 38

DEFINITIONS

For the purpose of the public review report on the processing of telecommunications data by GISS and DISS

The following list contains definitions of a number of terms as used in this review report and in the legal appendix. It was not the Committee´s aim to make the descriptions exhaustive, but rather tried to give readers a concrete idea of the terms included in the list.

Acquiring department	The department at (GISS) or (DISS) which, when a special power is deployed, is involved in acquiring the data – by technical means or otherwise. This is not the same department as the one that conducts the operational investigation in the context of which a special power is deployed. At GISS these are the operational teams, at DISS the operational bureaus.
Agent	A person specifically deployed by the services to collect data. Agents operate under the control and the supervision of the services.
Analogue data stream	Data transmitted from one system to another system using a non-digital connection. An analogue stream contains telephone and telefax traffic not transmitted via the internet.
Application	A computer programme (software) that can be used to perform a specific task (e.g. Microsoft Word, which can be used for text processing). The services utilise applications for tasks like making accessible and analysing data.
Approval	Permission to exercise a special power (e.g. the services require the minister´s approval for telephone tapping).
Bulk data	Large volumes of raw data.
Bureau head (DISS)	An officer at DISS positioned in the organisation's hierarchy as follows: director, department head, *bureau head*, section head.
Cablebound communication	Communication via a cable (e.g. fibre optic or copper cables).
Central Information Point for Telecommunications (Dutch abbrev.: CIOT)	A government agency handling authorised access for investigative, intelligence and security services to certain user data, specified by law, in the possession of telecom and internet providers (e.g. name, address, city, number of a user and the type of service to which he subscribes).
Communications intelligence (comint)	Sigint data relating to content and metadata of communications between parties.

Communication session	The communication between two or more users at a given moment (e.g. a (satellite) telephone conversation).
Compartmentation	Putting into practice the need-to-know principle of article 35 ISS Act 2002 in the sense that GISS or DISS ensure that within the organisation information is only disclosed to employees in so far as this is necessary for the proper performance of the tasks assigned to the employees in question.
Computerised device or system	A computerised device or system used for recording, processing and transmitting data by electronic means (e.g. a computer, a computer network, a mobile phone or a server).
Cyber	All things relating to the digital or virtual world, including the Internet.
Data mining	The structured searching of large collections of data.
Data processing	Collecting, recording, arranging, storing, updating, altering, demanding access to, consulting or using data, providing data by forwarding, dissemination or any other means of making data available, assembling or combining data, and protecting, deleting or destroying data (article 1(f) ISS Act 2002).
Data stream	Data moving from one system to another by means of a connection.
Department head (DISS)	Officer at DISS positioned in the organisation's hierarchy as follows: director, *department head,* bureau head, section head.
Digital data stream	Data moving from one system to another by means of an Internet connection. A digital stream comprises telephone traffic, telefax traffic and other Internet traffic.
Director (GISS)	Officer at GISS positioned in the organisation's hierarchy as follows: head, *director*, unit head, team head.
Director (DISS)	Officer in charge of DISS. At DISS, the director is positioned in the organisation's hierarchy as follows: *director*, department head, bureau head, section head.
E-mail account	E-mail means electronic mail traffic. A user of e-mail uses an account for sending and receiving e-mail messages. An e-mail account is obtained by applying to an Internet Service Provider (e.g. KPN) or another provider of e-mail services (e.g. Hotmail or Gmail).
Electronic intelligence (elint)	Sigint data from electronic signals (radar).
Ether	The space through which electromagnetic waves travel. This investigation concerns satellite signals and radio waves travelling through the ether.
Evaluated data	Data obtained by the exercise of special powers, which has been assessed for relevance.
FoIP	'Fax over Internet Protocol'. Used for sending fax messages via the Internet Protocol.
Hacking	Gaining access to a computerised device or system with the

	aim of retrieving or modifying data.
Head (GISS)	Officer who is in charge of GISS. The head occupies the following position in the organisational hierarchy at GISS: *head*, director, unit head, team head.
IMEI number	The unique number by which a mobile phone can be identified.
Informer	A person or body who/which the services can approach to collect data. An informer is not controlled by the service and provides information on the basis of his/its usual activities.
Intelligence service	A service that conducts investigations regarding other countries for the purpose of identifying (potential) threats to the service's own national security.
Intelligence task	Investigating other countries (see article 6(2)(d) and article 7(2)(e) of the ISS Act 2002).
Interception	The interception of data.
Internet Protocol (IP)	A system allowing computer networks to communicate with each other (e.g. the Hypertext Transfer Protocol (http) controls communications between a web browser (programme for viewing Internet pages) and an Internet page).
IP address	Every individual computer which communicates with other computers via IP has a unique address, the IP address. The IP address identifies the connection of the computer to the Internet, similar to a telephone number.
Lead	A characteristic (e.g. a telephone number) that is used for deploying the power to search for the purpose of untargeted interception (article 26 ISS Act 2002).
Making accessible	Making data accessible or searchable.
Metadata	Data about a communication session. The metadata of a telephone call, for example, comprises the telephone numbers involved, the starting and ending times of the call and the data of the mobile phone masts involved.
Metadata analysis	The process of looking for relevant links and data in a collection of metadata and of combining data already available (what/who has made contact with what/whom, for how long, how often, from where, etc.).
National Sigint Organisation (NSO)	An organisation run by GISS and DISS jointly which is responsible for the technical aspects of intercepting non-cablebound communications.
Network analysis	Identifying , combining and finding links between data relating to persons and organisations in order to gain insight into relationships between them, for example by providing insight (e.g. based on a technical characteristic) into the contacts of a target with other persons and subsequently into the contacts of the latter with yet other persons.

Non-cablebound communication	Communication taking place via wireless connections, namely through the ether (e.g. satellite links).
Operational process	Combining data that has been acquired with other data (already available), following which the data is analysed for the purpose of preparing reports which may, if required, be provided to the responsible authorities.
Personal data	Data relating to an identifiable or identified individual natural person (e.g. a name or a photograph).
Procedure	A service´s written policy and/or the procedure followed in practice.
Raw data	Data obtained by the use of special powers which have *not yet* been assessed for relevance.
Searching	Exploring non-cablebound communications originating from or destined for other countries, in particular HF radio traffic and satellite communications.
Section head (DISS)	Officer at DISS who occupies the following position in the organisational hierarchy at DISS: director, department head, bureau head, *section head*.
Signals intelligence (sigint)	Intelligence collected from intercepted electronic signals.
Special power	A power conferred on a service by law to use a specific means that infringes privacy, which provision of law also lays down the circumstances and conditions under which the power may be exercised. Special powers are usually exercised in secret. The special powers are set out in articles 20 - 30 of the Act on the Intelligence and Security Services of 2002 (e.g. tapping and surveillance).
Stored telecommunications data	Telecommunications data stored in a computerised device or system (e.g. a computer, a mobile phone or a server).
Streaming data /transmission phase	Communication being transmitted from sender to receiver. Such communication is in the *transmission* phase. Streaming data can, among other things, be intercepted using a tap.
Symbolon	A project of GISS and DISS to prepare for setting up a joint Sigint Cyber unit. This new unit has by now been established under the name of Joint Sigint Cyber Unit.
Targeted interception	Interception where the person, organisation or technical characteristic at whom/which the data collection is targeted can be specified in advance.
Team head (GISS)	Officer at GISS who occupies the following position in the organisational hierarchy at GISS: head, director, unit head, *team head*.
Technical characteristics	Characteristics that can be traced to various telecommunication elements, for example a telephone number, an IMEI number or an IP address.
Telecommunication	Communication at a distance by electronic means (e.g. telephone, radio, telefax or the Internet).

Telecom provider	Provider of public telecommunications networks and public telecommunications services (e.g. KPN or Vodafone).
Telephone traffic data	Telephone traffic data is traffic data relating to telephony (see explanation of traffic data).
Unit head (GISS)	Officer at GISS who occupies the following position in the organisational hierarchy at GISS: head, director, *unit head*, team head.
Untargeted interception	Interception where the person, organisation or technical characteristic at whom/which the data collection is targeted cannot be specified in advance.
User data	Also called subscription data. These are name, address, city and number of a user and the type of service.
Security Service	A service that investigates persons and organisations who or which may constitute a danger to the continued existence of the democratic legal system, or to the security or other vital interests of the state, or to the security and the readiness of the armed forces.
Security task	Task aimed at identifying dangers to the continued existence of the democratic legal order (article 6(2)(a) ISS Act 2002), or to the security or other vital interests of the state, or to the security and the readiness of the armed forces (article 7(2)(c) ISS Act 2002).
Traffic data	Data relating to a user (user data, e.g. name, address, city, number), to the persons or organisations with whom or which the user is or was connected or tried to make a connection, or who or which tried to make a connection with the user (name, address, city, telephone number), data relating to the connection itself (metadata, e.g. starting time, ending time, terminal equipment location data, terminal equipment numbers), and data relating to the subscription (the type of service the user is using or has used, the data of the party paying the bill) (article 28 ISS Act 2002).
VoIP	'Voice over IP', also called IP telephony, which means making telephone calls via the Internet Protocol.
Web forum	Digital public discussion pages on the Internet. Some forums require visitors to register to obtain access to the site. Usually, visitors can also exchange messages via these sites.

The report in a nutshell

In reaction to the revelations about the NSA, the Dutch parliament asked the Committee in July 2013 to investigate the activities of GISS and DISS. In this report the Committee intends to respond to the questions entertained in parliament and the media about the way in which the Dutch services acquire and use collections of (personal) telecommunications data and exchange them with foreign services. These activities can be brought together under the wider header of 'data processing', in this case particularly in the field of telecommunications, meaning all electronic forms of communication at a distance: telephone, telefax, radio and the Internet.

On the basis of its investigation the Committee formed the following general picture. Over the past few years GISS and DISS have increasingly started working with collections of (personal) data. This is due to the new technical possibilities and the digitalisation of society. The Committee observes that both services take the ISS Act 2002 as the guiding principle for both the acquisition of data and the exchange of data with foreign services. They have, however, been using existing powers in ways that were not always foreseen when the law was developed. It is the opinion of the Committee that in certain areas some of the procedures followed by the services do not adequately guarantee the protection of privacy. In some cases these procedures were unlawful under the ISS Act 2002, for example because of the failure to state reasons and/or the absence of permission at the required level. The Committee has established that there are a number of close cooperation relationships in which GISS and DISS exchange collections of (raw) data. They do so while trusting that foreign services respect human rights and act within the parameters of their own legal frameworks. It is the opinion of the Committee that in the light of recent revelations it is advisable to assess whether this trust is still justified. In this context the Committee also recommends that the ministers concerned assess the cooperation relationships (also in international groups) for transparency, and set out the considerations underlying the cooperation in more concrete terms.

The report deals with the nature of the procedures followed by GISS and DISS for the aforementioned forms of data processing. These are complex matters, which is true of both the systems to be discussed and the legal assessment framework. To assist readers in understanding the findings, the report contains a list of definitions explaining a number of the terms used. The legal appendix to this report outlines the broader legal framework within which data processing should take place on the basis of the ISS Act 2002, the Constitution and the ECHR. In addition, the report has two secret appendices, one concerning GISS and one concerning DISS. In the present report the Committee reviews whether the procedures followed by the services are lawful. Specific cases will be assessed in other review reports of the Committee, for example in the report on GISS' investigative activities on social media which will be completed in April 2014.

Since the Committee focused its investigation on the various forms of telecommunications data processing, the report is structured on the basis of these forms and follows the system and terminology of the ISS Act 2002. At the same time, however, the Committee did bear in mind the original questions submitted to the Committee by parliament. It is by reference to these questions that the main findings of the investigation are set out immediately below.

1. Is it possible to give an assessment of the nature and scope of the activities of the Dutch intelligence services in the fields of (a) large-scale data collection (particularly data fishing), (b) combining data, (c) data storage and (d) exchanging data?

There are various methods used by GISS and DISS to acquire telecommunications data.
One method which can definitely be regarded as being large-scale is the untargeted interception of non-cablebound telecommunications (signals intelligence, or sigint). The method is used to intercept many communication sessions with the corresponding metadata from the ether. After gathering such a data collection, the services perform metadata analysis, which means that the services analyse the metadata and combine it with data already in their possession. In addition, the services explore the available data to examine which other communication sessions are relevant. After obtaining permission from the minister concerned, they examine the content for possible use in the operational process (selection). Another method is to gain access to computerised devices or systems (hacking) in order to acquire stored telecommunications data, for example data from e-mail accounts or web forums. The services also deploy human sources to acquire telecommunications data. Other methods for data acquisition mentioned in the report, namely telephone and Internet taps, and demanding access to telephony traffic data and user data from telecom providers, are not used by the services for large-scale data acquisition.

The telecommunications data acquired by the services using these methods, both content and metadata, are intended for use in the intelligence process. The services combine the data with other data, and after characterising and analysing them the services prepare reports which they can provide to the responsible authorities if necessary.
For this purpose the acquired data are first stored on servers and made accessible using application software. The services search for relevant information in the acquired data, which is still raw data at that stage, and subsequently process and analyse the information (which is then called evaluated data). In most cases the remaining raw data is retained for some time. The services utilise various analysis applications for combining and analysing data. Within the organisation, access to raw data is in most cases restricted to employees who are involved in the investigation for the purpose of which the data was acquired. Exceptions to this rule are the applications utilised by GISS for metadata analysis and the application utilised by GISS to make data from web forums accessible. These applications are accessible to a wider circle of employees.

Cooperation of GISS and DISS with foreign services can take the form of providing and receiving (personal) data and of providing support, e.g. by exercising a special power at the request of a partner service. Within close cooperation relationships the partners may make structural arrangements. This happens in regard to issues for which a joint approach is considered necessary, for example in connection with the fight against terrorism or military operations abroad. In certain close cooperation relationships between GISS and DISS and foreign services the partners exchange collections of (raw) data, on a structural basis and otherwise.

2. How much scope does the Intelligence and Security Services Act 2002 (ISS Act 2002) leave for each of the four separate activities mentioned in the first question? Can the Committee say whether and in which cases the activities are not carried out lawfully within the parameters of the ISS Act 2002 or only party so? Specifically, what is the relation between articles 24-27 and article 59 of the ISS Act 2002?

The Committee has established that the methods used by GISS and DISS for collecting telecommunications data fall within the scope of the powers conferred by the ISS Act 2002 on

the services. There is no question of GISS and DISS systematically acquiring collections of (personal) data in disregard of the law.

The Committee has established, however, that nowadays technological developments make it possible to use existing powers in new ways not always foreseen by the legislator. A related factor is that far greater volumes of telecommunications data are available due to the digitalisation of society and the associated intensification of communications. Indeed the potential infringement of privacy by the services' use of these methods goes much further than was possible in 2002. As a result there are a number of areas in which the procedures followed by the services currently do not sufficiently guarantee the protection of privacy, though strictly speaking they do not overstep the boundaries of the ISS Act 2002.

For example, when the services analyse metadata acquired by untargeted interception, they fail to state reasons why the analysis satisfies the requirements of necessity, proportionality and subsidiarity, while the procedure does not include any other safeguards either. The Committee recommends that rules on metadata processing be included in the ISS Act 2002. In addition, the Committee points out that GISS must pay more attention to safeguarding the right to privacy when it uses and retains web forums which it has acquired in their entirety.

In addition to the above, the Committee has come across procedures which it considers unlawful under the ISS Act 2002. For example, when the services deploy human sources there are certain situations in which they fail to state adequate reasons and to obtain permission at the required level for the specific activities. When using the power of hacking, the services in certain situations failed to apply for internal permission at the required level. Moreover, as the Committee already established in earlier reports, the practice of searching after interception of sigint is partly contrary to the ISS Act 2002, while insufficient reasons are stated for the selection of sigint itself.

The ISS Act 2002 grants GISS and DISS broad powers to cooperate with foreign services. While the ISS Act 2002 was being drafted no express consideration was given to procedures for handling the exchange of collections of (raw) personal data. The Committee has established that under the ISS Act 2002 GISS and DISS are authorised to exchange such data collections and that in practice they actually do so in the context of various cooperation relations. The Committee holds that where the services provided collections of data, both metadata and communication content, within the cooperation relationships it investigated they did so lawfully. In addition to providing data, GISS and DISS may provide support if foreign services so request, including support by exercising the powers laid down in articles 24-27 ISS Act 2002. They must do so, however, subject to the requirements set by the Act on the exercise of these special powers. When the Committee investigated the exchange of data collections in a number of cooperation relationships it came across one unlawful procedure. It has established that DISS used the power of selection on behalf of foreign services without obtaining permission to do so from the minister, which is unlawful.

3. To what extent is each of the four separate activities mentioned in the first question compatible with the Dutch Constitution and with the Convention for the Protection of Human Rights and the Fundamental Freedoms (ECHR)?

The safeguards provided by article 8 ECHR, the case law of the ECtHR and articles 10 and 13 of the Dutch Constitution have been incorporated in the ISS Act 2002. This was based on the principle that the processing of personal data by the services infringes the privacy of the persons concerned to a greater or lesser extent and that a balance must be struck between the

extent of the infringement and its purpose, viz. the protection of national security. In order to ensure that such a balance will always be struck, the legislator included a number of structural safeguards in the ISS Act 2002, such as a limitative list of the tasks of the services and the corresponding intelligence means, the requirements of necessity, proportionality and subsidiarity that must be satisfied before the services may use a special power, and the requirement of permission, either internal or at ministerial level, for such use, as well as the general requirements applying to the processing of (personal) data including the requirements of necessity, propriety and due care.

The Committee will include these safeguards from the ECHR and the Dutch Constitution in its considerations when reviewing the procedures followed by GISS and DISS, as described in its answer to question 2, against the ISS Act 2002.

4. What are the rules governing the assessment for proportionality and subsidiarity – as required by the ECHR – when the services acquire data relating to Dutch nationals from foreign services?

GISS and DISS may happen to acquire (personal) data relating to Dutch nationals as a result of the fact that a foreign service provides the data or through the fact that a foreign service provides support, for example by exercising a special power in behalf of GISS or DISS. When foreign services provide data or support, they practically always do so in response to a request from GISS or DISS. It is the responsibility of the foreign service providing the data or the support to assess whether the provision of the data or support satisfies the requirements of necessity, proportionality and subsidiarity. In their capacity as receivers of the data or support GISS and DISS play a more limited role in the matter. Before making a request for specific data or support, however, GISS and DISS must assess to what extent the desired provision of data or support will satisfy the requirements of necessity, proportionality and subsidiarity. GISS and DISS are not permitted to request a foreign service to exercise a power which the Dutch services may not exercise themselves (sidestepping legal restrictions). Moreover, the services must refrain from using data received from foreign services if there are concrete indications that the data was acquired in a manner which by Dutch criteria constitutes unlawful infringement of privacy or of another fundamental or human right. Finally, it should be noted that no separate assessment is made with regard to Dutch nationals, since the ISS Act 2002, the Constitution and the ECHR do not make a distinction by nationality.

In the above, the Committee has outlined its findings in response to the questions submitted to it by parliament. The Committee is aware, however, that these conclusions still do not give clear answers to a number of important questions being asked in society about the activities of the Dutch services. In the following paragraphs the Committee will therefore briefly discuss a number of these questions.

The answer to the question whether GISS and DISS are involved in the large-scale collection of telecommunications data must be split into two parts. With respect to non-cablebound communications the answer is 'yes'. In fact, the law permits the services to do this (article 27(1) ISS Act 2002) and provides for the necessary safeguards with regard to processing the data thus acquired by untargeted interception (article 27, paragraphs 3-10, ISS Act 2002). With respect to cablebound communications the answer is 'no' as far as it concerns streaming communication, meaning communication that is in transit from sender to receiver. Under the ISS Act 202 the services are not authorised to acquire streaming communications data. The Committee has established that GISS and DISS do not practice untargeted

interception of cablebound telecommunications. They do, however, acquire stored (not streaming, therefore) telecommunications data, in particular by using human sources or by exercising the power to hack, and they may thus acquire collections of (personal) data. The Committee uses the term 'untargeted' if it is not possible to state in advance at which person, organisation or technical characteristic the acquisition of data is targeted. Based on this definition, the acquisition of collections of (personal) data by human sources might in certain cases be considered untargeted. The Committee emphasizes that this does not mean that the tasks assigned to the services should not constitute reason to acquire the data. The Committee has not found any indication that the services are exceeding the boundaries of their statutory tasks when they acquire telecommunications data using human sources.

The question whether GISS and DISS have used telecommunications data in violation of Dutch law when cooperating with foreign services cannot be answered by a simple 'yes' or 'no'. Foreign services with which GISS and DISS are cooperating may have more or different powers than the Dutch services. Receiving data is not unlawful unless the Dutch services know or may be assumed to know that the data was collected by the foreign service in a manner constituting unlawful infringement of privacy (or another fundamental right). This would be unacceptable, because it would impair the protection of fundamental rights which the State of the Netherlands has undertaken to protect under international conventions. However, when intelligence and security services cooperate, even when they do so in a close cooperation relation, it is not customary practice to share knowledge of how data has been collected. In the close cooperation relationships investigated by the Committee, GISS and DISS generally trust that the foreign services respect human rights and act within the parameters of their own national laws and regulations, unless they have evidence to the contrary. The recent revelations can be considered to be such evidence and make it desirable to verify whether the trust is still justified. In this connection the Committee also recommends that the ministers concerned reassess the cooperation relationships (also in international groups) for transparency and set out the considerations underlying the cooperation in more concrete terms.

The Committee has not found any evidence in the course of its investigation that GISS and DISS, by way of sidestepping legal restrictions, requested foreign services to collect data by a method they are not themselves permitted to use. The Committee did come across the situation that some foreign services with which the Dutch services cooperate are permitted by their national laws to perform untargeted interception of cablebound communications. For those services, this method is falls under the term sigint. The Dutch services are not permitted to do this. The Committee has established that when GISS and DISS receive sigint from those foreign services, which happens with some regularity, they thus receive data that may include data obtained by untargeted interception of cablebound communications. The Committee takes the position that untargeted interception of cablebound telecommunications does not in itself already constitute unlawful infringement of privacy or of another fundamental or human right. The fact is that the ISS Act 2002 confers a similar power on GISS and DISS in regard to non-cablebound telecommunications. When the ISS Act 2002 was drafted, no explicit constitutional considerations were devoted to the difference between cablebound and non-cablebound telecommunication. Neither can it be said beforehand that cablebound interception, if provided with adequate safeguards, is in itself contrary to the ECHR or other human rights conventions. In this context the Committee considers it permissible for GISS and DISS to cooperate with these foreign services, even if it cannot be excluded that they may receive data obtained by untargeted interception of cablebound telecommunications.

Another frequent question is whether GISS and DISS have in any way cooperated in the collection of telecommunications data in violation of Dutch law. What people have in mind here is allowing foreign services to tap telephone or Internet traffic in the Netherlands. The ISS Act 2002 only permits foreign services to engage in activities within the territory of the Netherlands if the minister responsible has given them permission to do so and provided they do so under the supervision and responsibility of GISS or DISS. The Committee has found no indications that foreign services gained independent access to Dutch telephone or Internet connections with the cooperation of GISS or DISS.

Finally, the Committee points out that it is (structurally) investigating or will start investigating a number of themes discussed in this review report. In the course of these investigations the Committee not only reviews procedures but also concrete cases. The Committee refers to its ongoing in-depth and follow-up investigations of the exercise by GISS of the power to tap and the power to select sigint (the report covering the period September 2012 through August 2013 is expected to be completed in early April 2014); of GISS' investigative activities on social media (expected to be completed in May 2014) and of the cooperation of GISS with foreign services (expected to be completed in August 2014). In the first quarter of 2014 the Committee will also start a (continuous) follow-up investigation of the use of sigint by DISS.

1 Introduction

Starting in June 2013 disclosures started appearing bit by bit in the world press about the practices of the American National Security Agency (NSA) based on information leaked by Edward Snowden, a former employee of this service. The first item to attract attention was the PRISM surveillance programme. According to the leaked documents and interviews with Snowden this programme was aimed at acquiring or searching the chat sessions, e-mails, photos and videos stored on the servers of large Internet companies such as Microsoft, Yahoo, Google, Facebook, Skype and YouTube.

In the course of the month of June several questions were raised in the Dutch media about the involvement of the General Intelligence and Security Service (GISS) and the Military Intelligence and Security Service (DISS) (further also referred to jointly as: the services) in, briefly stated, the collection and exchange with the US of bulk data relating to Internet traffic and telecommunications. This led to parliamentary questions in early June, particularly about the Symbolon and Argo II projects and the possibility that GISS and DISS were tapping the Internet hub Amsterdam Internet Exchange (AMS-IX).[1] On 21 June 2013 the minister of the Interior and Kingdom Relations wrote a letter to parliament explaining how the statutory powers of the Dutch intelligence and security services relate to the powers deployed in the PRISM programme or similar information gathering methods.[2] The minister stated in this letter that GISS and DISS did not use the PRISM software. He further explained that the services themselves did not have unhampered, unrestricted access to Internet traffic and mobile telephone traffic, and not via foreign intelligence and/or security services (further referred to as: foreign services) either. With regard to cooperation with foreign services the minister explained that GISS and DISS were not permitted to request other countries to engage in activities not permitted under the Dutch Intelligence and Security Services Act 2002 (ISS Act 2002), while noting that in international cooperation between services it was not customary practice to share knowledge of how data has been acquired.

On 26 June 2013 parliament held an experts hearing on the collection and storage of personal data by Dutch and foreign services. On the same day there was a non-public hearing of employees of the services.

Originally, a General Consultation had been placed on the agenda a week later, on 4 July, in reaction to the reporting on PRISM. Eventually, the General Consultation was cancelled and it was decided at the agenda-setting meeting of 4 July to send the Review Committee for the Intelligence and Security Services (further referred to as: the Committee) a request pursuant to article 78(2) ISS Act 2002 to conduct an investigation into the collection of data by GISS and DISS, accompanied by a number of research questions.[3] The Committee received the request on 23 July 2013. The following research questions were submitted to the Committee:

1. Is it possible to give an assessment of the nature and scope of the activities of the Dutch intelligence services in the fields of (a) large-scale data collection (particularly data fishing), (b) combining data, (c) data storage and (d) exchanging data?

2. How much scope does the Intelligence and Security Services Act 2002 (ISS Act 2002) leave for the each of the four separate activities mentioned in the first question? Can the Committee indicate whether, and in which cases the activities are not carried out lawfully within the

[1] *Annex to Proceedings II* 2012/13, no. 2649.
[2] *Parliamentary Papers II* 2012/13, 30 977, no. 56.
[3] *Parliamentary Papers II* 2012/13, 30 977, no. 57.

parameters of the ISS Act 2002 or only partly so? Specifically, what is the relationship between articles 24-27 and article 59 of the ISS Act 2002?

3. To what extent is each of the four separate activities mentioned in the first question compatible with the Dutch Constitution and the Convention for the Protection of Human Rights and the Fundamental Freedoms (ECHR)?

4. What are the rules governing the assessment for proportionality and subsidiarity – as required by the ECHR – when the services acquire data relating to Dutch nationals via foreign services?

After receiving this request the Committee considered how it should arrange its investigation in order to provide the best possible answers to the questions that had arisen (in society) within an acceptable period of time. It decided to aim the investigation at data processing by GISS and DISS, because for the purpose of the ISS Act 2002 the term data processing includes any action or any set of actions relating to data. Consequently, the term includes collecting, recording, storing, combining and providing data (article 1(f) ISS Act 2002). The Committee decided to focus its attention on the processing of telecommunications data. The term 'telecommunication' literally means transmitting information over distance and in addition to old methods such as telegraphy and flag-signalling which are obviously irrelevant to this investigation, it includes all electronic forms of distance communication: telephone, telefax, radio, Internet.

Within this general field of telecommunications data processing by GISS and DISS and in line with the request from parliament, the Committee selected four subjects which this report will in any case address:

1. The scope of the general and special powers of the services to process telecommunications data, considered among other things in relation to the Constitution and the ECHR.

2. The way in which the services use the different types of data files and the rules applying to such use.

3. The possibilities for and restrictions on the exchange of data with foreign intelligence and/or security services.

4. The way in which the criteria for review laid down in the ECHR – necessity, proportionality and subsidiarity – play a role in data processing by the services, in particular in the exchange of data with foreign intelligence and/or security services.

On 5 August 2013 the Committee announced its investigation to the ministers of the Interior and Kingdom Relations and of Defence and to the presidents of both chambers of parliament.

In the period after the investigation was announced the stream of media coverage of the activities of the NSA continued, which from August 2013 included reports on the tapping by the NSA of various foreign or international organisations and officials.[4] On 13 September the cabinet issued its reaction to the disclosures in the media, referring among other things to the

[4] 'US eavesdropping on United Nations', Dutch News Agency *ANP* 25 August 2013; 'NSA spies on French ministry', *ANP* 1 September 2013; 'Brazil furious with US about espionage', *Volkskrant* 13 September 2013; 'NSA spied on India embassy', *ANP* 25 September 2013; 'German criticizes digital occupation force', *NRC Handelsblad* 30 October 2013; 'NSA also eavesdropped on the Pope', 30 October 2013, www.nos.nl; 'NSA also monitored Ban Ki-Moon', 2 November 2013, www.nu.nl.

investigation being conducted by the Committee and the various consultations at EU level with the American government with a view to gaining a mutual understanding of each other's intelligence programmes and the statutory basis for and oversight of the programmes.[5]

On 16 October the cabinet's reaction was discussed at a General Consultation with the minister of the Interior and Kingdom Relations. The central topic at this meeting was whether a reaction to the reports on espionage by the United States should be given at EU level, or whether the Netherlands should do so in a bilateral context. Joining the German initiative to arrange an anti-espionage agreement was mentioned as an option for a reaction from the Netherlands. The minister promised that he would explore a bilateral solution after receiving the results of the fact-finding process undertaken by the EU-US expert group established on the initiative of the European Commission. The General Consultation also devoted attention to the meaning of the term metadata analysis. The minister explained that metadata analysis essentially means that the telephone numbers of known terrorists are compared with the bulk of metadata to see what information this delivers. It may happen that a person who has not yet attracted the service's attention turns up in the same circle as the known terrorists. The minister further explained that in the Netherlands this is only permitted with respect to non-cablebound communication, which virtually always concerns foreign contacts. He added that the Dessens Committee was considering the question to what extent this technology-dependent approach should be maintained.[6]

On 21 October the debate in the Netherlands took a new turn when a message was posted on the web site Tweakers.net that in December 2012 alone the NSA was believed to have collected the metadata of 1.8 million Dutch telephone calls. On 28 October, following a request on the initiative of D66, this message led to a written reaction from the minister of the Interior and Kingdom Relations.[7] In this reaction the minister stated that in view of American legislation – including the Foreign Intelligence Surveillance Act (FISA) – the government was aware of the possibility that the NSA might intercept telephone communications. He stated that in the context of investigations relating to terrorists and other threats to national security or in the context of military operations the government considered the interception and analysis of metadata in itself an acceptable method. However, when another country believes that there are sound reasons to gather intelligence in or from the Netherlands, it must first submit a request to GISS or DISS so that it can be assessed whether the intended action falls within the parameters of Dutch law, so the minister said in his reaction. The minister further said that the Dutch intelligence and security services were conducting talks with the NSA in order to reach a bilateral solution. He stated that the Netherlands took a positive view of the initiative of Germany and France [Committee: to bring about an anti-espionage agreement with the US] and would make an active contribution where possible.

In a broadcast of TV programme *Nieuwsuur* on 30 October the minister of the Interior and Kingdom Relations said that he had received a communication from the NSA stating that the metadata of the millions of monitored calls in Europe mentioned in the media had indeed been collected. According to the minister this was an implied confirmation that the numbers mentioned – 1.8 million in December 2012 as far as the Netherlands was concerned – were correct. The minister said in the broadcast that in any case it was not GISS that had provided

[5] *Parliamentary Papers II* 2012/13, 30 977, no. 61.
[6] *Parliamentary Papers II* 2012/13, 30 977, no. 71.
[7] *Parliamentary Papers II* 2012/13, 30 977, no. 63.

this data to the NSA. He further said that he deemed it unacceptable that partners working shoulder to shoulder in combating terrorism are at the same time eavesdropping on each other.

Critical questions continued to be asked in the media about the role of GISS in the activities of the NSA in regard to the Netherlands. On 30 and 31 October there were several reports to the effect, in brief, that GISS was in some way or other cooperating in the NSA's gathering of Dutch metadata.[8] These reports were based on a screenshot published by the Spanish newspaper *El Mundo* of a document on the cooperation of the NSA with several foreign services.

On 31 October the government issued a written reaction to two motions proposed in parliament[9] on what action the government was taking in response to the media reports on the NSA.[10] In its letter the government informed parliament that the Netherlands was on the one hand seeking a bilateral solution in talks with the NSA and would on the other hand contribute where possible to the French-German initiative for an anti-espionage agreement with the United States. In reaction to the motion to request clarification as to who was being tapped and to share the information on this issue with parliament, the government stated that it was discussing the issue with the United States and would – confidentially if necessary – inform the Second Chamber of the results.

International cooperation relationships between intelligence and security services aroused further interest after an article was published in *The Guardian* on 1 November 2013 about the cooperation between the British Government Communications Headquarters (GCHQ) and a number of European intelligence and security services.[11] The article reported that in addition to GCHQ itself, the German, French, Spanish and Swedish services had also developed methods for the mass surveillance of Internet and telephone traffic. With respect to the Dutch services the article said that in 2008 GCHQ had advised GISS and DISS about legal obstacles they encountered when processing Internet traffic.

An article in the Dutch daily paper *Volkskrant* on 4 November wrote among other things about the cooperation of the NSA with foreign services in the so-called *five eyes* cooperation group, in which five Anglo-Saxon countries were said to participate, and the broader *nine eyes* group which, in addition to the Anglo-Saxon countries, was said to include France, the Netherlands, Denmark and Norway. There were also rumours of a *14 eyes* cooperation group and a cooperation group of NATO member states. This article was reason for parliament to ask the minister of the Interior and Kingdom Relations for a reaction. In his reaction dated 5 November the minister stated that GISS and DISS were cooperating with foreign services within the scope allowed by the law. The minister also repeated what he had already said in his letter to parliament of 21 June: that GISS and DISS may not make requests to foreign services which are not permitted under Dutch law.[12] He further said that he could not make

---

[8] 'GISS may have cooperated in intercepting metadata of 1.8 million telephone calls', 30 October 2013, www.tweakers.net; 'GISS cooperating with NSA', *NRC Handelsblad* 30 October 2013, www.nrc.nl; 'GISS may have helped NSA in tapping 1.8 million telephone calls', *Volkskrant* 30 October 2013; 'GISS allows tapping by NSA', *Algemeen Dagblad* 31 October 2013.

[9] *Parliamentary Papers II* 2013/14, 21 501-20, no. 812 and no. 813.

[10] *Parliamentary Papers II* 2013/14, 30 977, no. 64.

[11] 'GCHQ and European spy agencies worked together on mass surveillance', *The Guardian* 1 November 2013.

[12] *Parliamentary Papers II* 2012/13, 30 977, no. 56.

any public statements about specific cooperation relationships or operations of GISS and DISS.[13]

On 6 November there was another General Consultation with the minister of the Interior and Kingdom Relations, specifically about the reports on the NSA. The SP member of parliament Van Raak said that he was no longer convinced that GISS and DISS were mere spectators. He put forward three reasons for this: (1) the secret tendering of the Argo II programme, which he believed to be intended for analysing data which could only have been gathered in the way the Americans and the English were doing this; (2) he had the impression that GISS and DISS had received data from the Americans and the English which must have raised the question: how can they obtain this kind of data? (3) the report that the Netherlands belonged to the *nine eyes* cooperation group. The doubts which the Socialist Party (SP) said it entertained about the role of GISS and DISS were shared in broad outline by the GreenLeft party (GL), the Democrats 66 (D66) and the Christian Democrats party (CDA); these parties likewise wanted to know whether the Dutch services had in any way assisted the NSA in acquiring Dutch metadata. In regard to the issue of metadata the minister explained that technically speaking it is only possible to gather metadata if one has physical access to the telephone exchange. If the United States possessed the metadata of 1.8 million Dutch telephone calls, these must therefore have been calls between the Netherlands and the United States or between the Netherlands and another country.[14]

Another subject discussed at the General Consultation of the Standing Parliamentary Committee on the Interior and Kingdom Relations of 6 November 2013 was the Committee's present investigation. MP Schouw (D66) said he found a remarkable difference between the request that parliament had made to the Committee and the investigation announced by the Committee. His point was that the Committee used the term 'data processing' instead of the term 'data gathering' or 'data collection' and the word 'possibilities' instead of the word 'facts' in connection with the cooperation with foreign services. At the close of the General Consultation it was decided that the minister would bring these matters to the attention of the Committee. Initially this was done by telephone and subsequently also in a letter to the head of GISS. In the telephone conversation which the Committee had with the clerk of the Standing Parliamentary Committee on the Interior and Kingdom Relations following the General Consultation, the Committee told him that pursuant to article 1 ISS Act 2002 'data processing' is a broad term which also covers 'data gathering' and furthermore that the Committee was also investigating the procedure followed by GISS and DISS for exchanging telecommunications data with foreign services.

Likewise on 6 November it became known that a coalition of journalists, lawyers and interest groups had instituted proceedings against the minister of the Interior and Kingdom Relations in order to ensure that GISS would stop using data obtained by the NSA in violation of Dutch law.[15]

On 30 November *NRC Handelsblad* published an article based on a leaked NSA document, which reportedly showed that GISS and DISS were hacking web forums. The article quoted a

---

[13] *Parliamentary Papers II* 2012/13, 30 977, no. 65.

[14] *Parliamentary Papers II* 2013/14, 30 977, no. 75.

[15] '*Burgers dagen Nederlandse staat voor samenwerking met NSA*' (Citizens sue Dutch State about cooperation with NSA), *Elsevier* 6 November 2013; '*De staat moet met feiten komen over afluisteren*' (The government must come up with facts about eavesdropping), *NRC Handelsblad* 7 November 2013.

number of experts, who cast doubts on the lawfulness of such hacking.[16] On the same day GISS released a statement to the effect that the investigation of jihadist web sites was conducted within the parameters of the ISS Act 2002.[17] On 18 December, moreover, the service heads of GISS and DISS organised a 'technical briefing' for the Standing Parliamentary Committee on the Interior. At this public meeting the two service heads gave a presentation on the subject of the processing of telecommunications data and answered questions from the Parliamentary Committee.

In a broadcast of TV programme *Nieuwsuur* on 13 January 2014 it was reported that the American ministry of Defence had its own equipment at the town of Burum (Friesland Province). Burum houses the satellite dishes of the Netherlands Sigint Organisation (NSO), which are used to intercept satellite traffic on behalf of GISS and DISS. On a site adjoining the NSO, so it was reported, the Americans had equipment for the interception of satellite data on the site of the international company Inmarsat. In reply to parliamentary questions about these reports the ministers of the Interior and Kingdom Relations and of Defence informed parliament that GISS and DISS did not possess any evidence that foreign powers were deploying intelligence activities at Burum.[18]

On 4 February 2014 the ministers of the Interior and Kingdom Relations and of Defence informed parliament by letter that the 1.8 million metadata records had not been gathered by the Americans but by the NSO. The data were said to have been gathered in accordance with the performance of the statutory tasks for the purpose of combating terrorism and of military operations abroad, and to have been lawfully shared with the United States in the light of international cooperation on these issues. In response to questions from the press the spokesman for the minister of the Interior and Kingdom Relations emphasised that the metadata did not relate to mobile phone calls, but to radio traffic and satellite telephone calls.[19] The minister of Defence said that the metadata emphatically did not relate to telephone traffic between Dutch citizens.

It will be clear from the above that what started as the "PRISM affair" has gained many new aspects since the announcement of the Committee's investigation on 5 August 2013. At the time of writing this review report and based on media reports, the Committee distinguishes two categories of concern that emerge from the media and that are felt in parliament regarding the activities of the Dutch intelligence and security services: (1) GISS and DISS are themselves engaging in large-scale and untargeted interception of Internet and telephone traffic; (2) GISS and DISS are cooperating (closely) with the NSA and possibly also with other foreign services and in this context (a) have made use of telecommunications data gathered in violation of Dutch law and/or (b) cooperated in some way or other in gathering telecommunications data in violation of Dutch law.

Within the framework of its investigation as announced, the Committee has tried to clarify and answer as fully as possible the questions raised in society about the activities of GISS

---

[16] '*AIVD hackt internetfora, tegen wet in*' [GISS is hacking Internet forums, against the law], *NRC Handelsblad* 30 November 2013.

[17] '*Verdachte webfora zijn legitiem doelwit*' [Suspect web forums are legitimate target], 30 November 2013, www.aivd.nl.

[18] *Appendix to the Proceedings II* 2013/14, no. 1084.

[19] '*Nederland verzamelde zelf telefoondata*' [The Netherlands gathered telephone data itself] and '*Ook coalitie kritisch op Plasterk over afluisteren*' [coalition also critical of Plasterk about eavesdropping], 5 February 2014, www.nu.nl.

and DISS. For the investigation of cooperation with foreign services the Committee had to choose between either focusing specifically on the cooperation of GISS and DISS with the NSA, or devoting attention, from a wider perspective, to the exchange of collections of data in the context of close cooperation relationships between the Dutch services and foreign services. The Committee chose the latter option because it believed that focusing exclusively on the NSA would be taking too narrow a perspective. It is only by first describing how GISS and GISS cooperate on a structural basis with their cooperation partners that the Committee can properly answer the questions submitted by parliament to the Committee about the exercise of privacy-infringing powers on behalf of international cooperation partners – exercised both by and for the Dutch services – and about the exchange of big data with international partners.

Some subjects discussed in this review report give cause for further in-depth investigation. The Committee points out that it has already for some time been conducting in-depth and follow-up investigations of the use of the power to tap and the power to select sigint (signals intelligence) by GISS (a continuous investigation),[20] the investigative activities of GISS on social media,[21] the cooperation of DISS with foreign services[22] and the cooperation of GISS with foreign services[23]. The Committee also intends to start a (continuous) follow-up investigation of the use of sigint by DISS.

Part of the questions submitted by parliament to the Committee are questions of a legal nature, namely the questions about the scope allowed by the ISS Act 2002 for certain activities of the services, about the relationship between articles 24-27 and article 59 of the ISS Act 2002 and about the extent to which certain activities of the services are lawful pursuant to the standards laid down in the Dutch Constitution and the European Convention on Human Rights (ECHR). These questions are answered in the legal appendix to this review report which sets out a detailed legal framework for data processing by GISS and DISS.

This review report has a secret appendix concerning GISS and a secret appendix concerning DISS. In these secret appendices some of the subjects addressed in the review report are discussed in greater detail. They also deal with several subjects that cannot be discussed in the review report because of their state-secret nature. The Committee has not established any unlawful actions in respect of these subjects. The Committee has, however, made recommendations in the secret appendices regarding three subjects not mentioned in the review report. Three of these recommendations concern procedures at GISS and two (related) recommendations concern a procedure at DISS.

The Committee completed its investigation in November 2013 and adopted the draft review report on 18 December 2013. In conformity with article 79 ISS Act 2002 the ministers of the Interior and Kingdom Relations and of Defence were given the opportunity to react to the findings set out in the review report. The Committee received the reactions of the ministers of the Interior and Kingdom Relations and of Defence on 14 January 2014 and 15 January

[20] The investigation covering the period September 2012 through August 2013 was announced to the presidents of the two Chambers of the States-General by letter of 17 September 2012. The review report resulting from this investigation is expected to be presented to the minister in early April, in conformity with article 79(2) ISS Act 2002.

[21] Announced by letter of 2 October 2013 to the presidents of the two Chambers of the States-General. The review report resulting from this investigation is expected to be presented to the minister in early April, in conformity with article 79(2) ISS Act 2002.

[22] Announced by letter of 27 October 2007 to the presidents of the two Chambers of the States-General.

[23] Announced by letter of 27 March 2013 to the presidents of the two Chambers of the States-General.

2014, respectively. As a result of these reactions some modifications were made in the review report, the legal appendix and the secret appendices, following which the review report was adopted on 5 February 2014.

2 The Committee's investigation

With a view to the nature of the questions submitted to the Committee and the time allowed for the investigation, the Committee has chosen to aim this investigation at mapping out the procedures[24] followed by the services when processing telecommunications data and at describing to what extent these procedures are consistent with the ISS Act 2002. In this context the Committee also reviewed to what extent the procedures of the services are compatible with the protection of privacy. The foregoing means that the Committee has not yet reviewed concrete cases to establish to what extent the applicable statutory requirements were satisfied in those cases. During its investigation the Committee established a short-term need for an in-depth investigation of concrete cases in which GISS deployed activities on social media. It met this need by including these cases in the Committee's current investigation of the investigative activities of GISS on social media. Similarly, the Committee is investigating subjects discussed in the present review report in concrete cases as part of its ongoing investigation into the exercise by GISS of the power to tap and the power to select sigint in the period September 2012 through August 2013.

In order to obtain a broad picture of the processing of telecommunications data by GISS and DISS the Committee investigated the different forms of acquiring telecommunication data and the use made of these data within a service. In this context the Committee devoted particular attention to the processing of data collections.

When addressing the part of the investigation concerning the cooperation by GISS and DISS with foreign services the Committee first considered which aspects of such cooperation were relevant. In view of the questions that had arisen in the media and in politics in the past months, the Committee chose to focus on the exchange of collections of raw data by intelligence and security services. Such exchanges might constitute an indication that intelligence and security services were mutually supplementing each other's powers, thus making it possible to circumvent national statutory restrictions. The Committee therefore investigated the exchange (provision or reception) of collections of (raw) telecommunications data by GISS and/or DISS.

Exchanging collections of (raw) data is a far-reaching form of cooperation. Such exchanges take place in the context of close cooperation relations. For this reason the Committee limited its investigation to these close cooperation relations. It is convinced that it has thus obtained a good picture of the relevant activities of the services.

For its investigation the Committee first of all sent written questions to the two services in order to obtain a general picture of the subject matter, so that it could consider what would be the best way to structure the investigation. Based on the answers to these questions and on exploratory talks with the two services the Committee planned investigation days for each of the services. On these investigation days the Committee held lengthy and detailed interviews with the employees involved, in most cases the heads of the acquiring

[24] The Committee understands procedure to mean not only the service's written policy, but also the procedure actually followed in practice.

departments, discussing the forms of data acquisition practised by the department in question and how the acquired data was stored and made accessible for internal use at the services. Following these interviews the Committee was shown how the applications utilised for making the data accessible work and which possibilities they offer. After these investigation days the Committee put additional questions to the services which were answered either in writing or at a second interview with the interviewed employees concerned. The subject of the cooperation of GISS and DISS with foreign services was not only discussed during the Committee's investigation days, but also separately. In addition, the Committee did supplementary research in the systems of the services.

The review report has the following structure. Sections 3-5 deal with the different types of data processing by the services in the field of telecommunications, viz.: the processing of data (section 3), the use of data (section 4) and the exchange of data with foreign services (section 5). Section 6 sets out the main conclusions and recommendations of the Committee.

3 The acquisition of telecommunications data by GISS and DISS

3.1 Introduction

This section deals with the *means* used by GISS and DISS to acquire telecommunications data: placing telephone taps or causing telephone taps to be placed, interception and selection of sigint, deployment of human sources, hacking computerised devices or systems and demanding telecom providers to give access to telephony data and/or user data.[25] These are the means used most frequently by the services for the acquisition of telecommunications data.[26] However, there is always a possibility of telecommunications data being sporadically acquired in another way. In theory a service may, when entering a dwelling, come across an itemized telephone bill of an investigation target. It also happens that the services acquire telecommunications data in the course of performing their task of promoting security. Naturally, the services also consult publicly accessible databases on the Internet, such as telephone directories and the RIPE database (issued IP addresses). In addition, telecommunications data may be provided by foreign services.

The most obvious method for acquiring telecommunications data is the *interception of telecommunication* while on its way from sender to receiver. The services have various powers which enable them to intercept such communications in specific cases. As regards these powers the law makes a distinction between telecommunication via a cable and telecommunication that is not cablebound, meaning telecommunication via satellites or radio waves. In the case of cablebound telecommunication the law permits targeted tapping only, while in the case of non-cablebound telecommunication it permits both targeted and untargeted[27] interception, subject to the condition that in the case of untargeted interception

[25] The Committee has not included the deployment of microphones in this list of means, because this means does not fall under the term telecommunication.

[26] See sections III and IV of the legal appendix to this review report for a discussion of the general legal framework for data processing, which includes the requirements of purpose limitation, necessity and propriety, and section II of the legal appendix to this review report for a discussion of the statutory safeguards governing the exercise of special powers, which include the requirements of necessity, proportionality and subsidiarity. Section V.2 of the legal appendix to this review report contains a separate explanation of the special powers in the field of telecommunications.

[27] The Explanatory Memorandum to the bill to adopt the ISS Act 2002 explains that this means that the interception is not targeted at communications originating from a specific person or organisation

and recording of non-cablebound telecommunications the services may not examine communication content until permission has been obtained from the minister concerned to select the communications in question from the 'bulk' acquired by untargeted interception. Communication that is on its way from sender to receiver is in the so-called transmission phase and as such falls under the privacy of the telephone and telegraph enshrined in article 13(2) of the Dutch Constitution. Infringement of this right is only lawful in the cases laid down by Act of Parliament by or with the authorisation of those designated for the purpose by Act of Parliament. The requirement of permission from the responsible minister to examine the content of tapped or intercepted telecommunications implements this statutory rule.

Another method is the *acquisition of stored telecommunications data*. This can be done by accessing a computerised device or system or by accessing another location where data is stored. The powers mainly used by the service to acquire stored telecommunications data are the power to hack and the power to deploy human sources. Pursuant to article 13 Constitution, stored telecommunications data does not fall under the privacy of the telegraph and telephone. This may change in the future; the bill to amend article 13 Constitution brings stored telecommunications data under the privacy of telecommunications (see the legal appendix to this review report, section II.3).

The third category of acquisition methods is that of *demanding access to telecommunications data* from providers of public telecommunication networks and public telecommunication services (further referred to as: telecom providers) or from the Central Information Point for Telecommunications (CIOT).

3.2 Wire-tapping and Internet interception

3.2.1 General

A wire-tap provides the services with different kinds of data: audio files of telephone calls, text files containing the content of text messages and the metadata of calls and text messages. These metadata comprise among other things the numbers involved in a call or text message, the starting time and the ending time of a call and the data of the mobile phone masts involved.

An Internet tap enables the services to examine the data packages sent or received from the IP addresses involved and the metadata of the Internet sessions. Data packages can relate to web pages visited, e-mails sent or received and/or chat traffic. The metadata of an Internet session relate among other things to the times at which the data packages were sent or received and the IP addresses involved (see the legal appendix to this review report, section V.2.3).

3.2.2 Permission for telephone and Internet taps

For both services, tapping of telephone calls and Internet traffic is based on an approval order: permission of the minister concerned to tap the telephone or Internet traffic from and to a specific telephone number or IP address (or several numbers/IP addresses) belonging to

---

or related to a technical characteristic, but that for example all data traffic sent via a specific satellite channel or at a specific frequency is as it were «hoovered» from the ether and then stored on computers (*Parliamentary Papers II* 1997/98, 25 877 no. 3, p. 44).

a specific person or organisation. It may happen that either the identity of the user or the telephone number or IP address used by a specific person is not yet known. Pursuant to article 25(6) ISS Act 2002 this need not prevent a service from obtaining permission for the tap. The missing data must, however, be added as soon as possible. In spite of the lack of a known identity, it must obviously be clear that tapping the communications in question serves the interest of the proper performance of its task by the service.

In their applications for the minister's permission the services must state the reasons why they consider that tapping the communications of the person or organisation in question for the purpose of performing specific statutory tasks satisfies the requirements of necessity, proportionality and subsidiarity (see the legal appendix to this review report, section III). After obtaining the minister's permission for the telephone or Internet tap,[28] the services request the relevant telecom provider to cooperate in tapping the telecommunications. It is obligatory for telecom providers to cooperate with such a request (article 13.2 Telecommunications Act). This procedure followed by the services - that a service does not make a request to the telecom provider until after it has obtained the minister's permission with respect to the person or organisation concerned - ensures that the safeguards for the protection of privacy laid down in the ISS Act 2002 are also upheld in actual practice. The Committee has established that the wire-tapping and Internet interception activities do not include any untargeted acquisition of (collections of) data.

The use of telephone and Internet taps by GISS in individual cases has been the subject of a continuous in-depth investigation by the Committee for years. No structural shortcomings in the exercise of the power to tap by GISS have emerged during this investigation. In the period 2008–2011 the Committee also monitored the relatively limited exercise of the power to tap by DISS.

3.3 Interception and selection of sigint

3.3.1 General

Pursuant to the ISS Act 2002, GISS and DISS are permitted to acquire non-cablebound telecommunications by untargeted interception. The services do not have power to acquire cablebound telecommunications by this means. The services' procedure for acquiring data from non-cablebound communications differs widely from the procedure for telephone and Internet tapping (see the legal appendix to this review report, section V.2.5). The former procedure is used to collect data from intercepted satellite and/or radio signals, known as *signals intelligence* or sigint. The part of sigint relating to communications between two parties is called *communications intelligence* (comint). GISS focuses exclusively on comint when acquiring sigint, while DISS acquires not only comint but also *electronic intelligence* (elint) from e.g. radar signals. This latter type of sigint falls outside the scope of this investigation, because it does not concern (tele)communication.

Sigint consists of analogue and digital data streams. The analogue stream contains telephone and telefax traffic. The digital stream that is transmitted via the Internet (IP) contains telephone traffic (VoIP), telefax traffic (FoIP) and other Internet traffic. Both streams contain communication content as well as metadata. Sigint metadata in any case provides

[28] In this context Internet tapping includes data tapping, which means a tap on Internet traffic from a smartphone.

information on the telephone numbers or IP addresses involved in the communication, the time and the duration of the call. In certain cases it also includes geographical data.

3.3.2 Untargeted interception by the NSO

Untargeted interception is carried out on behalf of GISS and DISS by the National Sigint Organisation (NSO), which is jointly controlled by the two services while its management has been placed with DISS. The activities of NSO are directed at satellite and/or radio communications. The Committee has established that its activities do not include any interception of cablebound telecommunications. When acquiring communications transmitted via satellites NSO intercepts bundles consisting of numerous communication sessions. Such acquisition is untargeted, since at the time of acquisition NSO does not know whose communications it is intercepting. In the case of *high frequency* (HF) radio traffic it is possible for NSO to discover the frequency at which a specific person or organisation is transmitting and thus to acquire the communications of this person or organisation by targeted interception.

For technical and financial reasons it is in the interest of the services to delimit the untargeted interception of satellite traffic, so that the number of irrelevant communication sessions included in the intercept material is kept at a minimum. There are several mechanisms for doing so. Based on the needs stated by the services NSO will explore the ether by exercising the power to *search* as regulated in article 26 ISS Act 2002. The permission of the minister is not required for this (see the legal appendix to this review report, section V.2.4). On this point the legislator took the ground that searching is not aimed at examining telecommunication content, and furthermore that a requirement to obtain permission would have no added value because it would be impossible to state in advance what NSO would be searching for.[29]

In addition to exploring the ether by exercising its power to search, NSO uses *filters* in behalf of the services when it is intercepting satellite traffic. GISS and DISS proceed in different ways in the matter of filtering satellite traffic.

For GISS, NSO separates digital traffic from analogue traffic. In the case of digital traffic, which is made up of larger files than analogue traffic and which moreover comprises huge numbers of data, metadata is separated from content. Relevant content of digital traffic is selected immediately upon its interception on the basis of so-called *leads* and approval orders. Only the selected content is intercepted and sent to GISS. This means that GISS only acquires content of digital communication sessions if it has either obtained the minister's permission to select on the basis of a specific identity, technical characteristic or search term, or if one of the operational teams has stated certain characteristics or search terms as *leads*. GISS uses *leads* to implement the search power under article 26 ISS Act 2002. A member of one of the operational teams who thinks that communications connected with a specific characteristic or search term are relevant to an investigation of the team, can choose to include the characteristic or search term in the *lead* list for NSO so that it can be used for filtering during interception. Under current policy at GISS no permission of a superior is required for this. It should be noted here that under the policy of GISS it is not permitted to examine the content of intercepted communications on the basis of a *lead* for the purpose of the operational process. If such content is to be used in the operational process, the *lead* must

[29] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 34 and 36.

be converted into an approval order, which requires the permission of the minister of the Interior and Kingdom Relations (see also section 3.3.4 of this review report).

The major part of the characteristics by which digital traffic is filtered by NSO derives from approval orders. The other characteristics derive from *leads*. NSO does not filter analogue communication streams for GISS; analogue traffic that is present in the intercepted satellite bundles is acquired and passed on to GISS in its entirety. It is not considered necessary to filter analogue traffic because this represents a relatively limited and steadily decreasing volume of data. This is due to the fact that people are increasingly switching to digital communication.

When intercepting for DISS, NSO already filters by certain technical characteristics at the time of interception. This means that NSO only intercepts satellite traffic having those characteristics. All the intercept material is then sent to DISS. The technical characteristics by which NSO filters can originate from various sources, for example earlier investigations by DISS or a publicly accessible source. They can be characteristics concerning a specific person or organisation with respect to whom/which an approval order for selection has already been obtained, or they can be broader characteristics relating, for instance, to the region in which the communication took place. The choices made on this point depend on the need, the technical possibilities and the information position of DISS. The Committee considers the application of these filters to be an element of interception under article 27 ISS Act 2002. Pursuant to the ISS Act 2002 no permission is required for such filtering, because at this stage the data is merely stored awaiting further processing, if needed.

3.3.3 Analysing metadata

After interception, there usually follows an investigation based on the intercepted metadata. The services store the metadata separately from the communication content and analyse it using applications. At GISS, the metadata obtained from sigint is analysed in combination with metadata from other sources. The aspect of combining sets of metadata by GISS will be discussed in greater detail in section 4.2. Metadata analysis may produce new technical characteristics of current investigation targets (persons or organisations) as well as new investigation targets. Both services use metadata analysis to support the process of sigint acquisition and selection.

In the course of its investigation the Committee took note of the position taken by employees of the two services that they are not required, before analysing metadata acquired by untargeted interception, to first select the metadata on the basis of an approval order obtained pursuant to article 27(3) ISS Act 2002. The services take this position because they deem metadata to be 'approval-free'. The services argued that the analysis of metadata does not involve examination of communication content, so that permission of the minister is not required.

In this respect the Committee takes the ground that it is indeed correct that in the Explanatory Memorandum to the bill to adopt the ISS Act 2002 it is argued that no requirement of permission of the minister is set on the untargeted interception of non-cablebound communications, because such interception does not involve any examination of content and consequently there is no infringement of privacy as yet, in this case the privacy of the telephone and telegraph.[30] The rest of this passage shows, however, that this argument

[30] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 44.

was based on the situation that the services would be unable to do anything with the data acquired.[31] This is no longer the case nowadays. When drafting the ISS Act 2002, the legislator apparently did not foresee the possibility of analysing intercepted metadata as currently practised by the two services. First of all it therefore remains to be seen whether analysis of metadata acquired by untargeted interception is permitted and if so, whether it would be appropriate to set further requirements for this form of data processing.

Regarding the first question the Committee observes that the fact that the ISS Act 2002 and the accompanying Explanatory Memorandum do not pay attention to the possibility of further processing intercepted metadata does not by definition mean that the law does not leave scope for such processing. The further processing relates to data that has already been gathered lawfully. The ISS Act 2002 provides a general legal basis for data processing (article 12(1)), which can be held to cover metadata analysis as well.

Regarding the second question, it will first have to be examined whether metadata analysis infringes privacy. To this end it must be established whether the intercepted metadata must be deemed to be personal data within the meaning of the ISS Act 2002: data relating to an identifiable or identified individual natural person. This is not by definition the case. For part of the metadata it can be established that it is not traceable to individual persons. Such metadata relate e.g. to the location of the transmitter masts involved or to the IP protocols used. This means that this metadata does not fall within the scope of article 10 Constitution and that processing the data does not infringe privacy. The situation for telephone numbers and IP addresses is less simple, because this data can under certain circumstances be linked to specific users. The legislative history of the Personal Data Protection Act shows that such data must be considered personal data if it is possible for the agency possessing the data to find out the user's identity without disproportionate effort.[32] The Committee has established that the metadata that have been collected may constitute a reason for the services to undertake follow-up action to discover the user's identity. Such action can take the form of demanding access at CIOT to the user data of a specific telephone number or IP address, or of linking the metadata to other data already available to the service. The Committee takes the view that identifying a user by linking data already in the possession of the services to the metadata must in any case be considered discovering the user's identity without disproportionate effort. The conclusion is therefore that part of the metadata acquired by the services by untargeted interception must be classified as personal data.

Since metadata falls under the protection of article 10 Constitution to the extent it concerns personal data, the Committee finds that in certain cases the processing of metadata acquired by untargeted interception infringes the privacy of the persons involved. In the light of this finding the Committee considers it important that the procedure for metadata analysis will be made subject to statutory safeguards to protect against unlawful infringement of privacy, for example the requirement to substantiate the necessity, proportionality and subsidiarity of processing the metadata in an application for internal or external permission (see the legal appendix to this review report, section III).[33] At present the process of metadata analysis after untargeted interception is not accompanied by these safeguards. The Committee recommends that specific rules pertaining to the processing of metadata be included in the law.

---

[31] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 44.

[32] *Parliamentary Papers II* 1997/98, 25 892, no. 3, p. 47.

[33] In the recent evaluation of the ISS Act 2002 the Dessens Committee proposed a new system of provisions pertaining to interception in which metadata, too, has been incorporated.

3.3.4 Searching and selecting

After the services have identified technical characteristics – possibly by means of metadata analysis – which are suspected to be related to investigation targets of the service or which belong to new investigation targets, they will in certain cases use the power to search in order to establish whether the characteristics do in fact belong to communications of the investigation target in question and, in the case of new investigation subjects, to establish whether a relationship with the investigation area does in fact exist. This is searching for selection purposes.

In its review report on the use of sigint by DISS the Committee assessed three common practices at DISS for searching for selection purposes:

1. Searching the communications bulk to determine whether the desired intelligence can be generated using the selection criteria for which permission has been obtained;
2. Searching the communications bulk to identify or characterise potential targets;
3. Searching the communications bulk for data from which it is possible to derive future selection criteria for the purpose of an expected new investigation area.

The first form of searching means that DISS searches for technical characteristics belonging to persons and organisations already designated as investigation targets and for the selection of whose data the minister has already given permission, on the basis of data relating to these persons and organisations. The second and third forms of searching are aimed at recognizing, characterising and identifying new investigation targets, either in the context of ongoing investigations (the second form of searching) or in the context of anticipated new investigation areas (the third form of searching). In the aforementioned review report the Committee held that only the first form of searching for selection purposes was lawful, because it is only for this form of searching that the privacy infringement is overcome by the minister's permission to exercise the power to select with respect to the person or organisation in question. In this situation the use of the power to search *supports* the use of the power of selection for which permission has been obtained.[34] That is necessary because article 13 Constitution requires authorisation by a competent authority before the privacy of the telephone and telegraph may be infringed. In the review report just mentioned the Committee suggested that the legislator consider whether it is necessary, with due regard to the protection of privacy, to grant DISS (and GISS) power to search for the purpose of a new deployment of the power to select.

It emerged from the interviews conducted by the Committee that DISS has been using the power to search in respect of new investigation targets following metadata analysis. This is the second form of searching for selection purposes; a procedure which the Committee considered unlawful in its earlier review report on the use of sigint by DISS. This shows that the problems or at any rate part of the problems regarding the power to search by DISS which the Committee identified in its aforementioned review report still exist.

The Committee will return to searching procedures at GISS in the continuing investigation of the use by GISS of the power to tap and the power to select sigint. The review report on this

[34] CTIVD Review Report no. 28 on the use of sigint by DISS, *Parliamentary Papers II* 2011/12, 29 924, no. 74 (appendix), available at www.ctivd.nl, sections 4.3.3 and 7.4.3.

investigation covering the period September 2012 through August 2013 is expected to be presented to the minister in early April 2014.

At both services the power to search intercept material for selection purposes is carried out by a limited number of employees of the acquiring department, who are not involved in the analysis of intelligence content. If the characteristics used for searching actually deliver communication content, permission of the minister to select the material must have been obtained before the content of the communications may be released for use in the operational process. This procedure is embedded in the technical system at both services.

In earlier review reports the Committee already established that both GISS and DISS did not state sufficient reasons for the use of the power to select. Briefly stated, the Committee held that the reasons stated for selection were insufficiently focused on the persons and/or organisations included in the selection list.[35] The Committee keeps emphatically demanding that attention be paid and continue to be paid to these issues.[36]

3.4 Human sources

3.4.1 General

One of the means available to the services for acquiring data are human sources who have or will gain access to certain data that is not publicly accessible (see the legal appendix to this review report, section V.2.1).

Insofar as DISS deploys human sources to acquire telecommunications data, the Committee's investigation did not give rise to observations.

The activities of GISS in this field fall into two categories. These categories are explained in greater detail in the secret appendix to this review report concerning GISS. Below, the Committee presents its findings in general terms, without compromising the secrecy of sources, the current level of knowledge and/or the procedure followed by GISS.

3.4.2 Permission for certain activities of human sources

When human sources are used to acquire data, this is done at the request of one or more of the operational teams of GISS. If such a request is made, the acquiring department first examines whether the desired data can be acquired through an existing human source. If it is not deemed possible to do so, the department will try to recruit a human source who has access to the data in some way or other. If the choice falls on deploying a new human source, and if a need for the data is felt by more than one team, the acquiring department files an application with the relevant unit head for permission to deploy an agent pursuant to article

[35] See e.g. CTIVD review report no. 28 on the use of sigint by DISS, section 8.3.4 and CTIVD review report no. 19 on the use of the power of tapping and signal interception by DISS, *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), section 7, both available at www.ctivd.nl.

[36] The continuing in-depth investigation of the use of the power to tap and the power to select sigint by GISS devotes attention to this issue. The Committee further intends starting a follow-up investigation of the use of sigint by DISS in the first quarter of 2014.

21 ISS Act 2002 and/or an informer pursuant to article 17 ISS Act 2002.[37] The difference between these two kinds of human sources is that an agent is controlled by the service, while in principle an informer passes on data he has obtained in the course of his usual activities.[38] This has the result that for the purpose of the ISS Act 2002 employing an agent is considered a special power, while deploying an informer falls within the scope of the general power to gather data.

The operational plans are explained in the application for permission to deploy an agent or an informer. The substantive assessment of the necessity, proportionality and subsidiarity of the application is done by the teams applying for permission, since they are in the best position to substantiate why the data to be acquired is necessary for the investigation and why the data must be acquired by this particular method. So the operational teams supply the input for the application which is prepared by the acquiring department. When data is to be acquired for one operational team only, the team prepares the application itself. Subsequently, the application must be assessed by the legal department, before it is submitted to the unit head for a decision.

Permission of the unit head to deploy an agent under article 21 ISS Act 2002 is valid for three months at most. When the operational team involved needs to continue the deployment, it must apply for permission to continue deploying the agent. Applications for renewed permission need no longer be made to the unit head as is required for the initial deployment, but to the team head. An application for renewal sets out operational developments and, if necessary, states adjusted operational choices. Permission to deploy an informer under article 17 ISS Act 2002 must likewise be renewed periodically at team head level.

The Committee has established that the services obtain permission to acquire the data at which the operational plans are directed before the first deployment of a human source and subsequently periodically for any renewed deployment. The Committee points out that the acquiring department or the relevant operational team does not, however, apply for separate permission for each individual assignment.

The Committee takes the ground that GISS has the task of responding flexibly to new developments. This also entails new ways of deploying human sources. The Committee holds the opinion that in such a dynamic field, privacy can only be adequately protected if emphasis is placed on the nature of the activity and the type of data acquired, as far as possible regardless of the means used to acquire the data (deployment of the human source).[39]

---

[37] In implementation of article 19 ISS Act 2002, the rules on mandating the authority to give permission for deployment and for renewal of deployment are laid down in the GISS Special Powers Mandate Decision 2009. Articles 4 and 5 of the Decision regulate the level at which permission for deployment of agents must be given. The Decision shows, moreover, that permission to deploy agents holding certain functions in society must be granted at a higher level. This can be at the level of director, head of service or the minister.

[38] See also CTIVD review report no. 8a on the deployment by DISS of informers and agents, more in particular abroad, *Parliamentary Papers II* 2005/06, 29 924, no. 11 (appendix), available at www.ctivd.nl, para. 4.

[39] See also the report of the Dessens Committee, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, [Evaluation of the Act on the Intelligence and Security Services 2002], December 2013, *Parliamentary Papers II* 2013/14, 33 820, no. 1 (appendix), p. 79.

The Committee has found in the course of its investigation that the legal affairs department of GISS has proposed a procedure that will better guarantee the protection of privacy. One of the proposals is that if a human source is to undertake an activity that is comparable to tapping or hacking, permission must be obtained at a higher level than is normally required for deployment of the human source in question. Separate reasons will have to be stated specifically for this activity in the application for permission. In respect of data that has already been gathered the memorandum recommends that this data need not be destroyed pursuant to article 43(2) ISS Act 2002, because the acquisition of this data was not unlawful under the Act. The proposal of the legal department is explained in greater detail in the secret appendix to this review report concerning GISS.

The Committee does not follow the position taken by the legal department on the lawfulness of current procedure in the aforementioned situations. It points out that where human sources exercise special powers on the instruction and under the direction of GISS, these powers must be considered to be exercised by GISS. In fact therefore, the powers of tapping as defined in article 25 ISS Act 2002 and of hacking as defined in article 24 ISS Act 2002 are exercised by GISS. Pursuant to the ISS Act 2002 an application for permission to tap must be submitted to the minister of the Interior and Kingdom Relations. Pursuant to the GISS Special Powers Mandate Decision 2009, an application for permission to hack must be submitted to the director of the unit. The required level at which permission must be obtained for deploying a human source is that of the unit head and is consequently lower than the level that is required in view of the nature of the activities. Moreover, reasons for exercising the special powers must be stated separately from the reasons stated for deploying the human source. The Committee considers it unacceptable that these safeguards are being disapplied.

The Committee holds the opinion that for the purpose of establishing the gravity of the above-mentioned shortcomings, a distinction should be made between situations in which, incorrectly, no permission has been obtained from the minister for an activity that must be considered tapping, and situations in which no permission has been obtained from the unit director for an activity that must be considered hacking. The former level of permission is prescribed by the ISS Act 2002 and is the implementation of the requirement of article 13 Constitution that infringement of the privacy of the telephone and telegraph is only permitted by or with the authorisation of those designated for the purpose by Act of Parliament. It is the opinion of the Committee that failure to comply with this requirement makes the activity unlawful.

The level at which permission must be obtained for hacking does not follow directly from the ISS Act 2002, but from the GISS Special Powers Mandate Decision 2009, which was adopted internally at GISS. Since it is not a statutory obligation and since the difference is only one level (director or head of the unit), the Committee holds the opinion that this procedure of GISS should not be automatically considered unlawful. This does not mean, however, that GISS acted lawfully in all of these cases. The statutory requirements applying to the exercise of special powers are not satisfied unless sufficient reasons have been stated to substantiate the necessity, proportionality and subsidiarity of the hacking (see the legal appendix to this review report, section III). Consequently, insofar as the reasons stated for the deployment or continued deployment of the human source who did the hacking did not sufficiently address the substantiation of the need for the hack, the Committee will conclude that the hacking was done unlawfully. In its ongoing investigation of the investigative activities of GISS on social media the Committee will assess whether GISS acted lawfully in concrete cases. The review report on this investigation is expected to be presented to the minister in early April 2014.

The Committee recommends that GISS adjusts its procedure without delay by henceforth applying for permission at the prescribed level and by stating separate reasons for the exercise of special powers by human sources in addition to the reasons for deploying the human sources in question.

3.5 Hacking

3.5.1 General

Both services acquire telecommunications data by hacking computerised devices or systems (see the legal appendix to this review report, section V.2.2). DISS carries out hacking in cooperation with GISS. Occasionally, for practical reasons, GISS will also hack a computerised device or system on behalf of DISS.

The services can obtain various types of data by hacking. The most important categories are e-mail accounts and web forums. They may, however, also obtain other types of Internet sites or other files stored in a computerised device or system. The services acquire both communication content and metadata of e-mail accounts, web forums and other Internet sites. One advantage of hacking an e-mail account over an Internet tap is that all e-mail traffic from different IP addresses converges in an e-mail account, while an Internet tap only taps traffic from and to one or more specific IP address(es).

3.5.2 Permission for a hack

In its policy GISS distinguishes between distance hacking and hacking a device that is in the physical possession of the service (for example the laptop of an investigation target). The level at which permission must be obtained for using the power of distance hacking is higher than for hacking a computerised device in the physical possession of GISS. Distance hacking requires permission of the director of the unit.[40] For hacking a computerised device to which GISS has physical access, permission of the head of the unit concerned will suffice.[41] For both forms of hacking the application for permission is drawn up by the operational team concerned and must be assessed by the relevant team head, the legal department and, in the case of distance hacking, also by the relevant unit head. The acquiring department carries out the hack after permission has been obtained.

The application for permission must state which computerised device or system is to be hacked and what data the service aims at acquiring by the hack. An application for permission to hack an e-mail account may also cover 'related characteristics' so that a new e-mail address created by the same investigation target will be covered by the permission. The legal department assesses in such a case whether the new characteristic falls under a permission already obtained.

GISS indicated to the Committee that applications for permission are sometimes formulated rather broadly in order to leave the service flexibility to acquire (copy) any files which – after consultation - turn out to be necessary to the operational team concerned. Although the Committee understands that prior to a hack GISS has only limited insight into the data it

[40] Article 7(1) Special Powers of GISS Mandate Decision 2009.
[41] Pursuant to article 7(2) Special Powers of GISS Mandate Decision 2009 the authors of the Decision could also have chosen to require of the director of the unit concerned.

may find and that preferably, therefore, the operational team should have several options, the Committee considers that it is important that applications state as specifically as possible on the basis of the available information what data a hack is targeting. Only then is it possible to make a full assessment of the necessity, proportionality and subsidiarity of the intended exercise of the power (see the legal appendix to this review report, section III). When in the course of a hack the acquiring department comes across data not covered by the permission, but which may be relevant to the investigation of the operational team, it can still – via a fast-track procedure – ask permission to copy this data after consulting the operational team.

DISS applies, where necessary, to the minister of Defence for permission to deploy the power to hack. Permission of the head of DISS is required for the renewed use of this power. Before being submitted to the minister the application is assessed by the head of the acquiring department, the legal department and the (deputy) director of DISS.

3.5.3 Permission for certain specific hacking activities by GISS

There has been an internal legal discussion at GISS about the appropriate level of permission to deploy the power to hack in some specific cases. The legal department has identified two points for attention regarding the use of the hacking power:

1) In many cases the use of hacking leads to examination of streaming data.[42] Pursuant to the GISS Special Powers Mandate Decision 2009 this requires permission of the minister of the Interior and Kingdom Relations;
2) at the time of starting a hack it is not always possible to foresee what exactly it will produce and how serious the potential privacy infringement will be. This regularly turns out to be equivalent to the privacy infringement by tapping.

By way of solution it has been suggested that the legal department should ensure that the minister's permission is obtained in accordance with the GISS Special Powers Mandate Decision 2009 when it is foreseeable or intended that the hack will result in examination of the content of conversations, telecommunications and/or data communication within the meaning of article 25 ISS Act 2002. From the perspective of due care, moreover, it has been proposed that the minister's permission should also be obtained if it cannot be excluded in advance that the service will, by using a hack, examine the content of conversations, telecommunications and/or data communication. Finally, the legal department has proposed assessing ongoing hacks bearing in mind the aforementioned issues.

The Committee has established that GISS sometimes formulates applications for permission to hack broadly because the abovementioned Mandate Decision is in keeping with the statutory requirement that the minister's permission must be obtained for hacking activities resulting in the examination of streaming telecommunication. This is also in keeping with the privacy of the telephone and telegraph under article 13(2) Constitution in its present wording. It is the opinion of the Committee that failure to obtain the minister's permission in such cases makes the hacking unlawful. It recommends that GISS, without delay, brings its procedure into line with the statutory requirement that permission must be obtained from the minister of the Interior and Kingdom Relations whenever hacking will result in the

[42] The term 'streaming data' or 'streaming telecommunication' refers to telecommunications acquired *real time*, which are therefore in transit from sender to receiver at the time of acquisition, as in a telephone tap pursuant to article 25 ISS Act 2002.

examination of streaming telecommunication within the meaning of article 25 ISS Act 2002, permission.

Furthermore the Committee points out that the proposed text of the new article 13 Constitution has consequences for the power to hack (see the legal appendix to this review report, section II.3). If stored communications are also brought under the protection of article 13 Constitution, examining content of such communications will also infringe the privacy of telecommunications. As a result, a considerable part of the hacking activities of the services will then have to satisfy the requirements set by the Constitution for such infringement.

3.5.4 Substantiating applications for permission by DISS

The acquiring department at DISS indicated to the Committee that there are cases in which it is not possible to name specific persons in the application for permission to hack. Its explanation for this was that the information in the possession of DISS often relates to a certain threat, without the identities of the persons involved in the threat being known at that moment. In practice the acquiring department substantiates its applications for permission by reference to known data relating to the digital activities linked to a specific technical characteristic. The Committee points out that in the case of telephone taps the law provides for the possibility of the minister granting permission subject to the condition that the lacking data concerning the identity of the person or organisation targeted by the tap will be supplemented. It is the opinion of the Committee that if DISS possesses reliable intelligence showing that certain digital activities are connected with activities posing a threat, the person who carries out these digital activities can be considered to be a lawful investigation target, irrespective of his or her identity. Consequently, hacking these activities is not unlawful. The Committee recommends that if the data concerning the identity of the user or users of the technical characteristic becomes known, DISS will immediately add the data to the reasons already stated and communicate it to the minister.

This subject will be discussed in greater detail in the secret appendix to this review report concerning DISS.

3.5.5 Hacking of web forums by GISS

When GISS hacks a web forum, this means that the service copies the entire forum. This subject will be discussed in greater detail in the secret appendix to this review report concerning GISS. In the following the Committee's findings are represented as far as it is possible to do so without compromising the secrecy of sources, the current level of knowledge and/or the procedure used at GISS.

The Committee has established that the acquisition of an entire web forum means acquiring a collection of (personal) data, including communication content. Such data is acquired from stored telecommunications and not from streaming telecommunications within the meaning of article 13 Constitution. The acquisition of an entire web forum entails serious infringement of the privacy of the persons who are active on the forum. It is the opinion of the Committee that this fact must be central to the substantiation of the application for permission to hack the server on which the forum is stored.

Among the web forums that GISS acquires or has acquired are forums that exclusively contain data of persons who give rise, by the goals they pursue or by their activities, to the serious suspicion that they constitute a danger to the continued existence of the democratic

legal system, or to the security or other vital interests of the state. The Committee takes the ground that with respect to such web forums it can generally be argued that in principle the acquisition of personal data, including communication content, falls under the performance of its task by GISS and will readily satisfy the requirements of necessity, proportionality and subsidiarity.

On the other hand, GISS has also acquired web forums which, in addition to the data of (potential) investigation targets, also contain the data of persons who cannot be deemed to be such targets. It is true that the acquisition of these web forums may be necessary for the performance of its task by GISS, but it will only be proportional to acquire communication content of persons who do not give cause for doing so from the perspective of national security, if there are compelling operational interests for such acquisition.

The lawfulness of hacking web forums in concrete cases will be assessed as part of the current investigation by the Committee of the investigative activities of GISS on social media. The review report on this investigation is expected to be presented to the minister in early April 2014.

The Committee points out that separate applications to the director of the unit for permission to acquire a specific web forum are present only with respect to web forums acquired by GISS by means of the power to hack. In addition to this source, however, GISS also acquires web forums from foreign services. In those cases no reasoned assessment is laid down in writing why it is lawful to examine the content of the web forum. The Committee recommends that when GISS acquires web forums, it will in all cases assess, for the purpose of its (internal) permission procedure, to what extent examination of the content of the web forum in question satisfies the requirements of necessity, proportionality and subsidiarity. This assessment must, moreover, be laid down in writing.

3.5.6 Carrying out hacks

The Committee has found that in certain cases the acquiring department of GISS, when carrying out a hack, will test whether the login data (login name and password) do in fact give access to an e-mail account while no permission to hack the e-mail account has been given. On this point the acquiring department has agreed with the legal department that it may only test whether the login data works. DISS, too, does a preliminary test prior to preparing an application for permission, to examine whether it is possible to gain access to the relevant account using the login data in its possession. The Committee has established that the services do not actually copy any content of the e-mail account until permission to do so has been given either internally (GISS) or by the minister (DISS). This means that the content of the e-mail account does not become available for use in the operational process until after permission has been obtained. Given this safeguard the Committee considers this procedure lawful.

3.6 Telephony traffic data and user data

3.6.1 General

The ISS Act 2002 confers power on the services to demand access to traffic data from telecom providers. The counterpart of this power to demand access to data is the statutory obligation of telecom providers to comply with the services' demands. Such a demand for access covers data relating to a user (name, address, city, number), data relating to the persons or

organisations with whom/which the user is or has been connected or tried to establish a connection or who/which tried to establish a connection with the user (name, address, city, telephone number), data relating to the connection itself (starting time, ending time, terminal equipment location data, terminal equipment numbers) and data relating to the subscription (the type of service which the user is using or has used, the data of the party paying the bill). In brief, a demand may relate to a combination of user data and metadata. In practice, GISS only acquires metadata by making such a demand for access. A service may demand to data for a specific period in the past, but it may also demand real time access to data (see the legal appendix to this review report, section V.2.6).

Article 29 ISS Act 2002 pertains to part of the data to which the services may demand access pursuant to article 28 ISS Act 2002: user data, also called subscription data. These are the name, address, city and number of, and the type of service used by a user. Demands for access to this data are not made to individual telecom providers, but to the Central Information Point for Telecommunications CIOT (see the legal appendix to this review report, section V.2.7).

3.6.2 Permission to demand access to telephony traffic data or user data

The requirement that the reasons substantiating necessity, proportionality and subsidiarity be laid down *in writing* does not apply to the deployment of the special powers for demanding access to traffic and user data. The Committee has recommended in the past, however – in a review report concerning DISS – that it considered recording the reasons for deploying these powers in writing important for purposes of internal and external control as well as for reasons of due care.[43]

The Committee has found that even in the absence of a statutory obligation, it is current procedure at both services to lay down in writing the reasons substantiating the necessity, proportionality and subsidiarity of applications for deploying article 28 or article 29 ISS Act 2002. It forms part of the procedure followed by the operational team or bureau concerned when it applies for internal permission to exercise the power. The Committee has established that these applications for permission focus on a specific investigation target (individual person or organisation). In this context there is no question of any demands for untargeted access to (collections) of telephony traffic data and/or user data.

Demands for access to telephony traffic data based on article 28 ISS Act 2002 must be made by the head of the service concerned. In the opinion of the Committee this is indeed the permission level prescribed by law for deployment of this power. The law permits the head of the service to mandate his authority in regard to demands for access to user data based on article 29 ISS Act 2002. At GISS, permission must be obtained from the team head of the operational team concerned. At DISS, power to give such permission is vested in the head of the acquiring department. There is a difference between the services as regards the application procedures for permission to deploy article 28 or article 29 ISS Act 2002, namely that at DISS the application is checked and authorised by the legal department before it is submitted to the service management or the head of the acquiring department, while no such legal assessment takes place at GISS.

[43] CTIVD review report no. 25 on the conduct of DISS with respect to two suspended employees, *Parliamentary Papers II* 2009/10, 29 924, no. 59 (appendix), www.ctivd.nl, section 4.2.

When a service identifies a telephone number of which it is important to discover the user's identity in the context of an investigation conducted in connection with their intelligence and/or security tasks, it will first check whether the number is already known at the service and what information concerning the user is available. If the necessary information is not available within the service, it may decide to apply for permission to demand access to the user data. Subsequently, the service demands access to the data of the user of the number at CIOT. Another possibility is for the service to demand access at the relevant telecom provider to both telephony traffic data and user data pursuant to article 28 ISS Act 2002. In the latter situation it must already be clear from the available information that it is necessary for the purpose of the investigation to gain insight into the network of the person in question.

3.6.3 Demand for access to data at CIOT

Both services use an automated system for accessing data at CIOT. Data may only be accessed after permission has been obtained at the appropriate level. The services safeguard compliance with this rule in different ways. At GISS, the operational team member sends a demand to the telecom service desk of the acquiring department. The desk checks whether an approval order for the demand exists and then accesses the data using an application. The result is passed on to the team. DISS has a limited number of accounts for automated data access and retrieval at CIOT which are used by employees of the operational bureaus. Input of the reference of the approval order obtained under article 29 is obligatory for each data access, so that it is always clear to which approval order the data access is linked. Because of the limited number of accounts and because of the obligatory input of the approval order reference, it can always be traced which employee carried out the data retrieval.

3.6.4 The provision of telephony traffic data by DISS to GISS

The Committee has found that it is standard procedure for DISS to share with GISS the lists of telephony traffic data which the service receives from telecom providers in response to demands pursuant to the ISS Act 2002. The reason for doing so is that GISS, because of its statutory tasks, possesses more information in the field of counterterrorism than DISS and is therefore in a better position to assess whether the person concerned and the telephone numbers in the list are relevant in that context. Where there are grounds for doing so, GISS provides DISS with a summary of the available information.

The Committee takes the ground that the services have a statutory duty to assist each other as much as possible and that such assistance may in any case take the form of providing data. Article 58 ISS Act 2002 is the legal basis for the exchange of data between the services. As is the case for any form of data processing, the provision of data must be necessary for the proper implementation of the ISS Act 2002 and in addition it must be done properly and with due care. It is the opinion of the Committee that these requirements are satisfied by following the procedure described above, because further characterisation of the data obtained can be considered necessary for the investigation by DISS and because in the context of this purpose it cannot be considered disproportional[44] that the services, where necessary, mutually use data already acquired by the other service in the performance of its task. With regard to the requirement that data must be processed with due care the Committee observes that it has not found any evidence that DISS has not been acting with due care when providing telephony traffic data to GISS.

[44] The proportionality of the chosen means to the purpose is part of the requirement of due care.

4 The use of telecommunications data by GISS and DISS

4.1 Storing telecommunications data and making it accessible

The telecommunications data which the services acquire by exercising their general and special powers (see the legal appendix to this review report, section V) is intended for use in the operational process and for being combined with other data for the purpose of preparing reports. After being acquired the data is, to this end, stored in digital form on servers and made accessible using computer software (applications).

For making accessible the data acquired by the exercise of special powers (for instance audio files of telephone taps or data acquired from hacked e-mail accounts), the two services in most cases use applications, with the permission to exercise the power required pursuant to ISS Act 2002 or pursuant to the relevant mandate order functioning as gateway to the data. This means that the data is only accessible to those employees who applied for permission to exercise the power and, where applicable, to employees involved in transcribing or translating conversations, messages or other data. In addition, the data is accessible to the employees charged with the operational or technical management of the application.

The above can be deemed the general procedure for making accessible data acquired by the exercise of special powers. It is the opinion of the Committee that this procedure is consistent with the statutory requirements pertaining to internal access to data which – briefly stated – are that employees of the services may only be given access to data to the extent necessary for the proper performance of their tasks and that the heads of the services must ensure that the necessary security features are in place to protect against unauthorised data processing (see the legal appendix to this review report, section IV.1).

The Committee has found that there are two exceptions to this general procedure. First, applications are used at GISS to combine different sets of raw data for analysis purposes while the data is also used for wider purposes than merely for the investigation in connection with which the data was acquired. Such combining of data is discussed in section 4.2 of this review report. Secondly, the content of the web forums acquired by GISS is made accessible using an application that is accessible to employees of more than one operational team. This application will be discussed in greater detail in section 4.3 of this review report.

After the data acquired by the exercise of special powers has been made accessible, it is processed and characterised by the (audio) processors, analysts and, where applicable, linguists involved in the investigation. In this step the data that is relevant to the investigation in question or to another ongoing investigation, if applicable,[45] is separated for further processing from the data lacking such relevance. The data is then classified as evaluated data. The raw material, i.e. the data not yet assessed for relevance, is in most cases retained for some time.

The Committee has established that it is not possible to give an unequivocal answer to the question how long raw data may be retained pending possible further processing, as long as it has not been established whether the data is relevant to the investigation in connection with which the data was acquired or to any other ongoing investigation. This situation must be distinguished from the situation in which GISS or DISS has established that certain data is *not* relevant to the investigation in connection with which it was acquired. On this point the

[45] Known as by-catch

law is clear: in this case the data must be removed and ultimately erased. The ISS Act 2002 only sets a maximum storage period for sigint data acquired by untargeted interception: this data may be stored for a period not exceeding one year for the purpose of further selection. The ISS Act 2002 does not prescribe a maximum storage period for other raw data acquired by the exercise of special powers, such as tapped data or data collections acquired by hacking. For the purpose of protecting the privacy of those in relation to whom GISS and DISS acquire data, the Committee considers it important that further rules be included in the law regarding the maximum storage period of raw data in other cases. It recommends that this issue be addressed in the forthcoming amendment of the ISS Act.

The evaluated data that is deemed relevant to the investigation are stored in a manner making it accessible to a wider circle of people. Both services have service-wide applications enabling employees to search all evaluated data which they are authorised to search.

4.2 Analysis of telecommunications data

In addition to accessing, combining and linking data by hand, both services have applications that make computerised data analysis possible. The Committee distinguishes three categories of applications used by the services for analysing telecommunications data: (1) analysis applications for the purpose of checking integrated data sources, (2) analysis applications for the purpose of network analysis and (3) analysis applications using extensive visualisation and analysis techniques.

A common denominator of these applications is that they can be used to combine and analyse data from different sources. This does not by definition mean, however, that the services thereby abandon compartmentation; a number of analysis applications only allow access to raw data from special powers to employees who are involved in the investigation for which these powers were exercised. In this context combining means that the raw data acquired by different special powers exercised for the purpose of the investigation in question are combined for analysis purposes, sometimes enriched with other data (e.g. geographical maps). GISS also uses applications which, for analysis purposes, give access to combined data from different sources, including raw data acquired by the exercise of special powers. These applications are only accessible to one of the acquiring departments of GISS and outside this department to only a very limited number of processors.

The Committee has considered the question whether or not combining and analysing raw data acquired by the exercise of special powers is compatible with the purpose limitation prescribed by the ISS Act 2002 and with the provisions governing the exercise of special powers (see the legal appendix to this review report, sections III and IV). Data acquired by means of a special power are acquired for a specific purpose. This purpose must fall within the scope of the intelligence or security tasks of the services (article 18 ISS Act 2002)[46] and must be recorded in the substantiation of the application for permission to use the power. With respect to the raw data acquired by the exercise of a special power, however, it has not been established yet whether this data is relevant to the investigation. So the question arises whether this raw data may also be used for other ongoing investigations or even for other

[46] Article 18 provides that special powers may only be exercised insofar as necessary for the proper performance of the a and d tasks of GISS and of the a, c and e tasks of DISS. So the law does not permit the exercise of a special power for screening purposes (the b task of the services), for the purpose of promoting security (the c task of GISS, the d task of DISS) or for the purpose of guarding and protecting the system (the e task of GISS, the f task of DISS).

statutory tasks of the services than the task(s) for which it was originally acquired. It could be argued that any data acquired lawfully through the exercise of a special power may subsequently be used for all task of the services. The Committee holds the opinion, however, that for reasons of privacy protection the infringement resulting from the exercise of a special power must be limited by restricting the use of the raw data so acquired exclusively to use for the purpose of the investigation in the context of which the data was acquired or for the purpose of another ongoing investigation within the scope of the intelligence or security tasks of the services.[47] The Committee points out that once the data has been evaluated, it may subsequently be used for all tasks of the services (also, therefore, for other tasks than the intelligence and security tasks).

The Committee has established that the raw data acquired by special powers which GISS combines for the purpose of analysing them by means of applications, are metadata (see also section 3.3.3 of this review report). The Committee holds that the use of combined metadata is lawful insofar as the analysis is made for the purpose of ongoing investigations falling within the scope of the intelligence or security tasks of GISS. This means that such combined metadata may only be used for the service's intelligence and security tasks and not for other tasks.

4.3 Use by GISS of data from web forums

When GISS processes data from a web forum it utilises an application in which it stores the web forums in its possession. The application serves two purposes: making the data accessible and analysing the data. These procedures are necessary because a web forum contains too much data to examine all of it in full, like the service does in the case of the audio files of telephone taps. This subject is considered in greater detail in the secret appendix to this review report concerning GISS. In the following the findings of the Committee are represented in general terms, without compromising the secrecy of sources, the current level of knowledge and/or the procedure of GISS.

Access to the application for processing web forums is restricted to specific operational team members. In addition, such a team member must then be authorised to access a specific forum. The authorisation is granted on the basis of relevance to the investigations in which the team member is involved. The Committee has established that this procedure is consistent with the requirement that data is only disclosed within the service to employees in so far as this is necessary for the proper performance of the tasks assigned to the employees in question (article 35 ISS Act 2002). The Committee points out that the raw (unevaluated) data stored in the application may only be used for the purpose of ongoing investigations which fall within the scope of the intelligence or security task of the service.

It emerged from the Committee's investigation that the web forums made accessible with the application usually remain available. GISS stated that the acquired web forums will always remain relevant, because the data is necessary for certain operational goals. The Committee notes that it considers storing and keeping available entire web forums, especially forums of which not all participants can be deemed in advance to be (potential) investigation targets of GISS, as a very onerous means which must be proportional to its operational goal (see also section 3.5.5. of this review report). The lawfulness of retaining web forums in concrete cases is being assessed in the context of the Committee's current investigation of the investigative

[47] Known as by-catch.

activities of GISS on social media. The review report on this investigation is expected to be presented to the minister in early April 2014.

5 The exchange of telecommunications data with foreign intelligence and security services by GISS and DISS

5.1 Cooperation relationships with foreign intelligence and security services

The basis for cooperation with foreign intelligence and security services is found in the first place in the ISS Act 2002, which provides that the heads of the services must maintain relations with foreign services that qualify for such cooperation. The Dutch services must assess whether a foreign service *qualifies* for close cooperation against a number of criteria, including the degree of respect for human rights, democratic anchorage and professionalism and reliability.[48] In addition, cooperation with foreign services is based on a certain degree of mutual trust and is given further substance by bilateral and multilateral agreements.

In reaction to the questions raised in the media and in political circles, the Committee investigated the cooperation with foreign services. It focused its investigation on the provision and receipt of collections of (raw) telecommunications data. In the terms of the ISS Act 2002 this can be considered as exchanging data or rendering support. The requirements which these forms of cooperation must satisfy pursuant to the ISS Act 2002 are described in the legal appendix to this review report, sections VI.2 - VI.4.

Exchanging collections of (raw) data is a far-reaching form of cooperation. The Committee has established that such exchanges take place within close cooperation relationships between friendly states that are based on strong mutual trust. According to the assessments made by GISS and DISS these foreign services satisfy the criteria for cooperation. The mutual trust is not unlimited. In the past, concrete incidents or media reports have caused the services to reconsider certain aspects of their cooperation with some of these services. GISS and DISS should also be aware of the fact that the Dutch interests they are protecting do not always run parallel with the interests of those foreign services and vice versa. As regards the exchanges of (raw) data in the context of the cooperation relationships which the Committee has reviewed the Committee has established that in each of these cases there was a clear common interest, for example in the context of combating terrorism and in the context of military operations abroad.

The Committee points out, in line with the observations in the Parliamentary Papers relating to the ISS Act 2002, that it is generally not customary in international dealings between intelligence and security services to ask the foreign service about the source or method used to collect data, nor for the service itself to provide information about how the data was acquired.[49] The legislator did not deem it inconceivable, however, that in some trusted relationships or for the purpose of joint operations the services would pursue greater openness as to their sources.[50]

---

[48] CTIVD review report no. 22a on the cooperation of GISS with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), available at www.ctivd.nl, section 5.

[49] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 63.

[50] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 63.

The Committee has established that in the close cooperation relationships it reviewed GISS and DISS trust to a considerable extent that the foreign services in question respect human rights and act within the parameters of their own national regulatory framework. It is the opinion of the Committee that in the light of the recent revelations it is desirable to verify whether such trust is still justified. Pursuant to the law[51] it is the duty of the heads of GISS and DISS, under the political responsibility of the minister concerned, to assess whether foreign services still qualify for the various forms of cooperation which take place in the context of a close cooperative relationship.[52] In practice this means that they must make further inquiries into the statutory powers and (technical) possibilities of foreign services, in order to be able to make well-considered assessments. Regarding this issue the Committee recommends that the ministers of the Interior and Kingdom Relations and of Defence assess the cooperative relations (also within international groups) for transparency and set out the considerations underlying a cooperation relationship in concrete terms.

The services generally cooperate with foreign services on the basis of the principle of *quid pro quo* or reciprocity. The basic principle is, simply stated, 'one good turns deserves another' and this is a maxim applying in the world of intelligence and security.[53] When GISS and DISS *provide* data or *render* support, the requirements for providing (personal) data and exercising special powers laid down in the ISS Act 2002 apply.[54] In sections 5.4 - 5.6 the Committee reviews to what extent the provision by GISS and DISS of collections of (raw) data and support in the context of a number of existing close cooperation relationships was done lawfully. When GISS or DISS *receives* data or support, the legal assessments they must make pursuant to the ISS Act 2002 are more limited. The Committee will discuss this aspect in section 5.2.

In sections 5.4 – 5.6 the Committee will discuss a number of cooperation relationships in general terms, without compromising the secrecy of sources, the current level of knowledge and/or the procedure of the services. In the secret appendices to this review report the Committee gives a more detailed account of its findings regarding a number of (categories of) cooperation relations. The Committee draws attention to the fact that this review report and the secret appendices do not aim at presenting an exhaustive overview of the existing cooperation relations.

5.2 GISS and DISS: receiving data and support

When GISS and DISS receive data or support, their legal task under the ISS Act 2002 is a limited one. The Parliamentary Papers relating to the Act show that in this situation it is the responsibility of the foreign service providing the data to ensure that it has been collected lawfully.[55] The foreign service is expected to respect the parameters of its own legal framework. Without concrete indications to the contrary, GISS and DISS may therefore assume that the relevant legislation and regulations have been complied with. In the case of

---

[51] Article 59 ISS Act 2002 imposes a responsibility on the heads of GISS and DISS to maintain relations with foreign services qualifying for such relations.

[52] CTIVD review report no. 22a on the cooperation with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), available at www.ctivd.nl, sections 5.1 and 6.1.

[53] CTIVD review report no. 22a on the cooperation with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), available at www.ctivd.nl, section 5.5.

[54] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 62; see also the legal appendix to this review report, sections VI.2 andVI.4

[55] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 62.

close cooperation relationships this means that GISS and DISS have already established in general that these foreign services satisfy the criteria for cooperation, including the requirements of democratic anchorage and respect for human rights. GISS and DISS must, in their turn, observe the law of the Netherlands when they *request* a foreign service to provide information or support, or when they want to *use* data they have received. This means that prior to making a request for certain data or support, they must assess to what extent the provision of the desired data or support satisfies the requirements of necessity, proportionality and subsidiarity. GISS and DISS are not permitted to request a foreign service to exercise a power which the Dutch services may not exercise themselves (sidestepping legal restrictions). In addition, the services must refrain from using data which they know or suspect to have been acquired by the foreign service while using a method which unlawfully infringes a fundamental right (see the legal appendix to this review report, sections VI.3 and VI.4).

The Committee draws attention to the fact that unlike GISS and DISS, some foreign services have the power of untargeted interception of cablebound telecommunications. For them, this falls under the definition of sigint. The question arising in this context is whether GISS and DISS, when they cooperate with these services in the field of sigint, are thereby sidestepping legal restrictions since it enables them to get access to data collected by the exercise of a power they cannot exercise themselves. Relevant factors are on the one hand that GISS and DISS may be aware that in the context of such cooperation they also receive data acquired by untargeted interception of cablebound telecommunications, since this cannot be excluded in advance. And on the other hand that GISS and DISS do not explicitly ask for such data, but that it is the providing foreign service which applies a broad definition of sigint. The Committee suggests on this point that the fact that the ISS Act 2002 does not provide for the power of untargeted interception of cablebound telecommunications does not in itself mean that such interception constitutes unlawful infringement of privacy. The fact is that the ISS Act 2002 grants GISS and DISS a similar power with respect to non-cablebound telecommunications. The drafting process of the ISS Act 2002 did not include an express constitutional assessment of the difference between cable-bound and non-cablebound telecommunications. Besides, it cannot be said beforehand that cable-bound interception, if accompanied by the same safeguards that apply to non-cablebound interception, is in itself contrary to the ECHR or other human rights conventions. Given this context the Committee holds that it is permitted for GISS and DISS to cooperate with these foreign services, even if it cannot be excluded that they will receive data obtained by untargeted interception of cablebound telecommunications.

The Committee has not found any indications in the course of its investigation that GISS and DISS explicitly requested foreign services to use methods which are unlawful under Dutch law.

5.3 Activities of foreign services within the territory of the Netherlands

In the Netherlands, foreign intelligence and/or security services require the permission of the minister of the Interior and Kingdom Relations to engage in intelligence activities within the territory of the Netherlands. Activities in places used by the ministry of Defence require the permission of the minister of Defence. It is emphasized in the legislative history of the ISS Act 2002 that the Act provides that GISS and DISS are exclusively authorised in the Netherlands and sets out the conditions under which they may exercise their authority. This means that it can be ruled out that a foreign intelligence and security service will be

permitted to engage in intelligence activities in the Netherlands on its own and independently.[56]

If a foreign service is granted permission to engage in activities within the territory of the Netherlands, it must do so under the responsibility of the minister and under the direction of the Dutch service. Such an operation is always considered a joint operation with the foreign service acting as an equal partner. Furthermore, it is the duty of the Dutch service to supervise the activities of the foreign colleague and to verify whether these activities satisfy the applicable conditions.[57]

The Committee expressly included cooperation relationships in the fields of sigint and cyber in its investigation. It did not find any indications that foreign services had gained independent access to Dutch telephone or internet connections with the cooperation of GISS or DISS.

5.4 The provision by GISS and DISS of metadata relating to specific issues

Within a particular international collaboration group in which GISS and DISS participate, the participating services share, on a structural basis, (raw) metadata obtained by untargeted interception relating to issues jointly agreed upon between the participants.

The Committee has found that DISS filters out all Dutch numbers from the list before sharing the data. GISS stated that it did not do this because the service primarily acquires and shares IP metadata, and because it is not possible in the case of such metadata to establish with certainty whether a number is a Dutch number.

The Committee has established that the provision of metadata within this international collaboration group is based on article 36 ISS Act 2002. Pursuant to this article the services are authorised, for the purpose of the proper performance of their tasks, to provide data to foreign services qualifying for such data sharing. This means that the provision must be necessary for this purpose and that the requirements of propriety and due care must be satisfied (see the legal appendix to this review report, section IV.1). The Committee holds the opinion that these data provisions satisfied the requirement that they were necessary for the proper performances of the service's task. For assessing the propriety of the data provision it is relevant that this metadata may include personal data and that its provision may consequently constitute privacy infringement. This must be taken into consideration when assessing whether the means chosen by the service was proportional to the purpose (an element of propriety). In the case of these exchanges of data the Committee holds the opinion that the purpose of the data provision outweighed its possible infringement of the privacy of the persons concerned. In this context the statutory requirement that data processing must be done with due care refers among other things to the accuracy of the data provided and to the fact that the considerations underlying the decision to provide the data must be recorded. The Committee notes that it has no indications that the services have not been acting with due care.

Consequently, it is the opinion of the Committee that the procedure followed by GISS and DISS for the structural exchange of data discussed above is lawful.

---

[56] *Parliamentary Papers I* 2001/02, 25 577, no. 58a, p. 25.
[57] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 64.

5.5 The exercise of the power to select by DISS on behalf of counterpart services.

Within an international cooperation relation, so the Committee has found, DISS exchanges collections of (raw) metadata obtained from untargeted interceptions of non-cablebound telecommunications with cooperation partners, doing so on a structural basis.

On an earlier occasion the Committee already took the position that rather than constituting data provision, this is a form of rendering technical support within the meaning of article 59 ISS Act 2002 (see the legal appendix to the review report, section VI.4).[58] The Committee holds that DISS is using a special power in this case, namely the power to select data obtained by untargeted interception, on behalf of partner services.

Any rendering of technical support to a foreign service must satisfy a number of requirements. First of all there is the condition that the interests protected by the cooperation partners must not be incompatible with the interests protected by DISS and the condition that rendering the support may not be incompatible with the proper performance of its task by DISS. The Committee has found no indications that these conditions were not satisfied.

Pursuant to the law, moreover, assistance may only be rendered with the permission of the minister concerned. In the case under consideration the Committee has not established whether the minister granted permission to render technical assistance. The Committee points out to DISS that there must be some form of evidence that the minister agreed to this form of cooperation, without which the requirement of the ISS Act 2002 is not satisfied.

It is particularly essential for the protection of privacy that any exercise of special powers for the purpose of supporting a foreign service is done in accordance with the ISS Act 2002 and that the requirements set by this Act are satisfied (see the legal appendix to this review report, sections VI.4 and III). This means that the requirements of necessity, proportionality and subsidiarity must be satisfied, too, before DISS may provide support. The Committee has found that DISS does not consider the selection of data obtained by untargeted interception on behalf of its cooperation partners to be selection within the meaning of the Act. For this reason, it does not make an application substantiated by reasons to the minister for each individual characteristic. The Committee holds the opinion that the current procedure at DISS is not in conformity with the ISS Act 2002 and does not implement the safeguards embodied in the law. Consequently, this procedure is unlawful. The Committee recommends that DISS adjusts its procedure without delay so that henceforth the minister will be asked to grant permission for exercising the power to select on the basis of an application stating reasons, supported by the available information.

5.6 The exchange of web forums by GISS

GISS exchanges web forums with a number of foreign services in bilateral or trilateral relations. The Committee has established that the provision of a web forum constitutes sharing a collection of (personal) data. It relates to communication content as well as metadata. GISS provides web forums in the context of the proper performance of its task and based on the ISS Act 2002. In this connection the Committee takes the ground that providing a web forum is only permissible if doing so is necessary for the proper performance of the

[58] CTIVD review report no. 28 on the use of Sigint in the use of Sigint by DISS, *Parliamentary Papers II* 2011/12, 29 924, no. 74 (appendix), available at www.ctivd.nl, section 9.3.

task of GISS and if it can be deemed proper to provide the data of all the persons concerned. In addition, the data provision must satisfy the requirement of due care, which in this context refers among other things to the accuracy of the data provided and to the fact that the considerations underlying the decision to provide the data must be recorded. The Committee has found that in virtually all cases the web forums shared by GISS are forums exclusively containing data of persons who give rise, by the goals they pursue or by their activities, to the serious suspicion that they constitute a danger to the continued existence of the democratic legal system, or to the security or other vital interests of the state. With respect to the provision of such web forums generally the Committee finds that this may be necessary for the purpose of the proper performance of the service's task and can be deemed proportional to the objective pursued thereby (an element of propriety). The Committee has not found any indications that these provisions of web forums did not satisfy the requirement of due care.

The Committee is currently assessing the lawfulness of the provision of web forums in concrete cases as part of its investigation into the investigative activities of GISS on social media. The review report concerning this investigation is expected to be presented to the minister in early April 2014.

6 Conclusions and recommendations

The acquisition of telecommunications data by GISS and DISS

Wire-tapping and internet interception (section 3.2)

Pursuant to article 25 ISS Act 2002 the services are authorised to intercept any form of telecommunications by targeted interception. Wire-tapping telephone calls and intercepting Internet traffic is done by both services on the basis of approval orders: permission of the minister concerned to listen to or intercept the telephone or Internet traffic from and to a specified telephone number or IP address (or several numbers/IP addresses) belonging to a specified person or organisation. The Committee has established that the wire-tapping and Internet interception activities do not include any untargeted acquisition of (collections of) data.

Interception and selection sigint (section 3.3)

GISS and DISS do not have the power of untargeted interception of cable-bound telecommunications. The Committee has established that the activities of GISS and DISS do not include any untargeted interception of cable-bound telecommunications.

GISS and DISS do have the power to collect and record non-cablebound telecommunications by untargeted interception (article 27 ISS Act 2002). The power covers both communication content and metadata. Only part of the communication content is selected for examination on the basis of selection criteria approved by the minister, and used in the intelligence process.

The metadata of the communications collected by untargeted interception is analysed by the services (metadata analysis). Part of this data constitutes personal data. The processing of this data therefore constitutes an infringement of privacy. For this reason it is important that the procedure for metadata analysis will be made subject to statutory safeguards to protect

against unlawful infringement of privacy, for example the requirement to substantiate the necessity, proportionality and subsidiarity of processing the metadata in an application for internal or external permission. This is not the case at present. The Committee recommends enacting specific rules on processing metadata.

Based on the results of metadata analysis DISS searches communication content for new investigation targets. DISS holds that this procedure falls under the power to search (article 26 ISS Act 2002). In an earlier review report the Committee has already stated that in its opinion this procedure is unlawful, because in this form of searching the infringement of privacy is not overcome by the minister's permission to exercise the power of selection with respect to the person or organisation in question. The procedure for searching at GISS will be further discussed in the Committee's ongoing investigation into the use by GISS of the power to tap and the power to select sigint. The review report on this investigation covering the period from September 2012 up to and including August 2013 is expected to be presented to the minister in early April 2014.

In earlier review reports the Committee already established that both GISS and DISS did not state sufficient reasons for using the power to select. The criticism related to the fact that the reasons stated for selection were not sufficiently focused on the persons and/or organisations included in the selection list.

Human sources (section 3.4)

The services may use human sources to acquire telecommunications data (article 17 or 21 ISS Act 2002). The Committee has established that human sources deployed by GISS performed activities that are similar to the power to wire-tap or intercept conversations, telecommunications and/or data transfers (article 25 ISS Act 2002) and to the power to hack (article 24 ISS Act 2002). For the purpose of privacy protection the service must, in addition to the assessment concerning the deployment of the human source, also assess the nature of each individual activity and which type of data will be acquired by it. They must do so among other things to determine whether the human source will exercise any special power, for which specific permission is required.

The Committee holds the opinion that the protection of privacy can only be adequately guaranteed if emphasis is placed on the nature of the activity and the type of data acquired, as far as possible regardless of the means used to acquire the data (deployment of the human source).

So far GISS has not, in cases where this would have been appropriate, stated separate reasons for activities by a human source that must be deemed to constitute wire-tapping (article 25 ISS Act 2002) or hacking (article 24 ISS Act 2002). Nor was permission granted for these activities at the required level. The Committee holds that this procedure is unlawful as far as it concerns activities that are comparable with wire-tapping, because it does not meet the statutory requirement that the minister's permission must be obtained for wire-tapping. In the case of activities that must be deemed to constitute hacking the Committee holds that GISS' procedure is not automatically unlawful, in particular because the level of permission required for these cases follows from the GISS Special Powers Mandate Decision 2009 which was adopted internally at GISS. It will have to be assessed in concrete cases whether GISS acted lawfully. To this end it must be determined whether GISS sufficiently substantiated the necessity, proportionality and subsidiarity of the hacking. This is being examined in the Committee's ongoing investigation of the investigative activities of GISS on social media.

The review report on this investigation is expected to be presented to the minister in early April 2014.

The Committee recommends that GISS adjusts its procedure without delay by henceforth applying for permission at the prescribed level and by stating separate reasons for the exercise of special powers by human sources, in addition to the reasons for deploying the human sources in question.

Hacking (section 3.5)

GISS and DISS have the power to acquire data by gaining access to a computerised device or system, which is known as hacking (article 24 ISS Act 2002). The law does not require the minister's permission for hacking. For the purpose of internal permission the services must indicate, stating reasons, which computerised device or system is to be hacked and what data the service aims at acquiring by the hack.

The Committee has established that GISS sometimes formulates applications for permission to hack broadly because prior to a hack it has only limited insight into the data it may find. The protection of privacy requires, however, that applications substantiate as specifically as possible what data a hack is targeting. Only then is it possible to make a full assessment of the necessity, proportionality and subsidiarity of the intended exercise of the power. When the acquiring department comes across data in the course of a hack that is not covered by the permission but which is relevant to the investigation, it can still – via a fast-track procedure – ask permission to copy this data.

When GISS exercises the power to hack there are certain cases in which it takes note of streaming telecommunication within the meaning of 25 ISS Act 2002. This means that GISS is in fact exercising the power to tap. It is the opinion of the Committee that failure to obtain the minister's permission in such cases makes the hacking unlawful. It recommends that GISS, without delay, brings its procedure into line with the statutory requirement that permission must be obtained from the minister of the Interior and Kingdom Relations whenever hacking will result in the examination of streaming telecommunication within the meaning of article 25 ISS Act 2002.

For DISS there are cases in which it is not possible to name specific persons in the application for permission to hack. The applications for permission are substantiated by reference to known data relating to the digital activities linked to a specific technical characteristic. It is the opinion of the Committee that this procedure is not unlawful. It recommends that if the data concerning the identity of the user or users of the technical characteristic becomes known, DISS will immediately add the data to the reasons already stated and communicate it to the minister.

GISS uses hacking to acquire entire web forums. Web forums contain collections of personal data, including communication content. It concerns stored telecommunication and not streaming telecommunication within the meaning of article 13 Constitution. With regard to the acquisition of web forums whose participants must all be considered – in advance – to be (potential) investigation targets of GISS it can generally be argued that in principle such acquisition falls under the performance of its task by GISS and will readily satisfy the requirements of necessity, proportionality and subsidiarity. This is different in the case of web forums which, in addition to the data of (potential) investigation targets, also contain the data of persons who cannot be considered such targets. It is true that the acquisition of

these web forums may be necessary for the performance of GISS' task, but it will only be proportional to acquire communication content of persons who do not give cause for doing so from the perspective of national security, if there are compelling operational interests for such acquisition. The lawfulness of hacking web forums in concrete cases will be assessed as part of the Committee's current investigation into the investigative activities of GISS on social media. The review report on this investigation is expected to be presented to the minister in early April 2014.

Separate applications to the unit director for permission to acquire a specific web forum are present only with respect to web forums which GISS acquired by using the power to hack (article 24 ISS Act 2002). In addition to this source, however, GISS also acquires web forums from foreign services. In those cases no reasoned assessment is laid down in writing why it is lawful to examine the content of the web forum. The Committee recommends that when GISS acquires web forums, it will in all cases assess, for the purpose of its (internal) permission procedure, whether examination of the content of the web forum in question satisfies the requirements of necessity, proportionality and subsidiarity. This assessment must, moreover, be laid down in writing.

Telephony traffic data and user data (section 3.6)

GISS and DISS are authorised to demand access to telephony traffic data at telecom providers (article 28 ISS Act 2002) and access to user data at CIOT (article 29 ISS Act 2002). Pursuant to article 28(4) ISS Act 2002 demanding access to telephony traffic data must be done by the head of the unit. The law permits the head of the service to mandate his authority in regard to demands for access to user data based on article 29 ISS Act 2002. There is no legal requirement to state reasons for demanding access to this data. However, the services do make internal applications for permission substantiated by reasons. Since the use of the powers is focused on a specific investigation target, there is no question of demanding untargeted access to (collections) of telephony traffic data and/or user data. The telephony traffic data acquired is shared in whole or in part between GISS and DISS. Such sharing satisfies all the applicable statutory requirements.

The use of telecommunications data by GISS and DISS

Storing telecommunications data and making it accessible (section 4.1)

A distinction is made between raw data and evaluated data. Raw data has not yet been evaluated for its relevance to the purpose for which it was acquired, or to another ongoing investigation of the service. Pursuant to the law raw data acquired by untargeted interception may be stored for one year for the purpose of subsequent selection (article 27(9) ISS Act 2002). The Act does not prescribe a maximum storage period for other raw data acquired by the exercise of special powers, such as wire-tapped data or data collections acquired by hacking. For the purpose of privacy protection the Committee considers it important that further rules be included in the law regarding the maximum storage period of raw data in other cases. It recommends that this issue be addressed in the forthcoming amendment of the ISS Act.

The general procedure at GISS and DISS for making accessible raw data acquired by the exercise of special powers is consistent with the statutory requirements regarding internal access. Employees are given access to data to the extent necessary for the proper performance of their tasks (article 35 ISS Act 2002). The heads of the services ensure that the

necessary security measures are in place to protect against unauthorised data processing (article 16 under b, ISS Act 2002).

Analysis of telecommunications data (section 4.2)

The Committee holds the opinion that the raw data acquired by special powers may only be used for the purpose of the investigation in the context of which the data was acquired or for the purpose of another ongoing investigation within the scope of the intelligence or security tasks of the services (see article 18 ISS Act 2002). This rule limits the infringement of privacy resulting from the use of special powers. Once data has been evaluated, it may subsequently be used for all tasks of the services (also, therefore, for other tasks than the intelligence and security tasks).

GISS uses applications which give access, for analysis purposes, to combined metadata originating from various sources, including metadata acquired by the use of special powers. The Committee holds the opinion that the use of combined metadata is lawful insofar as the analysis takes place for the purpose of ongoing investigations falling within the scope of the intelligence or security tasks of GISS. This means that such combined metadata may only be used for the service's intelligence and security tasks and not for other tasks.

Use by GISS of data from web forums (section 4.3)

Web forums are usually stored and remain available within GISS. The Committee considers this an onerous means, especially in the case of forums of which not all participants can be deemed in advance to be (potential) investigation targets. The means must be proportional to its operational goal. The lawfulness of storing web forums in concrete cases is being assessed in the context of the Committee's current investigation into the investigative activities of GISS on social media. The review report on this investigation is expected to be presented to the minister in early April 2014.

The exchange of telecommunications data with foreign intelligence and security services by GISS and DISS

Cooperation relationships with foreign intelligence and security services (section 5.1)

The exchange of collections of (raw) data takes place within close cooperation relationships based on mutual trust. It is not customary in international dealings to inquire about the source or method used to collect data, nor to provide information on the matter.

The Committee has established that in the close cooperation relationships it reviewed GISS and DISS trust to a considerable extent that the foreign services in question respect human rights and act within the parameters of their own national regulatory framework. It is the opinion of the Committee that in the light of the recent disclosures it is desirable to verify whether such trust is still justified. Pursuant to the law[59] it is the duty of the heads of GISS and DISS, under the political responsibility of the minister concerned, to assess whether foreign services still qualify for the various forms of cooperation which take place in the

[59] Article 59 ISS Act 2002 imposes a responsibility on the heads of GISS and DISS to maintain relations with foreign services qualifying for such relations.

context of a close cooperation relationship.[60] In practice this means that they must make further inquiries into the statutory powers and (technical) possibilities of foreign services in order to be able to make well-considered assessments. In regard to this issue the Committee recommends that the ministers of the Interior and Kingdom Relations and of Defence assess the cooperation relationships (also within international groups) for transparency and set out the considerations underlying a cooperation relationship in concrete terms.

International cooperation usually takes place on the basis of the principle of *quid pro quo* or ´one good turn deserves another'. GISS and DISS are authorised to provide data or support. When they do so the requirements for providing (personal) data and exercising special powers laid down in the ISS Act 2002 apply. GISS and DISS may also receive data or support. The legal assessment they must make pursuant to the ISS Act 2002 in this situation is more limited.

GISS and DISS: receiving data and support (section 5.2)

Some foreign services have the power to use untargeted interception also with regard to cable-bound telecommunications. GISS and DISS do not have this power. The question arising in this context is whether GISS and DISS, when they cooperate with these services in the field of sigint, are thereby sidestepping legal restrictions since it enables them to get access to data collected by the exercise of a power they cannot exercise themselves. The Committee holds the opinion that such interception does not in itself constitute unlawful infringement of privacy. The fact is that the ISS Act 2002 confers a similar power on GISS and DISS with respect to non-cablebound telecommunications. The drafting process of the ISS Act 2002 did not include an express constitutional assessment of the difference between cable-bound and non-cablebound telecommunications. Given this context the Committee holds that it is permitted for GISS and DISS to cooperate with these foreign services, even if it cannot be excluded that they will receive data obtained by untargeted interception of cable-bound telecommunications.

The Committee has not found any indications in the course of its investigation that GISS and DISS explicitly requested foreign services to use methods which are unlawful under Dutch law.

Activities of foreign services within the territory of the Netherlands (section 5.3)

The ISS Act 2002 only permits foreign services to engage in activities within the territory of the Netherlands if the minister responsible has granted permission and if they do so under the supervision and responsibility of GISS or DISS. The Committee has found no indications that foreign services gained independent access to Dutch telephone or Internet connections with the cooperation of GISS or DISS.

The exchange by GISS and DISS of metadata relating to specific issues (section 5.4)

Within an international collaboration group GISS and DISS share (raw) metadata on a structural basis. This metadata has been obtained by untargeted interception of non-cablebound telecommunications and may include personal data. This means that there is

[60] CTIVD review report no. 22a on the cooperation with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), available at www.ctivd.nl, sections 5.1 and 6.1.

potential infringement of privacy. The Committee holds the opinion that the provision of metadata within this collaboration group satisfies the statutory requirement of necessity for the purpose of performing the tasks of the services. Moreover, the purpose of the data provision outweighs its possible infringement of privacy. In addition, the Committee has no indications that the services are not acting with due care. It is the opinion of the Committee that the procedure followed by GISS and DISS for this structural exchange of data is lawful.

The exercise of the power to select by DISS on behalf partner services (section 5.5)

DISS provides support to foreign services by exercising the power to select with respect to non-cablebound communications acquired by untargeted interception. DISS does not, however, consider the support to be selection. For this reason it does not apply for the minister's permission, substantiated by reasons, for each individual characteristic. The protection of privacy requires that the safeguards embodied in the ISS Act 2002 are implemented when the service exercises special powers, also when it exercises them to support a foreign service. In the opinion of the Committee the current procedure at DISS is unlawful. It recommends that DISS adjusts its procedure without delay so that henceforth the minister will be asked to grant permission for exercising the power to select on the basis of an application stating reasons, supported by the available information.

The exchange of web forums by GISS (section 5.6)

GISS exchanges web forums with a number of foreign services. Web forums contain collections of personal data so that such exchanges constitute infringement of privacy. In virtually all cases the web forums are forums which exclusively contain data of (potential) investigation targets of the service. With respect to the provision of such web forums generally the Committee finds that this may be necessary for the purpose of the proper performance of its task by GISS and can be deemed proportional to the goal served thereby. The Committee has not found any indications that GISS is not acting with due care.

The lawfulness of the provision of web forums in concrete cases is being assessed as part of the Committee´s current investigation into the investigative activities of GISS on social media. The review report concerning this investigation is expected to be presented to the minister in early April 2014.

Thus adopted at the meeting of the Committee held on 5 February 2014.

CTIVD nr. 38

APPENDIX

Legal framework for data processing

Belonging to the public review report on the processing of telecommunications data by GISS and DISS

I Introduction

In essence, the activities of GISS and DISS focus on data processing, both personal data[61] and other data.[62] Data processing is a broad concept. For the purpose of the law regulating the activities of the services, the Intelligence and Security Services Act 2002 (ISS Act 2002), it means collecting, recording, arranging, storing, updating, altering, retrieving, consulting or using data, providing data by forwarding or disseminating it or by any other means, assembling or combining data, and protecting, deleting or destroying data.[63] When the services process data for the purpose of their investigations, this essentially takes the form of collecting data, and of analysing and, in some cases, providing that data to external parties.. The performance of data-processing activities, particularly the collection of data by exercising special powers, may directly infringe fundamental rights of individuals who are usually unaware of this infringement because of the secret nature of the activities. The processing of personal data always infringes the privacy of the investigated persons to a greater or lesser extent. When enacting the ISS Act 2002 the legislator aimed at creating a balance between the interest of national security and the tasks and powers of the services on the one hand, and the interest of protecting fundamental rights (which protect individuals from too far-reaching government intervention) and democratic control over the operations of the services on the other hand.

In this context the Committee draws attention to the evaluation of the ISS Act 2002 by an evaluation committee established for this purpose: the Dessens Committee. The report of this committee was presented to the ministers concerned in early December 2013.[64] In the report the Dessens Committee proposes to reinforce both the powers of the services in the field of cablebound communications in line with technological developments and the review of the lawfulness of the services' activities by the Review Committee for the Intelligence and Security Services (CTIVD). The Committee merely refers to the report here.

---

[61] Article 1(e) ISS Act 2002 defines personal data as data relating to an identifiable or identified individual natural person.

[62] For the purpose of this Appendix the term "data" refers to personal data and other data. The term refers to both individual data and collections of data.

[63] Article 1(f) ISS Act 2002.

[64] Report of Dessens Committee, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, December 2013, *Parliamentary Papers II* 2013/14, 33 820, no. 1 (appendix).

This appendix has the following structure. It starts with a description of the making of the ISS Act 2002 and the human rights considerations underlying the drafting process. This includes an explanation of how the protection of human rights, in particular the right to respect for privacy and the privacy of the telephone and telegraph, are regulated in the European Convention on Human Rights (ECHR) with corresponding case law and in the Dutch Constitution (section II). Next, it sets out the safeguards embodied in the ISS Act 2002 that ensure the protection of these fundamental rights of individuals (section III). Following the arrangement of the ISS Act 2002, section IV then deals with the services' general power to process data and the requirements set by law for data processing. This is followed by a discussion of two specific forms of data processing. The first concerns the deployment of the general and special powers conferred by law on the services to collect data in the interest of national security and the restrictions and conditions applying in such deployment, with a separate section being devoted to the special powers in the field of telecommunications (section V). The final section (section VI) deals with the cooperation of GISS and DISS with foreign intelligence and/or security services

II Privacy versus intelligence & security

II.1 Drafting the ISS Act 2002

The current ISS Act 2002 has its origins in two decisions of the Administrative Jurisdiction Division of the Council of State (further referred to as Administrative Jurisdiction Division) in 1994, in which the Intelligence and Security Services Act 1987 in force at the time was found to violate articles 8 and 13 of the ECHR.[65] The right to respect for privacy is enshrined in article 8 ECHR. Article 13 ECHR provides that everyone who has a plausible claim that his fundamental rights have been violated is entitled to an effective remedy before a national authority. In its case law the European Court for Human Rights (ECtHR) has laid down the requirements following from these rights. There are a number of judgments that relate to secret surveillance by intelligence and security services. In summary, the purport of this case law is:
1) that a system allowing secret surveillance of persons must provide for sufficient statutory safeguards, for example the requirements of clarity and foreseeability in the sense that citizens must be able to understand the circumstances and the conditions under which the authorities may exercise a particular power (article 8)[66], and
2) that it is true that the secrecy of the work of intelligence and security services entails restrictions on the oversight of their work, but that at the national level a system (not necessarily a legal system) must exist which taken as a whole sufficiently guarantees the availability of an effective remedy against possible infringements of human rights resulting from secret surveillance by intelligence and security services (article 13).[67]

Following this case law the Administrative Jurisdiction Division ruled that it was true that the ISS Act in force at the time (1987) contained provisions designating the persons or categories of persons with respect to whom or which data processing (secret surveillance) was permitted, but that the circumstances under which this was permitted and the means

[65] ABRvS 9 June 1994, *Van Baggum & Valkenier*, AB 1995/238.
[66] ECtHR 26 April 1979, *Sunday Times v United Kingdom*, §49; ECtHR 25 March 1983, *Silver a.o. v United Kingdom*, §85; ECtHR 2 August 1984, *Malone v United Kingdom*, §68; ECtHR 24 April 1990, *Kruslin v France*, §§33 and 35; ECtHR 24 April 1990, *Huvig v France*, §§32 and 34.
[67] ECtHR 6 September 1978, *Klass a.o. v Germany*, §67; *Silver a.o. v United Kingdom Koninkrijk*, §113.

that were available for this purpose were insufficiently regulated in the Act. For this reason, so the Administrative Jurisdiction Division held, the legal system did not satisfy the requirement of article 8(2) ECHR that there shall be no infringement of the privacy of citizens except as provided for by law. In addition the Administrative Jurisdiction Division ruled that there was no effective remedy in the Netherlands within the meaning of article 13 ECHR against violations of fundamental rights resulting from secret surveillance by the then intelligence and security services. The Administrative Jurisdiction Division held that the supervisory mechanisms existing at the time, particularly the complaints procedure before the National ombudsman and the parliamentary oversight by the standing parliamentary committee for the Intelligence and Security Services (ISS Committee), were inadequate to constitute an effective remedy because the National ombudsman had no authority to issue binding decisions and because parliamentary oversight would only satisfy the requirements arising from the ECHR if this safeguard was regulated by law, if such statutory regulation satisfied the requirements laid down in article 8(2) ECHR, and if there was a system in place ensuring that a person who had been investigated would at some point be informed of the fact that he had been a surveillance target. In response to the rulings of the Administrative Jurisdiction Division the Cabinet took a position on the issue.[68] In 1998 it presented a legislative proposal for a new Act to the Second Chamber.[69] The new Act, which came into force in May 2002, met the criticism of the Administrative Jurisdiction Division by demarcating and defining the circumstances under which surveillance of specific categories of persons is permitted for the purpose of data processing, by laying down and describing the special powers that may be deployed for such surveillance – subject to specific conditions – and by establishing a specialised and independent oversight body. One factor in the legislative process was that it largely happened in a period in which emphasis was placed more on extending safeguards and supervision than on extending the powers of the services.[70] The legislator thus aimed at properly reconciling and striking a balance between the interests of intelligence and security on the one hand and the interest of respecting fundamental rights (particularly the right to privacy) on the other hand in the ISS Act 2002.

II.2 Case law of the ECtHR on article 8 and intelligence and security services[71]

A great deal can be said about the case law of the ECtHR on article 8 ECHR, particularly because of the large number of judgments and the broad interpretation given by the ECtHR to the rights under this article. Because the subject of the investigation underlying this report is so closely linked to the rights under article 8 ECHR, in particular the right to protection of private life, the Committee has chosen to give an outline description of the case law of the ECtHR on the subject. It specifically examined the judgments in which the ECtHR gave rulings on two issues: in which cases does secret surveillance by an intelligence and/or security service interfere with the right to privacy, and under which conditions can such interference be justified on the grounds of the interests of national security.

II.2.1 Interference

Article 8(1) ECHR provides that everyone has the right to respect for his private and family life, his home and his correspondence. The elements are mentioned separately but they

---

[68] *Parliamentary Papers II* 1994/95, 22 036, no. 6.
[69] *Parliamentary Papers II* 1994/05, 25 877, no. 2.
[70] H.T. Bos-Ollermann, '*Meerdere wegen naar Straatsburg. Geheime methoden en toezicht op de inlichtingen- en veiligheidsdiensten in België en Nederland*', in *De orde van de dag*, issue 56 (Dec. 2011), p. 100.
[71] The judgments of the ECtHR are available at www.echr.coe.int via the browser HUDOC.

clearly interact since they follow naturally from each other while there is also a certain measure of overlap. A telephone tap may constitute interference with a person's privacy as well as with his correspondence, and maybe even with his home.[72] An important factor for holding article 8 ECHR to be applicable is whether an alleged infringement falls within the scope of (one or more of) the rights protected by this article, in other words whether there is interference with these rights. The article does not give any definitions. Case law, however, gives a better understanding of the interpretation given by the court to the rights protected by article 8.

It can be inferred from the rulings relating specifically to secret surveillance by an intelligence and/or security service for the purpose of national security that in those cases the ECtHR will readily find interference with the rights of the investigated persons mentioned in article 8 ECHR. The ECtHR proceeds on the assumption that the mere existence of legislation that permits a system of secret surveillance and interception of telecommunications constitutes interference with the exercise of the rights arising from article 8 ECHR by persons to whom the legislation may apply, apart from the question whether a power or means has actually been deployed.[73] In this context a factor that must be taken into account is whether a national remedy is available to challenge the use of the powers in question.[74] The ECtHR has brought various forms of (tele)communications within the scope of the right to respect for private life and correspondence, not only communication content such as telephone calls, postal items, facsimile and e-mail communications[75], but also traffic data, i.e. data which do not relate to communication content.[76] The ECtHR has also brought the storage in secret government data bases of data relating to a person's private life

---

[72] C. Ovey & R. White, *Jacobs & White The European Convention on Human Rights (4th Edition)*, Oxford: Oxford University Press 2006, p. 242.

[73] *Klass a.o. v Germany*, §41; *Malone v United Kingdom*, §64; ECtHR (Dec.) 29 June 2006, *Weber and Saravia v Germany*, §§77-78; ECtHR 1 July 2008, *Liberty a.o. v United Kingdom* §56; ECtHR 25 May 2011, *Association "21 Decembre 1989" a.o. v Rumania*, §114.

[74] ECtHR 18 May 2010, *Kennedy v United Kingdom*, §124.

[75] *Klass a.o. v Germany*, §41; *Malone v United Kingdom*, §64; *Weber and Saravia v Germany*, §§77-78; *Liberty a.o. v United Kingdom,* §56; *Association "21 Decembre 1989" a.o. v Rumania*, §114.

[76] The complaint in *Malone v United Kingdom* was about the wiretapping of the complainants telephones calls and the monitoring of the numbers he dialled. In regard to the latter issue the ECtHR found: "(…) a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Art. 8. The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Art. 8." (§84). The complaint in ECtHR 3 April 2007, *Copland v United Kingdom* was about the monitoring of the complainant's telephone calls and e-mail and Internet usage by her employer at her work place. Referring to *Malone,* the ECtHR found that "the use of information relating to the date and length of telephone conversations and in particular the number dialled can give rise to an issue under article 8 as such information constitutes an "integral element of the communications made by telephone"(…). The collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence." (§43).

within the scope of article 8.[77] According to the ECtHR public data may become part of private life if the data is systematically collected and stored in government files.[78] With regard to forms of interception the ECtHR has not only ruled on the targeted collection of data concerning persons, but also on the collection and recording of telecommunication data acquired by untargeted interception (known as *strategic monitoring*)[79] and on the untargeted interception of telephone calls, facsimile and e-mail and subsequent selection thereof using search terms or selection criteria.[80] According to the ECtHR the existence of certain powers, particularly those permitting the examination, use and storage of intercepted communications, may constitute interference with the exercise of the rights under article 8 ECHR.[81] The further provision of the intercepted personal data to others may also result in a separate interference with the exercise of the rights under article 8 ECHR.[82]

II.2.2 Justification of interference

It is true that article 8 ECHR prohibits all interference by public authorities with the exercise of the rights mentioned in this article, but pursuant to the second paragraph interference can be justified to the extent it is in accordance with the law and is necessary in a democratic society in the interests of *inter alia* national security. These conditions have been further elaborated in the extensive case law of the ECtHR on article 8 ECHR. The main features are as follows.

First, there must be a basis for the interference in national law, which is not restricted to formal legislation, but particularly may also include substantive law.[83] The law must also be accessible and foreseeable.[84] This means that the law on which the infringing action is based must have been adequately published or announced[85] and that the law must be sufficiently clear and precise. Given that secret surveillance entails the risk of abuse of powers, the ECtHR holds that the above applies all the more forcefully as the technology available for use in such surveillance is continually becoming more sophisticated.[86] According to the ECtHR the degree of clarity and precision required of the law depends on the particular subject matter. For this reason the law for the purpose of national security, for instance regarding the power to tap communications or to keep persons under secret surveillance, cannot give citizens the same degree of clarity and precision as laws having other objects.[87] Moreover, public authorities often have a certain margin of discretion in the former area. Sometimes, this is inevitable. The ECtHR has ruled that, with a view to the rule of law

---

[77] *Association "21 Decembre 1989" a.o. v Rumania*, §115.
[78] ECtHR 4 May 2000, *Rotaru v Rumania*, §43.
[79] *Weber en Saravia v Germany*, §4.
[80] *Liberty a.o. v United Kingdom*, §1.
[81] *Idem,* §57.
[82] *Weber en Saravia v Germany*, §79: "(…) the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Article 8 (…)."
[83] *Sunday Times v United Kingdom*, §47; *Kruslin v France*, §29; *Huvig v France*, §28.
[84] *Sunday Times v United Kingdom*, §49; *Silver a.o. v United Kingdom*, §85; *Kruslin v France*, §27; *Huvig v France*, §26.
[85] *Silver a.o. v United Kingdom*, §87; ECtHR 26 March 1987, *Leander v Sweden*, §53.
[86] *Weber en Saravia v Germany*, §93; ECtHR 2 September 2010, *Uzun v Germany*, §61; ECtHR 21 June 2011, *Shimovolos v Russia*, §68.
[87] *Malone v United Kingdom*, §67; *Leander v Sweden*, §51.

principle, the law must indicate the scope of that discretion.[88] In addition, the legal system must contain sufficient safeguards to protect citizens against arbitrariness.[89] This requires first of all that the law must in any case be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities may exercise a specific infringing power.[90] Furthermore, the ECtHR attaches importance to the presence of adequate legal remedies enabling citizens to contest alleged arbitrary interference.[91] The ECtHR has translated these basic principles into a number of minimum safeguards with respect to the targeted tapping of telecommunications (i.e. powers used against specific persons) which it has subsequently ruled to apply as well to powers of a rather more untargeted nature, e.g. the power of untargeted interception of telecommunications.[92] National law must in any case comprise rules on the nature of the activities that may give rise to interception, the categories of persons liable to have their communications intercepted, a limit on the duration of interception, the procedures to be followed for examining, using and storing intercepted data, the precautions to be taken when communicating the data to external parties and the circumstances under which data must or may be erased or destroyed.[93]

Secondly, the interference must serve a legitimate interest. The interests are listed exhaustively in article 8(2) ECHR. National security is a particularly important legitimate interest in the context of the present investigation. In principle it is left to the States themselves to make the initial assessment whether a specific interference serves a legitimate interest.[94] On this point the national authorities have a wide margin of appreciation. The concept of "national security" also features in the ISS Act 2002 as the framework within the parameters of which the services must perform their tasks. The ECtHR has not defined the meaning or scope of the term,[95] but will assess on a case-by-case basis whether a Contracting State has rightly invoked national security as a ground justifying infringement of a human right. The court has established types of threats to national security in a number of judgments. For example, national security can be threatened by espionage[96], separatist movements[97], terrorism[98], inciting to and condoning terrorism[99], publishing state secrets[100]

---

[88] *Silver a.o. v United Kingdom*, §88.
[89] *Malone v United Kingdom*, §67.
[90] *Malone v United Kingdom*, §68; *Kruslin v France*, §33 and 35; *Huvig v France*, §32 and 34.
[91] *Rotaru v Rumania*, §59.
[92] In the European Union a committee of inquiry established by the European Parliament examined the question of the potential impact of the ECHELON interception system on the rights of individuals pursuant to EU legislation and regulations. The ECHELON programme was carried out jointly by the United States, the United Kingdom, Australia, Canada and New Zealand and focused on the untargeted interception of communication traffic via satellites. The conclusion of the committee of inquiry was that: "(…) mass interception systems such as ECHELON have the potential to violate the right of privacy because they do not comply with the principle of proportionality with regard to the use of intrusive methods. While acknowledging that such interception systems may be justified on national security grounds, the committee recommends that their use be governed by clear and accessible legislation and that EU member states establish rigorous oversight"
[93] *Weber and Saravia v Germany*, §95; *Liberty a.o. v United Kingdom*, §§62 and 63.
[94] ECtHR 7 December 1976, *Handyside v United Kingdom*, §48 and 49; *Sunday Times v United Kingdom*, §59.
[95] Following the decision of the European Commission for Human Rights (ECHR) 2 April 1993, *Esbester v United Kingdom*.
[96] *Klass v Germany*, §48.
[97] ECtHR 30 January 1998, *United Communist Party of Turkey a.o. v Turkey*, §§33-36.
[98] *Klass v Germany*, §48.
[99] ECtHR 19 December 1997, *Zana v Turkey*, §§48-50.

and compromising the integrity of the civil service[101]. Case law of the ECtHR shows that secret surveillance practised by intelligence and security services in the interest of national security can be justified even if there has been no actual harm done to national security. There must, however, at least be a possibility of harm being done to national security, in other words: potential harm. If no harm to national security is to be expected at all, there is no justification for infringing privacy.[102]

Thirdly, the interference must be necessary in a democratic society. According to the case law of the ECtHR the criterion of necessity is only fulfilled if there is a pressing social need that justifies the infringement of a human right.[103] It must be assessed on a case-by-case basis whether such a need exists. The term necessity must be interpreted restrictively, which in the case of secret surveillance means that the infringement must be strictly necessary in a democratic society.[104] The means used while infringing a person's rights can only be deemed necessary if it contributes to the purpose for which it is deployed. For this to be the case the interference must be reasonably proportional to the interest which the interference is aimed at protecting.[105] The nature of the interference may not be such as to erode the essence of the infringed right. And interference is not proportional where a less infringing measure will suffice (also known as the principle of subsidiarity).[106] In accordance with the subsidiary nature of the Strasbourg mechanism, the State is left a certain margin of appreciation when deploying means in the interest of national security, provided there are sufficient safeguards against arbitrariness.[107] The assessment whether sufficient safeguards exist depends on all the circumstances of the case, including the nature, scope and duration of the power, the grounds on which deploying the power is permitted, the authorities that are competent to grant permission, to exercise the power and to supervise its exercise, as well as the legal remedy available to individuals under the national legal system.[108] In this context the ECtHR considers it important that the domestic law contains safeguards guaranteeing that data obtained by secret surveillance is destroyed as soon as it is no longer needed to achieve the intended purpose (in this context the ECtHR deems it important that a sufficiently specific objective is stated internally for the deployment of the infringing means).[109]

II.3 Protection of privacy in the Constitution

The Constitution's main rule on privacy is laid down in the first paragraph of Article 10, which contains a general provision that everyone shall have the right to respect for his privacy. This paragraph further provides that restrictions may be laid down by or pursuant to an Act of Parliament. This means that the exact scope of the protection of privacy is regulated in greater detail in other laws, such as the ISS Act 2002.

---

[100] ECtHR 26 November 1991, *Observer and The Guardian v United Kingdom*.
[101] ECtHR 12 December 2001, *Grande Oriente d'Italia di Palazzo Giustiniani v Italy*, §21.
[102] See inter alia *Klass a.o. v Germany*; *Leander v Sweden*.
[103] See inter alia *Leander v Sweden*, §58.
[104] *Klass a.o. v Germany*, §48; *Rotaru v Rumania*, §47; ECtHR 6 June 2006, *Segerstedt-Wiberg a.o. v Sweden*, §88 and *mutatis mutandis* on secret surveillance in connection with criminal law: ECtHR 2 November 2006, *Volkhy v Ukraine*, §43.
[105] *Handyside v United Kingdom*, §49.
[106] ECtHR 2 October 2001, *Hatton a.o. v United Kingdom*, §97.
[107] *Klass a.o. v Germany*, §46 and §§48-50; *Leander v Sweden*, §§59 and 60; *Malone v United Kingdom*, §81.
[108] *Weber and Saravia v Germany*, §106; *Uzun v Turkey*, §§61-63; *Shimovolos v Russia*, §68.
[109] *Klass a.o. v Germany*, §52; *Association "21 Decembre 1989" a.o. v Rumania*, §121.

Article 13 of the Constitution contains a specific elaboration of an aspect of privacy protection. It provides that the privacy of correspondence (§2) and of the telephone and telegraph (§2) is inviolable. Particularly the privacy of the telephone and telegraph is relevant to the present investigation. Restrictions on the privacy of the telephone and telegraph require the prior authorisation from a competent authority. The ISS Act 2002, for example, includes a provision that some special powers may not be deployed until permission to do so has been obtained from the minister concerned.

The privacy of the telephone and telegraph under Article 13 Constitution protects the sender of a communication transmitted via the telephone or telegraph against examination of the communication's content by the party entrusted with transmitting it or by any party having access to the communication via the transmitter. Because communication content is sometimes examined for technical reasons, the privacy rule also has the effect of prohibiting any further distribution of communication content. The privacy of the telephone and telegraph protects dedicated (private) communications. This means that the sender must have taken the necessary measures to keep his communication private. The communication is only protected during its transmission. However, everything falling outside the transmitting process and whatever is attributable to this process still enjoys the protection of the general right to privacy enshrined in article 10.[110]

Traffic data, in other words connection data concerning the transmission of communications such as times, location data, telephone numbers and IP addresses, falls outside the scope of protection of the privacy of the telephone and telegraph.[111] Traffic data does, however, enjoy the protection of article 10 Constitution to the extent it can be considered to be personal data.[112]

Guidance for deciding when traffic data is personal data is found in the Personal Data Protection Act and the legislative history. Personal data includes all data that may furnish information about an identified or identifiable natural person.[113] A person is identifiable if it is possible to find out the person's identity without disproportionate effort. In addition to the nature of the data, the capabilities (means) available to the person responsible for making the identification play a role as well.[114] Whether data contains information about a person may appear from the nature of the data (e.g. factual or assessing data relating to characteristics, views or conduct) or from the context in which the data is recorded and used. In the latter case it is important whether the data is relevant to the way in which the person concerned will be judged or treated in social life. Consequently, the (social) use made of the data is a relevant factor in determining whether the data constitutes personal data.[115] According to the explanatory memorandum to the Personal Data Protection Act, telephone numbers may under certain circumstances be part of a person's private life.[116] The ECtHR, too, has ruled in its case law that traffic data may be part of a person's private life (see for details section II.2.1).

---

[110] *Parliamentary Papers II* 1975/76, 13 872, nos. 1-5.
[111] *Parliamentary Papers II* 1975/76, 13 872, no. 3, p. 45; Report of the State Committee on Constitutional Reform, 2010, p. 89, available at www.rijksoverheid.nl.
[112] *Parliamentary Papers II* 1975/76, 13 872, no. 3, pp. 41-42.
[113] *Parliamentary Papers II* 1997/98, 25 892, no. 2, p. 45.
[114] *Idem*, pp. 47-50.
[115] *Idem*, p. 46.
[116] *Idem*, p. 46-47; *Parliamentary Papers II*, 1998/99, 25 892, no. 6, p. 27.

Although the scope and interpretation of article 13 Constitution have been the subject of discussions since as long ago as 1997, the only possible conclusion from the legislative history is that for the time being the current article only protects communications during the transmission phase.[117] In 2010 the State Committee on Constitutional Reform, established by Royal Decree of van 3 July 2009, issued a report[118] in which it recommended among other things to amend article 13 Constitution. The cabinet stated that it adopted this recommendation.[119] The proposal to amend article 13 Constitution was available for public consultation from 1 October 2012 until 1 January 2013. The text of the bill reads as follows:

Article 13 Constitution (bill)

1. Everyone has the right to respect for the privacy of his correspondence and telecommunications.
2. This right shall not be restricted except in the cases laid down by Act of Parliament with the authorisation of the court or, in the interest of national security, with the authorisation of one or more ministers designated by Act of Parliament.
3. Rules shall be laid down by Act of Parliament to protect the privacy of correspondence and telecommunications.

A number of changes will now be set out:
The proposal widens the scope of article 13 to include all (private) telecommunications, regardless of the means or technology used to communicate: e-mail, communication via *social media*, storage of personal data files in the cloud and search terms for information on the Internet using a browser all fall under the protection of article 13 Constitution.[120] The privacy of telecommunications within the meaning of article 13 is designed for an interpretation of the term telecommunications that is broader than the interpretation given to the term electronic communication in national and European rules and regulations, with the result that the number of communication means covered by the protection of article 13 will be extended to include all present and future means of communication (including non-electronic means).[121]

The proposal does not only aim at protecting data during its transmission but also during its temporary storage in the transmission phase. For example, the protection of article 13 also covers messages stored in a telecom provider's voice-mail box or in a mailbox of e-mail services like Gmail.[122] The norm is that the privacy of correspondence and telecommunications must be protected as long as the third party is in charge of the message and has access to its content. [123]

There are three cumulative conditions that must be satisfied for the privacy of correspondence and telecommunications to apply: (1) the communication process must include the use of a *means of communication*, (2) there must be *a third party* who is charged with managing the transmission and/or storage of the communication, and finally (3) the

---

[117] *Parliamentary Papers II* 1975/76, 13 872, no. 3, p. 39.
[118] Report of the State Committee on Constitutional Reform, 2010, available for inspection at www.rijksoverheid.nl.
[119] *Parliamentary Papers II* 2011/2012, 31 570, no. 20, p. 8.
[120] *Ontwerp toelichting Wetsvoorstel Wijziging article 13 Grondwet* [Draft explanatory memorandum to the Bill amending article 13 Constitution], version 1 October 2012, p. 8.
[121] *Idem*, pp. 8/11.
[122] *Idem*, p. 11.
[123] *Idem*, p. 14.

communication[124] must be *addressed*[125]. If these conditions are satisfied, the content of the message will at all times be protected by the privacy of correspondence and telecommunications, regardless of whether the sender of the message intended it to be so protected or not.[126]

Traffic data, i.e. data coming into existence when communication takes place via channels provided for the purpose, relates to the communication instead of to the content of the communicated message, for instance to the time, place, duration of and the numbers involved in a telephone call and to the time, address and size of an e-mail message.[127] It is recognized in the explanatory memorandum to the bill that traffic data does in fact provide insight into aspects that may be connected with communication content. Moreover, traffic data may by its nature concern the freedom of telecommunication, in the sense that a citizen may refrain from making certain calls if he knows or suspects that the authorities know which telephone calls he makes. This does not break through the confidentiality of the communication as such, but it does affect the freedom of (tele)communication. Nevertheless, traffic data has not been brought within the scope of article 13 Constitution, because it was reasoned that this data does not concern the content of telecommunications and that a different choice would have the result that judicial authorisation would be required for each and every examination of traffic data, which would go too far given the nature of such data.[128] To the extent that traffic data is also personal data, such data does fall under the protection of article 10 Constitution. The bill recognizes that in a technical sense telecommunication content will occasionally be considered to be traffic data as well, for example a text message or the subject line of an e-mail message. The conclusion on this point is that the protection provided by article 10 Constitution cannot take away the fact that from a technical perspective data relating to telecommunication content are considered traffic data. However, traffic data which does not at the same time relate to telecommunication content falls outside the scope of article 13 Constitution.[129]

The bill provides that restriction of the right to privacy of telephone and telegraph is only possible in the cases laid down by Act of Parliament, with the authorisation of the court or, in the interest of national security, with the authorisation of one or more ministers designated by Act of Parliament. The explanatory memorandum to the bill further shows that the system leaves room for such authorisation to be given in the name of the minister concerned on the basis of a mandate. The mandate is exercised in the name, under the responsibility and under the control of the minister.[130]

---

[124] *Ontwerp toelichting Wetsvoorstel Wijziging article 13 Grondwet*, [Draft explanatory memorandum to the Bill amending article 13 Constitution], version 1 October 2012, p. 12.
[125] 'Addressed' means that the communication must be addressed to one or more specific receivers. In principle, the content of a particular performance, a public speech, information on the Internet or realtime audio and video such as a live radio or television broadcast are not addressed communications.
[126] *Idem*, p. 16.
[127] *Idem*, pp. 16-17.
[128] *Idem*, p. 17.
[129] *Ontwerp toelichting Wetsvoorstel Wijziging article 13 Grondwet* [Draft explanatory memorandum to the Bill amending article 13 Constitution], version 1 October 2012, p. 18.
[130] *Idem*, p. 22.

The public consultation on the bill was completed on 1 January 2013. The bill has been submitted to the Council of State for its opinion. The government has promised that it will submit the bill in the first half of 2014.[131]

III Safeguards in the ISS Act 2002

A number of powers laid down by law are available to the services and permit them to process data for the purpose of performing the tasks assigned to them in the interest of national security[132]. Processing (personal) data, in particular collecting and if necessary exchanging such data, can infringe the privacy of citizens to a greater or lesser extent. The statutory rules and the safeguards included in the Act to protect the privacy of citizens reflect the various degrees of interference. In drafting them the legislator also took into account that from an effectiveness point of view the activities of the services usually take place in secret with the result that citizens are left in the dark about the interference with their fundamental rights. In order to achieve a balance between the interest of national security and the interest of privacy, the ISS Act 2002 provides for a system of procedures, requirements and safeguards applying to the deployment of (special) powers, which become more stringent in proportion to the increasingly serious nature of infringement of the privacy of citizens as a result of the exercise of a (special) power by the services. The main mechanisms provided for in the ISS Act 2002 to safeguard the protection of privacy are discussed in greater detail below.

The requirement of necessity laid down in article 8 ECHR is included in the ISS Act 2002 in several places. First of all in article 12 ISS Act 2002 which pertains to all data processing activities of the services. The article sets out that the services may only process data if they do so for a specific purpose and only to the extent necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act. The phrase "proper implementation of the ISS Act 2002 or the Security Screening Act" means that the data processed by the services must primarily relate to the performance of the tasks assigned to them – in the interest of national security, therefore – and to the management duties connected with these tasks (such as (personnel administration and payroll accounting), but that scope is allowed for other data processing – for which provision is made by or pursuant to the ISS Act 2002 or the Security Screening Act – for example the provision of data for the purpose of enabling an individual to exercise the right to examine data and for the purpose of cooperation with

---

131 *Nationaal actieplan mensenrechten, bescherming en bevordering van mensenrechten op nationaal niveau* [National action plan on human rights, protection and promotion of human rights at the national level], ministry of the Interior and Kingdom Relations, December 2013, p. 17, available for inspection at www.rijksoverheid.nl.

132 *Tasks of GISS* (article 6(2) ISS Act 2002): conducting investigations into (potential) dangers to the Netherlands or to Dutch interests (a task), security screening (b task), taking measures to promote security (c task), investigating specified countries to support the government with political intelligence (d task), drawing up threat and risk assessments in the context of the monitoring and protection system (e task). *Tasks of DISS* (article 7(2) ISS Act 2002): conducting investigations in support of the performance of international crisis-management and peace-keeping operations (a task), security screening (b task), conducting counterintelligence and security investigations for the benefit of the armed forces (c-task), taking measures to promote security (d task), conducting investigations into certain countries regarding matters with military relevance to support the government with political intelligence (e task), drawing up threat analyses in the context of the monitoring and protection system (f task).

foreign services.[133] The requirement of necessity is also made applicable to the exercise of special powers in article 18 ISS Act 2002. This article provides that special powers may only be used to the extent necessary for the performance of specified tasks of the services.[134] The legislator did not deem it necessary, let alone advisable, for the services to be able to use special powers for any and all of their tasks. The restriction to specified task areas is closely connected with the fact that the use of special powers may constitute considerable infringement of the privacy of citizens. For the tasks for which the services are not permitted to exercise special powers the general power to collect data provided in article 17 ISS Act 2002 is quite sufficient.[135] In addition to article 18, the requirement of necessity applying to the use of special powers is also laid down in article 32 ISS Act 2002. This article provides that the exercise of a special power must be terminated if the purpose for which the power was exercised has been accomplished, in other words: if exercising the power is no longer necessary for accomplishing the purpose. It is self-evident that if the means does not or cannot contribute to the purpose or cannot or can no longer do so, the means may likewise not or no longer be used. This means that the services, prior to exercising a special power, must have a purpose for which the means is deployed and that the expectation must be that the data the deployment will yield will contribute to accomplishing that purpose. After the service has started using the power, it will only be permitted to continue using it if the data so obtained actually contributes to the investigation.

Since the exercise of special powers may seriously interfere with the privacy of citizens, the legislator has incorporated a number of strict safeguards, for example a limitative list of permitted means of intelligence, the permission requirement, a limit on the duration of the exercise of a special power and the requirements of necessity (already discussed above), proportionality and subsidiarity of deploying the powers.

The package of special powers available to GISS and DISS cannot simply be arranged into a hierarchical structure based on the degree in which the rights of the person concerned are infringed. It can be inferred from the different levels prescribed by the legislator at which permission must be given for deployment of a means of intelligence that a higher level of permission means a more serious infringement of the rights of the persons concerned than a lower level. That is not the whole story, though. The fact is that in practice the severity of the infringement is mainly determined by the technical and practical details of exercising a special power, its duration and the data information obtained thereby.[136] For example, if a telephone is tapped for only one day or a frequency intercepted for only a short while or if the selection of untargeted interception does not yield any hit at all, then the actual infringement is less severe than when one of the services demands access to the telephony traffic data of a person on a monthly basis for a year. This does not, however, change the fact that even if the special power is only exercised for a short time and the yield is nil, it still constitutes infringement.[137] It will therefore have to be assessed in advance on a case-by-case basis how serious the expected infringement will be and whether the requirements of proportionality and subsidiarity are satisfied. The reasons stated for deploying a special power must clearly reflect these issues. When the ISS Act 2002 was drafted, these assessment criteria arising from the ECHR and the case law of the ECtHR (see section II.2) were

[133] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 18.
[134] For GISS these are the a task and the d task. For DISS the a task, c task and e task.
[135] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 26.
[136] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 29.
[137] CTIVD review report no. 28 on the use of Sigint by DISS, *Parliamentary Papers II* 2011/12, 29 924, no. 74 (appendix), section 5.2, available at www.ctivd.nl.

embodied in articles 31 and 32 ISS Act 2002. The requirement of proportionality (article 31 ISS Act 2002) means that the exercise of a power must be proportional to the intended objective (paragraph 4) and that the service must refrain from exercising the power if its exercise would cause the person involved disproportionate harm compared to the intended objective (paragraph 3). This means that the interest served by exercising the special power (national security) must be balanced against the interests of the person involved (the right to respect for his privacy).[138] At the same time the interference must be kept at a minimum, also known as the requirement of subsidiarity (article 31(1) and (2) and article 32 ISS Act 2002). This means that exercising a special power is only permitted if the intended collection of data cannot take place or cannot take place in time without exercising a special power (article 31(1) ISS Act 2002).[139] Furthermore, a service may only exercise the power which, in view of the circumstances of the case including the gravity of the threat to the interests protected by the service, will cause least harm to the person concerned compared to other available powers (article 31(2) ISS Act 2002). Moreover, the service must cease exercising a special power if exercising a less infringing power will suffice (article 32 ISS Act 2002).

With a view to the privacy of citizens the law distinguishes data collection acts by level of infringement, thus giving expression to the requirement of subsidiarity. The services must first use the least infringing powers (the general power) and only then, if it proves necessary, they may scale up to more infringing powers (special powers). In concrete terms this means that they must first consult their own files (information already in the possession of the services), next they may, if necessary, consult sources of information accessible to everyone – public sources – such as the Internet, or sources of information the services have the right to access and examine the information recorded therein, such as the Municipal personal records database or police files, or apply to informers (article 17 ISS Act 2002) and finally, to the extent the law provides for this possibility and to the extent it proves necessary, they may deploy special means of intelligence (articles 18 ff. ISS Act 2002)[140], taking into account that the infringing natures of the special powers differ from each other and that the service must choose the least interfering power.

A safeguard that is important for the protection of the privacy of individuals is the requirement to obtain permission to deploy special powers. The level at which permission must be obtained is not the same for all special powers. As a rule, permission must be given by the minister concerned or by the head of a service on behalf of this minister, unless the applicable provision provides otherwise (article 19(1) ISS Act 2002). The head of a service may further mandate the power to give permission (article 19(2) ISS Act 2002). With respect to a number of cases the law expressly provides that only the minister concerned is competent to grant permission. This is connected with the protection of the privacy of the telephone and telegraph by article 13 Constitution.[141] Such a provision applies – insofar as relevant to the present investigation – to tapping (article 25 ISS Act 2002) and the selection of

---

[138] Depending on which special power is used and on the social position of a person or organisation targeted by the special power, a person's interests may include other rights, such as the privacy of the telephone (article 13 Constitution), the professional privilege of lawyers and other holders of confidential information, the right to source protection of journalists or diplomatic immunity.

[139] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 52.

[140] *Parliamentary Papers II* 2000/01, 25 877, no. 59, pp. 4-5.

[141] The bill to amend article 13 Constitution proposes making permission of the minister the general rule in the case of restrictions in the interest of national security, but expressly allowing the minister to mandate this power; *Ontwerp toelichting Wetsvoorstel Wijziging article 13 Grondwet* [Draft explanatory memorandum to the Bill amending article 13 Constitution], version 1 October 2012, p. 22.

recorded telecommunications obtained by untargeted interception (article 27(3) and (4) ISS Act 2002). For other special powers the level of permission may either be the head of the service or be delegated to a lower official level pursuant to a submandate. At GISS, power to give permission to deploy an agent (article 21 ISS Act 2002) and to hack (article 24 ISS Act 2002) has been assigned, pursuant to the GISS Special Powers Mandate Decision, to the director of the unit and the head of the unit, respectively.[142] In respect of DISS the law provides that the power to grant permission on a first application for permission to deploy an agent and to hack a computerised device or system is not mandated to the head of the service, so that in these cases permission must be obtained from the minister of Defence.[143] The law does not prescribe a formal permission procedure for demanding access to telephony traffic data (article 28 ISS Act 2002)[144] or access to subscription data (article 29 ISS Act 2002), because such demands do not relate to traffic content, nor for searching (article 26(2) ISS Act 2002) and untargeted interception (article 27(2) ISS Act 2002), because the exercise of these powers does not involve the examination of data content, nor for military message traffic (article 25(8(ISS Act 2002) because such traffic hardly ever touches upon privacy. In some specific cases[145] permission must be granted by the minister of Defence in agreement with the minister of the Interior and Kingdom Affairs if the special power is used at a location that is not in use by the ministry of Defence.[146] This rule serves to prevent undesirable interference with investigations by GISS. Linked to the requirement of permission is the rule that a special power may not be exercised for an unlimited period after the required permission has been obtained. The limitation of the duration during which a power may be exercised is another important safeguard for the protection of the privacy of citizens. In principle a special power may be exercised for a period not exceeding three months, unless otherwise provided by law, after which period the service can apply for renewal of the permission for a similar period each time (article 19(3) ISS Act 2002).

IV Data processing by the services

IV.1 General framework for data processing

The ISS Act 2002 sets a number of conditions for data processing by the services. These conditions apply to all forms of data processing. Article 12 ISS Act 2002 provides for the general power of the services to process data. It covers both personal data and other data. The article states expressly that when the services process data they must comply with the requirements set for this activity by or in accordance with this ISS Act 2002 or the Security Screening Act. The rules on data processing laid down in the ISS Act 2002 constitute an exhaustive set of rules. The Personal Data Protection Act is expressly declared not applicable (article 2 Personal Data Act). On some points, however, the rules in the ISS Act 2002 were drafted to tie in with provisions of the Security Screening Act, for example the definition of data processing and the general requirements set on data processing. These requirements in their turn constitute an expression of the general principles of *inter alia* proportionality and subsidiarity that were developed in privacy law and with respect to article 8 ECHR.

---

[142] GISS Special Powers Mandate Decision 2009, article 4 (agent), article 7 (hacking).

[143] Defence Mandate under the Intelligence and Security Services Act 2002 and the Security Screening Act, *Official Gazette* 2002, 147.

[144] It should be observed in this context that a demand for access to traffic data pursuant to article 28(4) ISS Act 2002 must be made by the head of the service.

[145] For the purpose of the present investigation the following provisions are relevant: article 24(2); article 25(3); article 27(8); and article 28(5).

[146] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 17.

Data processing must comply with a number of general requirements, which are laid down in articles 12, 13, 15 and 16 of the ISS Act 2002. For example, data processing may only take place for a specific purpose and to the extent necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act (article 12(2) ISS Act 2002). The requirement of necessity was discussed in section III. The requirement of purpose limitation implies a sufficiently specified purpose that has been recorded within the organisation. Data which has lost its meaning given the purpose for which it is being processed must be deleted and destroyed with due observance of the provisions of articles 43 and 44 ISS Act 2002. Furthermore, data processing must take place in accordance with the law and with proper and due care (article 12(3) ISS Act 2002). The general requirement that data processing must take place with proper care provides a basis for a requirement of proportionality, as required by article 8 EVRM, for all forms of data processing, since proportionality of means to purpose is one of the norms for proper government conduct. In addition, one element of proper government conduct is that the authorities respect the fundamental rights of their citizens, which means that the services, when processing (personal) data, must take account of the fact that they are thereby infringing the right to privacy and possibly other rights of the person involved.[147] Processed data must, moreover, be provided with an indication of the degree of reliability or a reference to the document or source from which the data is derived (article 12(40 ISS Act 2002). Article 13 ISS Act 2002 contains an exhaustive list of the categories of persons whose data may be processed. Articles 15 and 16 ISS Act 2002 lay down a number of duties of care, which the services have further elaborated in practice within their organisations. The services must, for instance, ensure the secrecy of relevant sources from which data is derived (article 15(b) ISS Act 2002) and the safety of the persons cooperating in the collection of information (article 15(c), ISS Act 2002). Pursuant to article 16 ISS Act 2002 – which primarily concerns the technical and organisational arrangements of data processing – the services must ensure the accuracy and completeness of the data, the presence of data security measures, and restrictions on access to the data. The latter duty together with article 35 ISS Act 2002, which lays down the *need to know* principle, constitutes the basis for the services' authorisation and authentification policy on access to information systems and to the data and data files stored in them. The need to know principle sets the standard for the internal provision of data. Internally, data may only be provided to the extent necessary for the proper performance of the task assigned to the functionary[148] in question.

IV.2 Processing data collections

Data processing not only involves data relating to specific persons or organisations in which the services are interested in pursuance of their tasks, but may also concern collections of data (data collections). Data collections can come into existence within the services by the combination of processed data, but they can also be acquired from public sources, by requesting external parties to give access to data on a voluntary basis (authorities, business sector or other parties who increasingly possess data collections), by deploying a special power (for example untargeted interception or hacking), or by cooperating with foreign intelligence and/or security services. Under certain circumstances the services can also have direct access (at a distance) to specific data collections. Sections IV and V contain a more detailed discussion of how the services collect data. (Computerised) data collections enable the services to acquire large volumes of relevant data that is relevant for the performance of

[147] See on the general standards of proper conduct: *De Nationale ombudsman, 'Behoorlijkheidswijzer', 2012*, available via www.nationaleombudsman.nl.

[148] Employed by one of the services or working for the services pursuant to article 60 ISS Act 2002.

their tasks. Because these data collections include data relating to persons who are not relevant to the tasks of the services and because the files often require data analysis prior to their further internal use, processing such data collections raises questions about the legal basis in the ISS Act 2002 for such processing.

Article 1 of the ISS Act 2002 uses the term "data" to refer to personal data and other data. Neither the law nor the legislative history expressly mentions data collections, but there appears to be no reason why the term data should not cover collections of (personal) data. This means that the general legal framework for data processing, as laid down in articles 12 - 16 ISS Act 2002, applies to the processing of data collections as well. Particularly article 13 ISS Act 2002 should be mentioned here because this article sets out an exhaustive list of the persons and categories of persons whose data may be processed. Their designation links up primarily with the tasks assigned to the services in articles 6 (GISS) and 7 (DISS). For both services the list of article 13 ISS Act 2002 includes a category of persons "whose data is necessary to support the proper performance of its tasks by the service" (paragraph 1(e) (GISS) and paragraph 2(e) (DISS)). This category can be considered to constitute a legal basis for processing the data stored in (computerised) data collections of persons who are not subjects of interest in connection to the tasks of the services. The legal basis for the legitimacy of data analysis as a form of (computerised) data processing is provided by article 1 ISS Act 2002, which elaborates the concept of data processing, in combination with article 12(1) ISS Act 2002. Furthermore, the term data processing includes the acts of combining data and linking data, which are two forms of data analysis. According to the legislative history, moreover, data processing should be understood to mean both manual and computerised processing.[149]

Although it can be argued that the ISS Act 2002 provides a sufficient basis for (computerised) processing of data collections, the Act does not contain any express provisions on the subject. In connection with the increased use of this method by the services in recent years, the question arises whether the legal basis in the current ISS Act 2002 is still adequate.

The bill proposing the post-Madrid measures[150], which was eventually withdrawn, included a provision pertaining to this method, in particular to meet public concern and the uncertainties regarding the issue. The bill was aimed at helping to make the services function more effectively and efficiently, also in the light of the attacks in New York, Madrid and London and the assault on Van Gogh. The explanatory memorandum to the bill stated that the implementation of the ISS Act 2002 had shown among other things that in a number of cases the Act was not sufficiently explicit regarding the use of, or the possibilities of using certain data processing methods, e.g. data analysis, and the possibilities to obtain (or grant, as the case may be) direct access to specific data collections.[151] According to the explanatory memorandum to the bill, data analysis was an accepted procedure at the services which was performed in various forms and offered ever increasing possibilities as a result of information technology developments. The proposed article 12a expressly made data analysis a procedure used by the services in that it provided that searching data on the basis of profiles or comparing data with a view to detect patterns counted as forms of data

[149] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 17.
[150] Bill amending the Intelligence and Security Services Act 2002 in connection with improving the possibilities available to the intelligence and security services to investigate and take measures against terrorist threats and other dangers to national security as well as some other amendments, *Parliamentary Papers II* 2005/06, 30 553, no. 3.
[151] *Idem*, p. 3.

analysis which the services practised or were permitted to practise. For the purpose of these forms of data analysis, so the explanatory memorandum stated, the services used data in their own computerised data collections, but also data included in computerised data collections in the possession of third parties which had been made available to the services on a voluntary basis (either with or without application of article 17 ISS Act 2002).[152] Although according to the explanatory memorandum to the bill data analysis was already part of the toolkit of the services and already had a sound legal basis as well, it was nevertheless deemed desirable to lay down by law more express standards with respect to some elements in order to make the law more foreseeable and provide additional safeguards for its application.[153]

The amendment of the ISS Act 2002 also provided for adjustment of article 13 ISS Act 2002 on account of the uncertainties experienced in practice regarding the interpretation of subparagraphs (e) of the current first and second paragraphs of this article, in relation to the data analysis procedure as a form of data processing. For this reason a new paragraph expressly provided that when a service applied either of the two forms of data analysis mentioned in the proposed article 12a to data collections of third parties, it could also process personal data relating to persons who had not caught the service's attention before, but whose data it must nevertheless be deemed to be necessary to process in support of the proper performance of its task by the service for the simple reason that this data formed an integral part of the data file.[154] The bill also provided for an amendment to article 17 (in the sense that it would expressly state that the voluntary provision of data may also concern data collections) and the introduction of an article 29b (making it obligatory for administrative bodies and categories of financial services providers and carriers to be designated by law to provide (parts of) computerised data collections).

In its advisory opinion on the bill the Dutch Data Protection Authority (DPA) stated among other things that it was not convinced of the necessity of introducing an obligation for certain categories of persons and institutions to provide data collections. The DPA also entertained doubts about the proposed provision pertaining to data analysis because the services would thereby come to be under greater pressure to analyse more data, because there were no guarantees of the quality of the acquired data nor guarantees that conclusions drawn from the data would be in accordance with reality, and because of the risk of *function creep* in the sense that on the one hand technologies that were originally directed at a specific group of persons (who required the attention of the services in connection with their tasks) could gradually be applied to (virtually) everyone, while on the other hand data collected for a specific objective (the objective of the person or institution that had recorded the data) would be provided and processed for another objective (in the interest of national security).[155]

In its reaction to the advisory opinion of the DPA on the bill, the government emphasized among other things that the services were by no means pursuing the creation of limitless data collections that had no relevance to their statutory tasks. In fact they had no power to do so, as appeared from articles 12 and 13 ISS Act 2002.[156] The government also emphasized that any data processing by the services must always be based on a specific investigation issue

---

[152] *Idem.*

[153] *Idem*, pp. 24-26; *Parliamentary Papers I* 2007/08, 30 553, C, p. 12.

[154] *Parliamentary Papers II* 2005/06, 30 553, no. 3, p. 26.

[155] Advisory opinion CPB of 20 December 2007, appendix to *Parliamentary Papers I* 2007/08, 30 553, B, pp. 7-8/10-11.

[156] *Parliamentary Papers I* 2007/08, 30 553, C, p. 5.

arising from the statutory tasks of the services. *Fishing expeditions* or untargeted comparison of files was unlawful and contrary to article 12 ISS Act 2002.[157]

The bill to amend the ISS Act 2002 was adopted by the Second Chamber of Parliament but it failed to pass the First Chamber of Parliament[158], partly on account of the critical comments of the DPA[159]. In 2011 the government decided to withdraw the bill.[160]

In the current situation the processing of data collections must satisfy the general requirements applying to data processing (article 12 ISS Act 2002), so among other things such processing must be done for a specific purpose and only to the extent necessary for the proper implementation of the law. It follows from the proper care requirement that the infringement of citizens' privacy caused by the processing must be proportional to the purpose pursued. The requirement that data processing must be done for a specific purpose means that when the services are collecting data, they may not copy and further process external data collections at random (or get direct access to them). To fulfil the requirement of necessity it must be assessed in advance, i.e. prior to the actual acquisition, which data is deemed necessary for the proper performance of the service's task. As regards the purpose for which a data collection is acquired the question arises how specific the purpose must be. Apart from being necessary for a specific investigation, it is very well possible that data collections are necessary to support the task performance in a broad sense – not only at a specific moment therefore but also in the future, for example because the service may need to access a file more than once. In the ISS Act 2002 the purpose criterion is formulated less strictly than in the Personal Data Protection Act, which provides that personal data may only be collected for specified, explicit and legitimate purposes (article 7). It can be inferred from the broader wording of the purpose criterion in the ISS Act 2002 that gathering data collections is also legitimate if done for a broader purpose, which must, however, be described and substantiated by reasons in advance, to show that processing is necessary for the proper performance of tasks. Subsequently, to safeguard the protection of the privacy of citizens, access to the files must be sufficiently restricted in accordance with the provisions of articles 15, 16 and 35 ISS Act 2002. The rules laid down in articles 43 and 44 ISS Act 2002 about the deletion, destruction and archiving of processed data are likewise a guarantee for the protection of the privacy of citizens.

Data collections must be used in accordance with the purpose for which they were acquired. Unlike the Personal Data Protection Act (article 9), the ISS Act 2002 does not set further rules for the use of data or data files for other purposes than the purpose for which they were acquired. Under the Personal Data Protection Act a compatibility requirement applies to the effect that personal data may not be further processed in a way that is incompatible with the purposes for which the data was acquired, one of the criteria being the principle of purpose limitation, which means that the further the original purpose is removed from a subsequent purpose, the lesser the degree of compatibility. The ISS Act 2002 does not have such a provision. Article 43 ISS Act 2002 merely provides that data which in view of the purpose for

[157] *Idem*, p. 8.
[158] *Parliamentary Papers I* 2008/09, 30 553, E.
[159] Advisory opinion CPB of 20 December 2007, appendix to *Parliamentary Papers I* 2007/08, 30 553, B; reaction CPB of 25 June 2008 to the government reaction to CPB advisory opinion ISS Act 2002 (30 553, C), appendix to *Parliamentary Papers I* 2007/08, 30 553, D.
[160] *Parliamentary Papers I* 2010/11, 30 553, F; *Parliamentary Papers II* 2010/11, 30 553, no. 18.

which it is being processed is no longer meaningful, must be deleted. The deleted data is subsequently destroyed, unless statutory rules on retention prevent destruction.[161]

V Collecting data

V.1 General power

Article 17 ISS Act 2002 grants the services a general power to collect data. On the basis of this power the services may collect data in performing their tasks and also in support of properly performing their tasks, which refers among other things to investigations aimed at establishing the reliability of the persons whose services are used, for example an agent of the service.[162] The article provides that for the purpose of obtaining data the services may apply to (a) administrative bodies, public services and/or any persons deemed capable of providing the necessary data, and (b) persons responsible for processing specific data. In principle the necessary data is gathered from sources accessible to the public (open-source information), by consulting non-public data collections (with respect to which the services are granted the right to examine the data stored therein[163]) and by consulting persons and agencies who or which may possess the relevant data (also called informers), including foreign intelligence and/or security services (cooperation with foreign intelligence and/or security services is discussed in section VI). Pursuant to the third paragraph of article 17 ISS Act 2002 the regulations applicable by or pursuant to the law to the provision of the requested data cannot be invoked against the services. This provision does not mean, however, that article 17 ISS Act 2002 imposes an obligation on the intended provider to provide the requested data. Voluntary provision of data is the basic principle.

Article 17 ISS Act 2002 gives the services a wide power. It is not a special power, even though this power, too, can be used in secret and may infringe privacy. By virtue of this provision the services may collect data or data files by acquiring them from all persons and authorities who or which can be deemed capable of providing the data. This means that the services may approach and request data from all informers who are able to gather data for the services on a voluntary basis, for instance because they have access to such data by reason of the position they hold or the group in which they move.[164] An informer may only be consulted and not instructed or controlled.[165] Collecting banking data also falls under this general power, which means that the services do not require permission for this procedure.[166] This is different, for instance, in Belgium where this form of data collection falls

---

[161] With respect to GISS the Committee has established that in practice the service does not have a structural and active declassification programme, see for a more detailed discussion of this issue CTIVD review report no. 33 on the classification of state secrets by GISS AIVD, *Parliamentary Papers II* 2011/12, 30 977, no. 47 (*appendix*), section 10, available at www.ctivd.nl.

[162] *Parliamentary Papers II* 2000/01, 25 877, no. 15, p. 5.

[163] It was established in the legislative history that this refers to data 1) from the municipal personal records database (article 88 Municipal Database (Personal Records) Act), 2) provided by the persons and authorities referred to in articles 61 and 62 ISS Act 2002 (judicial authorities), and 3) from registers kept pursuant to the Judicial Records and Certificates of Good Conduct Act, *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 37.

[164] CTIVD review report no. 8b on the use by GISS of informers and agents, more in particular abroad, no Parliamentary Peper, section 5.3, available at www.ctivd.nl.

[165] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 59.

[166] CTIVD review report no. 20 on financial and economic investigations by GISS, *Parliamentary Papers II* 2008/09, 29 924, no. 35 (appendix), section 3.3.1, also available at www.ctivd.nl.

in the category of exceptional (highly interfering) methods.[167] It was established in the legislative history that in exceptional cases article 17 ISS Act 2002 may be used to request access, on a voluntary basis, to so-called printer data (meaning *a posteriori* data from the personal data file) of (historic) telephony traffic, in addition to the special power to do so under article 28 ISS Act 2002 (in the latter case there is in fact an obligation to cooperate).[168]

Some safeguards apply when the services use the general power under article 17 ISS Act 2002. It is not only the service's own statutory tasks that impose limits on what the services may request pursuant to article 17 ISS Act 2002, the rules on data processing explained in section IV also impose limits on what they may ask. In particular articles 12 and 13 ISS Act 2002 are relevant, which were discussed above and which set requirements on the quality of data processing (it may only take place for a specific purpose and to the extent necessary for the proper implementation of the law and provided it is done with proper and due care) and which contain an exhaustive list of the persons whose data may be processed.

V.2 Special powers

Subject to strict conditions the services may also collect (personal) data or (personal) data collections by deploying special powers. The special nature of these powers is due among other things to the fact that they are exercised in secret. In addition, the exercise of these powers infringes certain fundamental rights. The services may only deploy special powers in connection with specified tasks: for GISS these are the a and d tasks (article 6 (2)(a) and (d)), for DISS the a, c and e tasks (article 7 (2)(a), (c) and (e)). Below, each of the special powers that are relevant to the collection of telecommunications data will be explained separately.

V.2.1 Article 21 ISS Act 2002

The power to deploy agents is embodied in article 21 ISS Act 2002:

> "to deploy natural persons (…) who, under the responsibility and on the instruction of a service, are charged with (1) the targeted collection of data (…) (2) promoting or taking measures (…)"

An agent is a person deployed purposefully for the targeted collection of data relating to persons and organisations which may be relevant to the performance of its tasks by a service (article 21(1)(a)(1º) ISS Act 2002). The explanatory memorandum to the ISS Act 2002 explains that the primary task of an agent is to get into what is called an information position in relation to a specific person or in a specific organisation who/which has attracted the attention of a service in connection with an investigation and – after acquiring such a position – to maintain it.[169]

An important element of deploying an agent is that the services *instruct* the person concerned to do something. Agents work under the control and supervision of the service in question. This distinguishes agents from informers as described in article 17 ISS Act 2002.[170]

---

[167] H.T. Bos-Ollermann, 'Meerdere wegen naar Straatsburg. Geheime methoden en toezicht op de inlichtingen- en veiligheidsdiensten in België en Nederland', in *De orde van de dag*, nr. 56 (Dec. 2011), p. 101.

[168] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 47.

[169] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 31.

[170] CTIVD review report no. 8b on the deployment by GISS of informers and agents, more in particular abroad, no Parliamentary Paper, section 5.3, available at www.ctivd.nl.

For control to be targeted it is important that the service knows quite well what it is trying to achieve by deploying an agent. Deploying an agent is a quite different type of special power than e.g. the power to place a telephone tap. While in the case of a tap it is certain in advance what is the risk of using the power and it can be assessed how seriously it will infringe privacy, these things are less evident when an agent is deployed. The point is that an agent can be asked to perform all sorts of different activities. His contacts with an investigation target may be superficial or on the contrary very personal, the agent may merely keep his ear to the ground or he may actively participate in activities, he may do occasional jobs for the service or carry out assignments on a daily basis. It is not a matter of turning a switch on or off, as in the case of a telephone tap. For every decision whether or not to control an agent in a specific way the service is deemed to assess the necessity, proportionality and subsidiarity of the choice made (see section III).

Pursuant to article 19(3) ISS Act 2002 permission to deploy an agent is granted for a maximum period of three months and can each time be extended for a similar period in response to a request to that effect. The ISS Act 2002 does not require the permission of the minister concerned or of the head of the service for the deployment of an agent. In principle, the initial deployment of an agent by GISS requires the permission of the unit director or unit head involved.[171] Renewal of the deployment requires the permission of the team head. It is provided with respect to DISS that the initial permission must be granted by the minister since mandating this power to the head of the service is prohibited.[172] The power to renew the deployment has been mandated to the head of the service unless it concerns a fundamental and sensitive matter of policy or politics.[173] The power may not be mandated to a lower level at DISS.[174]

An agent can be an employee of the service but also an external person, who is approached specifically for this task.[175] Agents cooperate with the service on a voluntary basis,[176] and the service has the possibility to remunerate them for their work. An agent can only be deployed effectively and safely if the relation between GISS or DISS and the agent is not known to the public. Pursuant to the duties laid down in article 15 ISS Act 2002 the services must ensure that information about and originating from an agent is not spread or disclosed except subject to stringent conditions. The basic principle of the Act is to keep secret any data and sources of data that qualify for confidential treatment.

V.2.2 Article 24 ISS Act 2002

Article 24(1) ISS Act 2002 regulates the power to hack computerised devices or systems:

---

[171] In implementation of article 19 ISS Act 2002 the rules on mandating the authority to give permission to deploy and to renew the deployment are laid down in the GISS Special Powers Mandate Decision 2009. Articles 4 and 5 of the Decision regulate the level at which permission for deployment of agents must be given. The Decision shows, moreover, that permission to deploy agents holding certain functions in society must be granted at a higher level. This can be at the level of director, head of service or the minister.

[172] Defence Mandate under the Intelligence and Security Services Act 2002 and the Security Screening Act, article 3(4)(a $1^{0)}$, *Official Gazette* 2002, 147.

[173] *Idem*, under a 2^{0}.

[174] DISS Submandating and Authorisation Decree 2009, article 3(2), *Official Gazette* no. 7168.

[175] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 31.

[176] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 59.

"The services are authorised, whether or not using technical means, false signals, false keys or a false capacity, to gain access to a computerised device or system. The powers referred to in the first sentence include the power:

a. to breach any security;
b. to introduce technical features to decrypt the encryption of data stored or processed in the computerised device or system;
c. to copy the data stored or processed in the computerised device or system."

The legislator has sought to link the description of the power to hack to the wording used in article 138ab of the Dutch Criminal Code (Sr) to make the hacking of a computer a criminal offence.[177] Pursuant to article 80 sexies Sr, "a computerised device or system" must be taken to mean "a facility for the purpose of storing, processing and transmitting data by electronic means". The definition comprises storage *and* processing *and* transmission of data. The conditions are in fact cumulative: facilities intended exclusively for the purpose of data transmission (a simple telephone, certain types of transceiver equipment) or data storage (usb sticks) fall outside the definition.[178] It is stated in the legislative history that in practice the provision pertains in particular to hacking (*stand-alone*) computers[179] and computer networks[180].

Article 24(1)(c) ISS Act 2002 shows that the power to gain access includes the power to copy the data stored or processed in the computerised device or system. The term *copy* is likewise defined in accordance with the Criminal Code. The legislative history of article 138ab Sr shows that the term refers to the act of copying proper.[181] Although it would seem logical for 'copying' within the meaning of article 24 ISS Act 2002 to include examination of content, neither the law nor the legislative history show this to be the case. It can be argued that where data is copied, this constitutes data processing within the meaning of the ISS Act 2002 (article 1(f)). Because data copying falls under the power of article 24 ISS Act 2002, the requirements set on the deployment of special powers apply, namely that reasons must be stated substantiating the necessity, proportionality and subsidiarity of the deployment (see section III).

The explanatory memorandum to 24 ISS Act 2002 prescribes that the power to hack may only be exercised if either the minister concerned or the head of the service has granted permission to do so (article 19(1) ISS Act 2002).[182] While the law provides with respect to a number of situations that exclusively the minister is competent to grant permission (e.g. tapping pursuant to article 25 ISS Act 2002), the legislator does not mention article 24 ISS Act 2002 in this context.[183] Consequently, submandating by virtue of 19(2) ISS Act 2002 is permitted by law. Pursuant to this article the head of the service may, by a written decision, appoint subordinate functionaries to grant such permission on his behalf, which was done in article 7 of the GISS Special Powers Mandate Decision 2009 with respect to article 24 ISS Act 2002. The DISS Mandate Decision provides that the head of the service has no mandate to

---

[177] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 39: "The provision refers to the intentional unauthorised intrusion into a computerised device or system for the storage or processing of data, or into part thereof, by breaching any security or getting access using a technical means, false signals or a false key or by adopting a false capacity."
[178] *Parliamentary Papers II* 1998/99, 26 671, no. 3, p. 44.
[179] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 39.
[180] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 63.
[181] *Parliamentary Papers II,* 1998/99, 26 671, no. 3, p. 28
[182] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 39.
[183] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 48.

grant permission on the first application for permission, nor with respect to any renewal where it concerns a fundamental and sensitive matter of policy or politics.[184] In those cases permission must be obtained from the minister of Defence. The Dessens Committee recommended vesting the power to grant permission for deployment of article 24 ISS Act 2002 in the minister concerned. This recommendation follows from the line of reasoning taken by the Dessens Committee that the more intrusive the infringement of privacy and of the privacy of communications, the more strongly the permission procedure must be anchored in law, and that restraint must be exercised as regards mandating or submandating powers that infringe fundamental rights.[185]

Article 24 ISS Act 2002 confers power on the services, when they are gaining access to a computerised device or system, "to copy the data stored or processed in the computerised device or system". So it is important that the data has been stored or processed. Examples of such data are files stored on a computer or server (photos, text files, etc.) but also types of conversations (chat conversations), telecommunications (e-mail), websites or transferred data as listed in article 25 ISS Act 2002. The difference with article 25 ISS Act 2002 is that data acquired under article 24 ISS Act 2002 is in principle copied *afterwards*, and is not tapped, received, recorded or monitored (*real time*). An example to illustrate this: in the case of an Internet tap (article 25 ISS Act 2002) an e-mail message is intercepted between sender and receiver, while in the case of an approval order under article 24 the same e-mail message is copied while the message is still (or already) in the possession of one of the two parties. The content of data obtained via intrusion into a computerised device or system can be similar, though, to that of data acquired by tapping. What is more, permission to hack pursuant to article 24 may often bring greater results. With a tap on an IP address (article 25 ISS Act 2002), for example, a service can only acquire the e-mail messages sent from and received by that specific IP address. If a service hacks an e-mail account, it can copy all e-mail messages stored in the mailbox, regardless from which computer the messages were sent or on which computer they were received. On the other hand, the use of an IP tap (article 25 ISS Act 2002) enables a service to copy all messaging to and from the various e-mail addresses used from one IP address. By hacking under article 24 a service will only obtain the messages sent from and received by the specific e-mail address for which it has obtained an approval order to hack.

At present, the current article 13 Constitution only provides protection of communications during the transmission stage, so that in principle intrusion into a computerised device or system pursuant to article 24 falls outside its scope of protection. The bill to amend article 13 extends the protection of communications to include in-transit storage at a third party, for example in a mailbox kept by an e-mail provider. Article 13 Constitution is discussed in section II.3 above. So it therefore conceivable that eventually the results obtained by the application of article 24 ISS Act 2002 will also fall under the privacy of telecommunications enshrined in article 13 Constitution.

The third paragraph of article 24 ISS Act 2002 provides for a duty to cooperate, meaning a duty to cooperate in undoing data encryption. Article 89 ISS Act 2002 makes refusal to cooperate a punishable offence.

---

[184] Defence Mandate under the Intelligence and Security Services Act 2002 and the Security Screening Act, article 3(4)(a) under 1^0 and 2^0, *Official Gazette* 2002, 147.

[185] Report of the Dessens Committee, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, December 2013, *Parliamentary Papers II* 2013/14, 33 820, no. 1 (appendix), p. 172.

V.2.3 Article 25 ISS Act 2002

Article 25(1) ISS Act 2002 confers power to intercept (tele)communications by targeted tapping :

> "The services are authorised to use a technical means for the targeted tapping, receiving, recording and monitoring of any form of conversation, telecommunication or data communication by means of a computerised device or system, regardless of where it takes place. The authority referred to in the first sentence includes the power to decrypt the conversations, telecommunications or data communications."

The article is couched in general and broad terms. It covers *any form of* conversation, telecommunication or data communication via a computerised device or system. This may be understood to include electronic communication. This means among other things that the services may not only wiretap telephone *conversations* but also data traffic via telephone lines[186], for example fax or text messages. The advantage of this broad wording is that it enables GISS to respond to new communication technologies.

Article 25 permits targeted interception of both cablebound and non-cablebound communications by the services. The services may, for example, record conversations using a microphone, wiretap telephone conversations, read e-mail messages, monitor a person's Internet behaviour and intercept *High Frequency* (HF) radio traffic. The word "*targeted*" in this context means that a service specifically examines the content of communications connected with a person, organisation, frequency, telephone number or IP address known to the service.

In the drafting process of the ISS Act 2002 the question was raised whether the words "regardless of where it takes place" mean that conversations, telecommunications and data transfers in other countries may also be tapped from the Netherlands. The government gave the following answer:

> "First of all it is noted that the power of the services to tap conversations, telecommunications and data transfers as regulated *inter alia* in article 25, does not extend beyond the jurisdiction of the State of the Netherlands, since the Dutch legislator cannot unilaterally create jurisdiction in other countries. This does not alter the fact that the exercise of the power regulated in article 25, in particular where it concerns the interception of telecommunications, and the exercise of the powers embodied in article 25a [Committee: the present article 26] and article 26 [Committee: the present article 27], which were inserted pursuant to a policy document amending the bill, may also extend to include interception of telecommunications originating from or intended for a foreign country."[187]

Deployment of the means mentioned in article 25 ISS Act 2002 infringes the privacy of the persons concerned, because it includes targeted examination of the content of communications of persons and organisations.[188] By deploying this special power a service violates the privacy of the telephone and telegraph enshrined in article 13 Constitution. In drafting the ISS Act 2002 the legislator chose not to provide for a mandating system in respect of special powers that violate rights specifically enshrined in the Constitution, such

---

[186] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 41.
[187] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 65.
[188] Military data traffic is an exception to this rule.

as the right to inviolability of the home and the privacy of the telephone and telegraph.[189] This means that pursuant to article 19 in conjunction with article 25(2) of the ISS Act 2002, exclusively the minister of the Interior and Kingdom Relations or the minister of Defence, respectively, is competent to grant GISS and DISS, respectively, permission to wiretap.[190]

Pursuant to article 25(4) ISS Act 2002 an application for permission submitted by (the head of) a service to the minister responsible must in any case state:

a) the power to be exercised and, if applicable, the number;
b) data concerning the identity of the person or organisation in respect of whom or which the power will be exercised;
c) the reasons for the application.

If the application is not for targeted interception of HF radio traffic based on a number as referred to under (a), but for interception based on a technical characteristic (i.e. frequencies), then according to the legislative history the technical characteristic need not be stated. The reason given for this was that persons and organisations usually communicate at several and changing frequencies. The requirement of stating the technical characteristic would in practice have the result that GISS or DISS would repeatedly have to submit new or supplementary applications. This would create an undesirable and unworkable situation.[191]

Permission is granted for a maximum period of three months and can be renewed after each period. According to the legislator this implies that if it is considered necessary, proportional and subsidiary to continue using the means in question, the head of the service must, upon the expiry of the three months, again apply for permission.[192]

Paragraph (6) of article 25 lays down rules for cases in which the identity data of the person or organisation against whom or which the power will be exercised is not known at the time when the application for permission is submitted to the minister. In those cases permission will only be granted subject to the condition that the data in question will be supplied as soon as possible.

V.2.4 Article 26 ISS Act 2002

Article 26(1) ISS Act 2002 provides for the power to search:

> "The services have power to receive and record non-cablebound telecommunications originating from or intended for other countries while using a technical means, based on a technical characteristic in order to explore communications. The services have the power to examine the content of the data thus received. The power referred to in the first sentence includes power to undo the encryption of telecommunications."

In practice, the exercise of the power of targeted interception (to the extent it concerns non-cablebound communications; article 25 ISS Act 2002) and selection after untargeted interception (which is only permitted with respect to non-cablebound communications; article 27 ISS Act 2002) are closely connected with the power to search (article 26 ISS Act

---

[189] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, pp. 45-46; *Parliamentary Papers II* 2000/01, 25 877, no. 59, pp. 7-8.
[190] In the case of places not being used by the ministry of Defence, permission must be granted in consultation with the minister of the Interior and Kingdom Relations (article 25(3) ISS Act 2002).
[191] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 18-19.
[192] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 43.

2002).[193] Searching usually precedes the exercise of these powers, in other words: it makes it possible to exercise the powers.[194]

The power of searching may only be exercised for exploring non-cablebound communications originating from or intended for other countries; in particular HF radio traffic and satellite communications.[195] Only a small part of HF and satellite traffic is relevant to the proper performance of tasks by the services. While searching, the services identify or explore, within the framework of their tasks, which sections of the ether may satisfy the requirements for interception.[196] They try to find out what is the nature of the telecommunications taking place via specific frequencies or channels (technical characteristic, for example what kind of transmitting equipment or transmission system) and which person or organisation is sending the telecommunications (the identity of the sender).[197] With regard to the latter the service ascertains whether the signals are digital or analogue, which medium is used (telex, traffic or data traffic) and in what language the data is sent.[198] Furthermore, searching is aimed at establishing whether it concerns telecommunications which it is necessary for the services to examine for the proper performance of their tasks.[199] In order to be able to determine who are participating in the communications and whether they are persons or organisations who or which merit the services' attention, it is important that the services have power to examine the content of the telecommunications.[200] Indeed, the legislator expressly permits the services to do so in article 26(1) ISS Act 2002. However, examining content should be done at random, for a short time and is merely a tool, not the objective of the means.[201] It is not permitted to follow a transmission longer than is strictly necessary to establish the identities of the persons or organisations, since then the searching would turn into a non-permissible form of targeted examination of communication content[202] Pursuant to the first paragraph, the power to search includes the power to undo the encryption of the telecommunication.

Three forms of searching can be distinguished: 1) for the purpose of targeted interception (HF radio traffic); 2) for the purpose of untargeted interception (satellite communications); 3) for the purpose of selection.

Searching for the purpose of targeted interception (HF radio traffic) is done by examining random samples of communication content and following transmissions for brief periods only. The activity is very different from tapping. In the legislative history, searching HF radio traffic is compared with turning a radio knob to find out which organisation is transmitting at which frequency.[203] The minister of Defence explained at the time that there is a very essential difference between searching for the purpose of knowing what is available on the market, so that information will be available at the very moment it has to be obtained for a specific purpose, and the targeted collection of information. When a service is really

---

[193] For a more detailed discussion of these subjects we refer to CTIVD review report no. 28 on the use of Sigint by DISS, *Parliamentary Papers II* 2011/12, 29 924, no. 74 (appendix), available at www.ctivd.nl.
[194] *Parliamentary Papers II* 2000/01, 25 877, no. 14, pp. 30/32.
[195] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 23-24.
[196] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 30.
[197] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 21.
[198] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 30.
[199] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 21-22.
[200] *Idem*, pp. 21-23.
[201] *Parliamentary Papers II* 2000/01, 25 877, no. 14, pp. 36-37.
[202] *Idem*, p. 35.
[203] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 30.

listening in and the communications are stored, translated and placed in a broader context, then, he said, the service is purposively collecting information for a specific operation. This falls under the permission regime (article 25 ISS Act 2002). Merely bringing together possibilities falls under the regime of "turning the knob".[204]

An important reason for searching for the purpose of untargeted interception (satellite communications) is that it is impossible for the services to intercept and record all satellite communications travelling the air waves so that they have to make choices. Searching serves to optimise these choices. For example, by searching the service finds out from which region the communications via a specific satellite channel originate, to which region the communications are sent and what type of communication it concerns (voice, fax, internet, etc.). Searching satellite communications supports the process of untargeted interception (Article 27 ISS Act 2002) through the fact that searching enables the services to examine which are the satellite channels used for transmitting communications that may be relevant to the performance of tasks by the services.[205] Searching enables the services to limit the satellite traffic they will intercept and record to the traffic of specific channels.[206] Subsequently, a service can choose a number of satellite channels and receive and record the communications transmitted via these channels by untargeted interception, and then – with the minister's permission – deploy the power of article 27(3) ISS Act 2002 (characteristic-based selection) to select from the large volume of satellite communications (the bulk) that has been intercepted and recorded the communications the service needs to examine for the proper performance of its tasks.

Three forms of searching for the purpose of selection can be distinguished: 1) searching the communications bulk to determine whether the desired communication can be found using the selection criteria for which permission has been obtained; 2) searching the communications bulk to identify or characterise potential investigation targets; 3) searching the communications bulk for data from which future selection criteria (e.g. telephone numbers) can be derived to be used in an expected new investigation area. In the opinion of the Committee the ISS Act 2002 provides a basis for the first form of searching. There is no basis in the ISS Act 2002 for the other two forms.[207]

Article 26 (2) ISS Act 2002 provides that no permission as referred to in Article 19 of the Act is required for searching. The legislative history of Article 26 ISS Act 2002 shows the reason for this to be that the nature of the activity is partly comparable to that of the untargeted interception and recording of non-cablebound telecommunications under Article 27 ISS Act 2002. Its untargeted nature follows not so much from the fact that the services may scan various frequencies or satellite channels, but rather from the fact that they do not know in advance which communications (type and content) from whom (which person or organisation) they will come across in the process.[208] The legislator observed, moreover, that a requirement of permission would have no added value. The searching does not target a specific person or organisation. Neither is it possible to state a specific reason for the searching (cf. Article 25(4)(c) ISS Act 2002).[209] This means that the required permission would

[204] *Parliamentary Papers II* 2000/01, 25 877, no. 72, pp. 4-6.
[205] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 32.
[206] *Parliamentary Papers II* 2000/01, 25 877, no. 59, p. 12.
[207] CTIVD review report no. 28 on the use of Sigint by DISS, *Parliamentary Papers II* 2011/12, 29 924, no. 74 (appendix), section 7.4, available at www.ctivd.nl.
[208] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 22.
[209] Idem.

only relate to the general purpose of searching, as provided for in Article 26(1) ISS Act 2002. The legislator held this to be hardly worthwhile.

It is stated in the legislative history of the ISS Act 2002 that the privacy of the telephone is not infringed unless and until listening in to a telephone conversation is aimed at gaining knowledge of the content itself. If note is taken of the content of a telephone conversation purely as a brief element of an investigation into the identity of the persons or organisations communicating with each other, this does not violate the privacy of the telephone. Rather, so the legislator held, it was comparable to the examination of traffic data. According to the legislator such examination could be held to infringe the right to privacy enshrined in Article 10 of the Constitution, but not the privacy of the telephone and telegraph enshrined in Article 13 of the Constitution.[210] The legislator also made the comparison between searching and the monitoring of telephone conversations by providers of telecommunication networks and services in order to establish whether the connection is functioning properly. It would go too far, so it was held, to interpret the privacy of the telephone so broadly that such technical monitoring and repair activities, which inevitably entail overhearing bits of a conversation, must also be deemed to constitute infringement thereof.[211]

In review report no. 28 the Committee made a critical note on the comparison of searching to the examination of traffic data. In making this comparison the legislator ignored the fact that searching is certainly directed at communication content, since searching on the basis of content is used to try and establish the identity of the sender and the communication's relevance to the performance of their tasks by the services. This is expressly not the case in the examination of traffic data, where no note is taken of any communication content at all. The comparison with technical monitoring and repair activities by providers of telecommunications networks and services does not hold good either, since in those cases examining content is not an intended result of the activities. These activities are not aimed at examination of content.[212]

The fact that during searching, communication content is examined only very briefly and that the content is not examined in full does not, in the opinion of the Committee, change the fact that searching violates the privacy of the telephone and telegraph enshrined in Article 13 Constitution. It does so regardless of the different interpretations given to the object and the scope of the fundamental right. The aforementioned circumstances can only play a role in assessing the severity of the violation. If one compares searching with a postman who opens an envelope and, after briefly glancing through the purport of the enclosed letter, reseals it, then in that, case too, there is no reason to conclude that the privacy of correspondence has not been violated.[213]

The power to search is embodied in the ISS Act 2002 as a special power. This means that the exercise of the power must satisfy the requirements of necessity, proportionality and subsidiarity (see section III).

V.2.5 Article 27 ISS Act 2002

[210] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 35.
[211] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 23.
[212] CTIVD review report no. 28 on the use of Sigint by DISS, *Parliamentary Papers II* 2011/12, 29 924, no. 74 (appendix), section 4.3.3, available at www.ctivd.nl.
[213] *Idem*.

Article 27(1) confers the power of untargeted interception of non-cablebound telecommunications:

> "The services have power to receive and record non-cablebound telecommunications using untargeted interception and a technical means. The powers as referred to in the first sentence include the power to undo the encryption of the telecommunication."

Contrary to article 25 ISS Act 2002 which provides for the *targeted* interception of the (tele)communications of a person, organisation or telephone number known to the services, article 27(1) ISS Act 2002 makes it possible for the services to receive and record telecommunications by *untargeted* interception. They may only do so with respect to non-cablebound telecommunications, meaning communication traffic over the air. This relates in particular to the interception of telecommunication traffic via satellites.[214] Article 27 ISS Act 2002 does not confer the power of untargeted interception of cablebound telecommunications.

The term *untargeted* is used, because it is not clear in advance what will be found and whether what is found will contain any data that is relevant for the services. The interception is not targeted at communications originating from a specific person or organisation or related to a specific technical characteristic; all data traffic sent via a specific satellite channel is, as it were, plucked from the ether (bulk).

During the activity of untargeted interception and recording of communications, there is no examination of communication content yet. The bulk data is simply stored in the computer systems. The services are not allowed to do anything with the intercepted and stored telecommunications, except undoing the encryption if the data is encrypted (article 27(1) ISS Act 2002). The services do not require permission for this untargeted interception and recording of data (article 27(2) ISS Act 2002), because the legislator held that there was as yet no infringement of privacy, more in particular of the privacy of the telephone and telegraph. The legislator noted with respect to this power that it saw little added value in imposing a requirement of permission, which would only relate to the satellite channel targeted by the interception and would therefore have little substantive meaning.[215]

If, however, a service wishes to examine communication content, which in principle infringes a person's privacy, it must apply to the minister concerned (for GISS this is the minister of the Interior and Kingdom Relations, for DISS the minister of Defence) for permission to select the bulk data acquired by untargeted interception, and after obtaining permission it may examine the part of the intercepted data to which the selection criteria apply. Article 27(3) ISS Act 2002 regulates the power to select:

> "The services may select the data collected by exercising the power provided in paragraph (1), on the basis of:
> a. data relating to the identity of a person or an organisation;
> b. a number as referred to in article 1.1(bb) of the Dutch Telecommunications Act, or a technical characteristic;
> c. search terms relating to a specified subject."

The selection criteria mentioned under a and b may, for example, be a name, address details (under a) or a telephone number or IP address (under b). Collecting data on the basis of these

[214] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 44.
[215] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 44.

selection criteria concerns specific persons and organisations, which is why it is referred to as *targeted* searching. For this reason, selection based on these data is governed by the same rules that apply to the deployment of article 25 ISS Act 2002, which means that exclusively the minister of the Interior and Kingdom Relations is competent to give permission for a period of three months at most, after which the service may apply for renewed permission for a similar period.

The deployment of the power of "targeted" data selection infringes privacy. The severity of the infringement depends on the actual circumstances of the case and cannot be simply equated with the severity of privacy infringement by the measure of telephone tapping. One factor that plays a role is that selection after untargeted interception does not lead to the service having intercepted and recorded all communications of a specific person or organisation, but only those communications which are found in the bulk and which have therefore been intercepted "accidentally". This does not change the fact that selection after untargeted interception can certainly be severely infringing, when a service can intercept the communications of many different satellites and has good capability to filter the communications bulk. The only difference with telephone tapping in such a case is the moment of examining communication content. In the case of telephone tapping this usually happens *real time*, i.e. at the time the communication takes place, while in the case of selection after untargeted interception the service examines communication content after the communication took place. This distinction is not so very great, however, since the service frequently does not listen to telephone tap recordings until later, while in the case of selected communications it is not always certain that the addressee has already read a communication at the time the service examines its content.[216]

Different rules have been laid down for selection on the basis of search terms relating to a specified subject (selection criterion c). In this case the collection of data is not directed at a person or organisation, but is important for the investigations on which a service is working (e.g. the proliferation of chemical weapons) in the general sense.[217] In this case the search terms do not relate to persons or organisations, but to a specific subject. When this power was introduced into the ISS Act 2002, the following explanation was given:

> "A list of search terms relating to a subject will as a rule consist of (combinations of) specific technical terms and specifications in various languages. Lists are prepared in such a way as to result in optimal use of the selection system to find the desired information. A list of search terms to be used for an investigation into the proliferation of certain dual-use goods to a specific country or region may for instance include the names of certain chemical substances and chemical compounds in combination with these countries or regions. A somewhat simplified example is the search for messages in which the word sodium (or the Dutch equivalent *natrium*) occurs and also within two positions the word chloride or fluoride. A list of search terms for the purpose of an investigation into the export of a missile system to certain countries or regions might consist of various names used to refer to the specific missile system, project names, if applicable, or designations of the various elements forming part of the system in question."[218]

Just as in the case of article 25(2) ISS Act 2002, the services are not authorised to examine on the basis of search terms whether the non-cablebound telecommunications received and recorded by untargeted interception include data that is relevant for the investigation until

[216] An e-mail communication, for example, may be left unread in the inbox for a long time.
[217] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 45.
[218] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 33.

the service in question has obtained permission to use the power to select from the minister concerned (article 27(4) and (5) ISS Act 2002). Since this selection does not directly affect the privacy of persons and organisations –the collection of the data *did not target* any persons or organisations – the minister concerned may grant permission to select for the purpose of a specified subject for a longer period, viz. for one year at most. The application for permission must at least contain a detailed description of the subject and the reason for selection (par. 5). According to the legislative history these requirements safeguard that the minister will have the necessary understanding of the matter when deciding whether to grant permission. The search terms relating to the subject have no added value for such understanding. As a rule a list of search terms relating to a subject will consist of (combinations of) specific technical terms and clues in various languages. Since the search terms may change frequently, the law further provides that the search terms may be determined by the head of the service or by an officer designated by him on his behalf (par. 6). Lists are prepared in such a way as to result in optimal use of the selection system to find the desired information. GISS has opted to have this power exercised exclusively by the head of GISS. The DISS Submandating and Authorisation Decree 2009 authorises the head and the analysts of the Sigint department of DISS to determine the search terms.[219] It was decided in the legislative history that the power to select referred to under c must be exercised very selectively (mainly restricted to satellite traffic) and with restraint.[220]

It cannot be ruled out that data not selected in a selection based on selection criteria as referred to in article 27(3) ISS Act 2002 and whose actual content may therefore not be examined, nevertheless contains relevant information and might still be selected after all on the basis of selection criteria subsequently determined. Such subsequent selection criteria may stem from information derived from other sources of a service or derived from data intercepted and recorded at a later point in time.[221]

An example taken from the legislative history. Searching on the basis of search terms (article 27(3)(c) ISS Act 2002) occasionally results in the selection of messages showing that a ship is carrying chemicals or goods that can be used for the production of weapons of mass destruction, though it is not clear from the intercepted messages who is the supplier or buyer of the goods. Using new search terms derived from the messages intercepted in the first search, the service can then examine whether it is possible to find supplementary information about supplier and buyer in data traffic already intercepted by earlier searches, but which had not been selected. Sometimes, moreover, it is possible to establish in this way whether the relationship between supplier and buyer has already existed for some time. If the service should have to destroy the data originating from telecommunications intercepted and recorded pursuant to Article 27(1), ISS Act 2002 immediately after the first selection, it would not be able to do a subsequent selection – as outlined above – offering a possibility of further enlarging and supplementing information that is relevant to current investigations. The legislator considered this an undesirable situation. Subject to conditions, the service should have the opportunity to do such a subsequent selection, which therefore implies a certain period of retention of the data in question.[222]

Pursuant to Article 27(9), ISS Act 2002, data obtained from non-targeted interception which has not been selected may be retained for further selection purposes for up to one year. The

---

[219] *Official Gazette* no. 7168, article 3(1) under e and j.
[220] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 45.
[221] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 26-27.
[222] *Idem*.

Act stipulates two conditions for this. Selection may only take place in the context of an investigation based on a reason as referred to in paragraph 4(b) or in relation to a subject as referred to in paragraph 5(a), for which permission had been granted at the time the data in question was intercepted and recorded (paragraph 9(a)). The legislator did not consider it desirable that such data should also become available for selection in the context of service investigations that were not being conducted at the time the telecommunications were intercepted and recorded, since the telecommunications were intercepted for the purpose of investigations being conducted at the time of the interception. In addition, further selection must also be urgently necessary for the proper execution of the investigation concerned (paragraph 9(b)). According to the legislative history, these conditions were included because unrestricted and unconditional further selection of intercepted data is unlawful. It is barred by Article 8 ECHR.[223]

Article 27(10), ISS Act 2002 provides that paragraph (9) applies by analogy to data that has not yet been decrypted, with the proviso that the one-year retention period does not begin to run until the time of decryption.

V.2.6 Article 28 ISS Act 2002

Article 28(1) ISS Act 2002 provides the following power:

> "The services are authorised to apply to providers of public telecommunication networks and public telecommunication services within the meaning of the Telecommunications Act with the request to provide data pertaining to a user and to the telecommunication traffic relating to this user. The request may only relate to data designated by general administrative measure and may concern data already processed at the time of the request as well as data that will be processed after the time of the request."

By virtue of this provision the services are authorised to demand public telecommunication networks and public telecommunication services to give them access to (telephony) traffic data. They may only exercise the power with respect to a "user", i.e. a specific person. Article 28 ISS Act 2002 may not be deployed to make general or untargeted requests to provide (telephony) traffic data. The power pertains exclusively to the categories of traffic data designated by a general administrative measure in an exhaustive list.[224] The general administrative measure pursuant to article 28 ISS Act 2002 defines traffic data as data concerning the user and the telecommunication traffic relating to this user. For the purpose of this Decision the term traffic data has a broader meaning than in the Telecommunications Act, because it also covers user data, such as name, address, city, number and the type of service which the user is using or has used. According to the Explanatory Memorandum to the Decision the services must use the system and procedures at the Central Information Point for Telecommunications (CIOT) for demanding access to user data.[225] The services have a special power to do so pursuant to article 29 ISS Act 2002. The Decision defines the

---

[223] *Idem*.

[224] Article 2 of the Decision under article 28 ISS Act 2002: A request may relate to data regarding a user (name, address, city, number), regarding the persons or organisations with whom or which the user is or was connected or tried to make a connection, or who or which tried to make a connection with the user (name, address, city, telephone number), data concerning the connection itself (starting time, ending time, terminal equipment location data, terminal equipment numbers), and data concerning the subscription (the type of service used by the user, the data of the party paying the bill).

[225] Explanatory memorandum to the Decision under article 28 ISS Act 2002, available at http://wetten.overheid.nl.

term telecommunications as including not only cablebound telecommunications but also all forms of telecommunication transferred, transmitted or received via public networks or services, such as mobile telecommunications, telecommunications via cable and via satellites. Pursuant to the Decision the services can demand access to *inter alia* data on the dates and times when a person made calls, the telephone numbers the person contacted and the location.[226] They can demand access to data concerning outgoing traffic: traffic involving numbers that have been or are being called or with which connections have been made or are being made from a number specified in the demand. They can also demand access to data on incoming traffic: traffic involving numbers from which a number specified in the demand has been or is being called or has been or is being connected.[227]

Article 28(1) ISS Act 2002 provides that a demand for access may concern data already processed at the date of the demand as well as data that will be processed after the date of the demand. This means that the services may ask telecommunication providers about a person's calling behaviour in e.g. the past month, but also to be kept informed of a person's calling behaviour in e.g. the next two weeks. In the latter case a technical facility makes it possible for the services to have real time access to the data relating to a person's calling behaviour. This is sometimes called a "silent tap" because it does not involve examination of communication content.

The European Data Retention Directive (2006)[228] had the objective of harmonising the obligations imposed by the national laws of the Member States on providers of electronic communications services or public communications networks to retain certain telecommunications data (traffic and location data and user data) for a specified period for the purpose of combating serious crime. In the Netherlands the Directive was implemented in the Telecommunications Data Retention (2009). This resulted in the introduction of statutory retention periods in the Telecommunications Act (article 13(2)a: twelve months for telephony-related data, six months for data relating to internet connections. Pursuant to article 13(4) of the Dutch Telecommunications Act, providers of public telecommunications networks and services are obliged to provide specific information or data if GISS or DISS demand access thereto pursuant to article 28 or article 29, respectively, (duty of cooperation).[229]

Article 28 ISS Act 2002 does not purport to enable the services to examine the content of the communications taking place via telephone connections. In that case they would have to apply for permission of the minister concerned pursuant to 25 ISS Act 2002, because it would involve receiving (any form of) telecommunications. The difference arose indirectly in the drafting process of the ISS Act 2002 when the issue of monitoring military data traffic was discussed:

> "We believe that the privacy of the telephone is violated if the content of a telephone conversation is examined with a view to learning the content itself. If the content of a telephone conversation is examined purely as a brief element of an investigation into the

[226] See article 2 of the Decision under article 28 ISS Act 2002 for an exhaustive list of the data to which the services may demand access.
[227] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 46.
[228] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, entered into force on 3 May 2006, *OJ EU*, L105/54.
[229] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 37.

> identity of persons or institutions communicating with each other, we do not consider this to violate the privacy of the telephone. Rather, it [Committee: monitoring military traffic data] is comparable to examining traffic data. Such an examination must be considered to infringe the right to privacy, as enshrined in article 10 Constitution, but not the privacy of the telephone enshrined in article 13 Constitution."[230]

The services do not require the permission of the minister concerned (article 28(3) ISS Act 2002) for demanding access to (telephony) traffic data. It is sufficient that the head of the service demands that telecommunication providers give access to the data concerned (article 28(4) ISS Act 2002). The reasons for not imposing the requirement of permission are connected with the fact that the power is hardly infringing and with its expected use. The legislative history shows that the power regulated in article 28 ISS Act 2002 is considered less infringing than a telephone tap, because the latter involves examination of the content of calls. It was expected that a demand for access under 28 ISS Act 2002 would often precede an application for a telephone tap, because article 28 ISS Act 2002 can be used to collect further data that may be relevant to the decision whether and, if so, with respect to which person or organisation a telephone tap is considered necessary. If this is the case, article 28 ISS Act 2002 can help to limit the deployment of the more infringing means of telephone tapping to those cases in which it is considered absolutely necessary.[231]

In the explanatory memorandum to the bill introducing rules on demanding access to telecommunications data in the Dutch Criminal Code, consideration is given to the fact that traffic data may provide insight into the telecommunications behaviour of a user and into a person's pattern of contacts, which may yield a more or less complete picture of specific aspects of a person's life. As a result, demanding access to these data may infringe the privacy of the person concerned.[232] In that case it is important that the requirements set by the ECHR such as the quality requirements for the legislation and sufficient statutory safeguards against arbitrariness and abuse are satisfied (see section II.2 on this subject). Pursuant to the explanatory memorandum to the bill all this does not apply to user data, i.e. data which help identify a person, such as name, address, city, number and type of telephone service, since this is a much more limited category of data.[233] There is the possibility, however, that the data is used for a different purpose from the one for which the provider processed it. Pursuant to the Data Protection Convention of the Council of Europe, data may be used for a different purpose where this is provided for by law and subject to appropriate safeguards, and provide it is necessary for a legitimate purpose and is not excessive.[234]

V.2.7 Article 29 ISS Act 2002

Article 29(1) ISS Act 2002 provides as follows:

> "The services are authorised to apply to providers of public telecommunications networks and public telecommunications services within the meaning of the Telecommunications Act and demand access to data relating to name, address, postal code, city, number and type of service of a user of telecommunications."

---

[230] *Idem*, p. 35.
[231] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 47.
[232] *Parliamentary Papers II* 2001/02, 28 059, no. 3, p. 4.
[233] *Idem*, p. 5.
[234] *Idem*, p. 6.

This power relates to demands made to providers of public telecommunications networks and services for access to user data or subscriber data (so-called name and address data, numbers of the user and the type or types of services which the user is using or has used[235]) relating to a natural person or legal entity who/which has entered into an agreement with the provider regarding the use of a public telecommunications network or the provision of a public telecommunications service, or relating to a natural person or legal entity who/which is using the service (par. 2). The power may only be exercised with respect to a 'user", i.e. a specific person. Article 29 ISS Act 2002 cannot be used for general or untargeted demands for access to user data.

Just as in the context of article 28 ISS Act 2002, providers of public telecommunications networks and services are obliged pursuant to the Telecommunications Act (article 13.4) to give GISS and DISS access to specific information or data to if they so demand on the basis of the special power in article 29 ISS Act 2002.[236]

Pursuant to paragraph (4) of article 13.4 Telecommunications Act, the Central Telecommunications Investigation Information Point (Dutch abbreviation: CIOT) was established by the Telecommunications (Provision of Data) Decree (the "CIOT Decree"), which also lays down rules on which user data providers must retain to meet demands for access as well as the procedure for demanding access to the data via CIOT.[237] Demands from the services for access to user data are made via CIOT using a computer system.

If a service needs the data to enable it to apply for permission to tap (article 25 ISS Act 2002), it must demand access to the data pursuant to par. 7 of this article. According to the legislative history article 29 ISS Act 2002 may also enable the services to carry out an investigation if a telephone number comes into their possession which is possibly used by a person who is e.g. involved in terrorist activities and if this number may lead to that person´s place of abode.[238]

Although the power embodied in article 29 ISS Act 2002 is not considered to be severely infringing, it is nevertheless a special power – even though the legislative history does not expressly state the reason why – which for this reason, like the power embodied in article 28 ISS Act 2002, must be deployed with respect to a specific target, and reasons must be stated (internally) which substantiate the necessity, proportionality and subsidiarity of the deployment, even though the law does not require reasons to be laid down in writing.[239]

VI Cooperation with foreign intelligence and/or security services

VI.1 Article 59: duty of maintaining relations

[235] It follows from article 2(g) that the term "services" includes both the telecommunications services within the meaning of the Telecommunications Act, which involve transferring signals via telecommunications networks, and related facilities such as call forwarding feature or a computerised answering feature; explanatory memorandum to the Decision under article 28 ISS Act 2002, available at http://wetten.overheid.nl.
[236] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 37.
[237] Decree of 26 January 2000, Bulletin of Acts and Decrees 2000, 71.
[238] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 48.
[239] CTIVD review report no. 25 on the conduct of DISS with respect to two suspended employees, *Parliamentary Papers* II 2009/10, 29 924, no. 59 (appendix), section 4.2, available at www.ctivd.nl.

Article 59,(1) ISS Act 2002 imposes a duty on the heads of GISS and DISS to maintain relations with intelligence and/or security services in other countries that qualify for such relations.[240] It is recognized in legislative history that cooperation with intelligence and security services of other countries is essential for the effective and efficient operation of the services, precisely and particularly on account of the transnational and international nature of security problems.[241] It is necessary for the adequate performance of tasks by the services that they cooperate with foreign services where possible.[242]

In principle the cooperation by GISS and DISS with foreign services must comply with the generally applicable provisions on data processing laid down in the ISS Act 2002. Paragraphs (2)-(6) of article 59 ISS Act 2002 provide for a number of possibilities to cooperate with other services if GISS or DISS do not have a direct interest in doing so. This therefore constitutes an exception to the principal rule that in principle GISS and DISS cooperate with other services in the context of the performance of their own tasks.

It is stated in the legislative history that GISS will maintain contacts with civil intelligence and/or security services and DISS with military intelligence and/or security services and with intelligence liaison services. When the performance of tasks by the services so requires, the heads of GISS and DISS will inform each other when it is necessary to contact military or civil foreign services, respectively,.[243]

Cooperating with foreign intelligence and security services is important for national security. One must bear in mind, however, that such cooperation, and in particular exchanging data, may entail interference with the fundamental rights of citizens. This will by definition be the case where it concerns the exchange of personal data. This may have far-reaching consequences for the privacy of individuals. The legislator recognized this inherent tension. When working out the rules and procedures applying to cooperation between services the legislator sought to strike a balance, just as it did throughout the entire ISS Act 2002, between the national security interest served by cooperating with foreign services and the interest of the fundamental rights of citizens that is threatened by such cooperation, in particular by the exchange of (personal) data. Several important safeguards are embodied in the law and the legislative history aimed at protecting the privacy of citizens. These are discussed below.

GISS and DISS may not simply enter into a cooperation relationship with any foreign service. It was determined in the legislative history that a number of matters must be examined before GISS or DISS may enter into a cooperation relationship with an intelligence and/or security service of another country. The services must assess the degree of democratic anchorage of the service and its respect for human rights, its professionalism and reliability, the nature of the service, whether international obligations make cooperation desirable and to what extent cooperation with a service can enhance national security.[244] Based on these criteria GISS and DISS must assess whether a foreign service qualifies for cooperation and which forms of cooperation are in principle permissible. In principle, this assessment is done

[240] See for a detailed discussion of this subject CTIVD review report no. 22a on the cooperation of GISS with foreign intelligence and-or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), available at www.ctivd.nl.
[241] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 73.
[242] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101.
[243] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 73.
[244] *Parliamentary Papers II* 2000/01, 25 877, no. 59, p. 16. See also CTIVD review report no. 22a on the cooperation of GISS with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), section 5, available at www.ctivd.nl.

at the level of the service itself. The minister concerned is informed about the assessment. If a service considers cooperating with a so-called "risk country", the minister must be involved in the decision-making process.[245]

The activities of GISS and DISS that take place in the context of cooperation with foreign services must comply with the provisions on data processing laid down in the ISS Act 2002. Where the cooperation takes place in the interest of the foreign service, article 59(2)-(6) ISS Act 2002 applies. With regard to the specific forms of cooperation mentioned in article 59 ISS Act 2002 (namely: providing data and giving technical support to a foreign service) this article provides that they may only take place if the interests served by the foreign service are not incompatible with the interests served by the Dutch service and if the cooperation is not incompatible with the proper performance of its tasks by the Dutch service. According to the legislative history the question whether conflicting interests exist must be assessed among other things on the basis of Dutch foreign policy, including its human rights policy.[246] Sometimes the interests served by the service have been translated into concrete and established government policy, such as the human rights policy, but often this is not the case. There are a multitude of interests.[247] It was not considered necessary to include a guideline in the services' task description. The Act provides that GISS and DISS must perform their tasks in accordance with the law (article 2 ISS Act 2002). This means that the standards, and definitely also the fundamental rights and human rights, enshrined in the Constitution and in the international conventions (including the ECHR) that have been ratified by the Netherlands, must also be counted among the interests served by the services.[248] As regards the question when the proper performance of tasks by the services is incompatible with their providing data or technical support to a foreign service, this will be the case for example if the provision of data would frustrate current operations of GISS or DISS itself. In the same context the services must also assess whether the request does not exceed the legal parameters within which the services must operate.[249]

In practice, cooperation between services entails certain restrictions to the transparency about the origins of shared data. In the legislative history this fact was indeed recognized where it is stated that in transactions between services it is not common practice to actively inquire about the methods of the other party or actively inform it about the methods used to obtain specific information. Just like GISS and DISS, foreign services prefer to keep their sources and methods secret.[250] With regard to human sources this is usually a statutory duty, as it is for GISS and DISS (article 15 ISS Act 2002). Depending on the nature of the cooperation relationship with a foreign service it may be possible to pursue greater openness on this point, particularly in the case of joint operations.[251]

---

[245] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 102 and *Appendix Proceedings II* 2004/05, no. 749.
[246] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 74.
[247] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101.
[248] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 65.
[249] *Parliamentary Papers II* 2000/01, no. 14, p. 64.
[250] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 63.
[251] *Idem.*

VI.2 Providing data

VI.2.1 Legal basis

The ISS Act 2002 has a closed system of permitted data provision, which means that external provision of data, i.e. to other persons or bodies, is only permitted if there is a specific legal basis for doing so.

De ISS Act 2002 provides two legal bases for providing data to foreign services. Article 36(1)(d) ISS Act 2002 is the legal basis for providing data for the purposes of the Dutch services' own task. This subparagraph provides that the services are authorised to forward data processed by or on behalf of the service to eligible intelligence and security services of other countries and to eligible international security bodies, signals intelligence bodies and intelligence bodies.

If the interest of the foreign services is the predominant interest, then article 59(2) ISS Act 2002 is the legal basis for the provision of data. This paragraph provides that the Dutch services may, in the context of maintaining relations with eligible intelligence and security services of other countries, provide data to these services for the purpose of the interests served by them.

The explanatory memorandum shows that a distinction must be made between the two forms of data provision, pursuant to article 59(2) ISS Act 2002 and pursuant to article 36(1) ISS Act 2002. Data provision pursuant to article 36 ISS Act 2002 takes place in the context of the proper performance of tasks by the Dutch services, while in the case of data provision pursuant to article 59 ISS Act 2002 the interest of the foreign service in the data provision is predominant. In the case of data provision pursuant to article 59 ISS Act 2002 the main consideration is that of maintaining good cooperation relationships with the eligible foreign service.[252] If GISS or DISS possesses data which may be relevant for a foreign service but which may not be provided pursuant to article 36(1)(d) ISS Act 2002, the data may – under certain circumstances – be provided to the foreign service without thus contributing to the proper performance by GISS or DISS of its own task. A foreign service may, for example, request data relating to a person or organisation who or which is not being investigated by GISS or DISS itself. When GISS or DISS has the requested data in its possession, the service may provide the data under article 59(2) ISS Act 2002. In such cases the data provision does not make a contribution to any concrete current investigation of the Dutch service. In most cases, however, data is provided to foreign services pursuant to article 36 ISS Act 2002.

Actually, both types of data provision to foreign services take place in the interest of national security. This is evident where data is provided for the purpose of the performance of the services' own tasks, but even when data is provided for the purpose of maintaining relations with foreign services and the provision predominantly serves the interest of the foreign service, it also serves the interest of national security. This is closely linked with the principle of reciprocity (*quid pro quo*). Cooperation between services is not a one-way process. It is not so that only GISS and DISS may request foreign services to provide data that is relevant to the performance of their tasks, foreign services, too, may consider it important to obtain specific data from the Dutch services. In principle the services should take a positive approach to such requests in order to ensure that requests from GISS and DISS will – in their

[252] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101.

turn – meet with a similar approach.[253] Complying with requests from friendly foreign services indirectly serves a service's own national security, because over time the foreign service can be expected to return the favour, if needed.[254]

VI.2.2 Safeguards

The preceding section outlined a framework of safeguards applying to cooperation with foreign services. This section addresses a number of safeguards relating specifically to the exchange of (personal) data.

When GISS or DISS is considering whether to provide (personal) data to a foreign service in a specific case, it must first examine whether this form of cooperation fits within the general assessment of the service in question on the basis of the aforementioned general criteria. In this connection it should be pointed out that excluding any and all forms of cooperation with services that do not meet the criteria for cooperation could have disastrous consequences. Some channels of communication should always be kept open to receive information on acute, life-threatening situations.

The general rules on data provision apply to the provision of data to foreign services. In principle, therefore, the same system of standards is applicable. Data provision must satisfy the general requirements set for data processing (article 12 ISS Act 2002) and must therefore take place for a specific purpose and only to the extent necessary for the proper implementation of the law, and with due observance of the standards of proper and due care. The services may only provide data to a foreign service in the context of performing their own tasks under article 36 ISS Act 2002 if disclosure of the data to be provided to the foreign service in question is necessary in the interest of national security.

Providing data to foreign services under article 59(2) ISS Act 2002, where this predominantly serves the interest of the foreign service, is only permitted if providing the data is necessary in the context of maintaining contacts with the foreign service in question. As stated above, maintaining contacts with foreign services (indirectly) serves the interest of national security. The Committee notes that the provision of data in the interest of the foreign service can be readily assumed to be necessary on the basis of the duty of the Dutch services to maintain relations and on the basis of the principle expressed in the legislative history that the services should take a positive approach to requests from friendly services.[255]

Data is usually provided subject to the condition of the so-called third party rule, according to which data obtained from a counterpart may only be passed on to third parties if the service that originally provided the data has given permission to do so (article 37 ISS Act 2002). According to the legislative history of the Act this rule is an essential condition in international cooperation:

> "If a service cannot rely on the addressee country to keep the data secret and using it exclusively for its own information, there can be no question of any real cooperation between the services concerned. If a service gets the impression that the rule is not observed, it will stop or marginalise the exchange of data with that counterpart."[256]

---

[253] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 73; *Parliamentary Papers II* 1999/2000, 25 877, no. 8. p. 101.
[254] *Parliamentary Papers I* 2001/02, 25 877, no. 58a, p. 24
[255] *Parliamentary Papers I* 2001/02, 25 877, no. 58a, p. 24.
[256] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 57.

Some intelligence and/or security services proceed on the basis of the "third *country* rule" which gives a wider interpretation to the international rule. In principle the third country rule allows data originating from a foreign counterpart to be passed on between the intelligence and security services of the same country, unless the providing service has expressly precluded it.

Compliance with the third party rule is an important safeguard in cooperation relationships between intelligence and security services. For one thing, the rule contributes to source protection, the possibility of interchanging secret information and the mutual trust that is the basis for a cooperation relationship between intelligence and security services. Furthermore, the rules ensures control over the further disclosure of data. This reduces the likelihood that information originating from one single source finds its way to several parties, who in their turn pass on the information, with the result that subsequently the information seems to originate from several sources. The uncontrolled further provision of information may also have the result that remarks made by the providing service concerning its reliability are lost.

The provision of personal data to a foreign service infringes the privacy of the person concerned. With regard to the provision of data to foreign intelligence and security services the legislative history of the Act makes a distinction between personal data and other data. A service must take special care when providing personal data. When GISS or DISS wish to provide personal data to a service of a country whose respect for human rights may be doubted, the personal data may only be provided if and to the extent that an urgent necessity (inevitability) exists on account of an unacceptable risk to society and its citizens and which requires quick action (e.g. innocent civilians are in danger of falling victim to terrorist attacks).[257] In addition, the provision of personal data to foreign services must be done in writing (article 40(1) ISS Act 2002) and records must be kept of all such data provisions (article 42 ISS Act 2002).

VI.3 Receiving data

In international traffic between services and in the principle of reciprocity (*quid pro quo* or "one good turn deserves another") that applies in this traffic, there is a significant link between the acquisition of data from foreign services and the provision of data by GISS and DISS. The legislative history includes the observation that for GISS or DISS to be able to obtain as complete a picture as possible of a specific subject, it is desirable that they have the possibility of asking an eligible service whether it possesses information on the subject in question or, if this is not the case, whether that service can use its contacts to obtain information on the subject. According to the legislator, certainly the intelligence and/or security services of large countries have data collections and contacts of such a nature that they may include valuable information for GISS and DISS.[258] The data obtained by cooperating with these services substantially reinforces the existing information position of GISS and DISS, thus enhancing their capability to assess risks to national security and give the responsible authorities timely warning of such risks.[259] If foreign services possess data that may contribute to the proper performance of their tasks by GISS or DISS, it is important for them to be able to obtain this data.[260] The ISS Act 2002 does not expressly provide for the

[257] *Parliamentary Papers II* 2000/01, 25 877, no. 59, p. 16.
[258] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 73.
[259] *Idem*, pp. 73-74.
[260] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101.

possibility of requesting and receiving data from foreign services, but it is implied in article 59 ISS Act 2002 which pertains to maintaining relations with foreign services. A request made by a Dutch service to a foreign service must, however, satisfy all the criteria applying to data processing.

By virtue of international human rights conventions and the Dutch Constitution, moreover, GISS and DISS must refrain from using data acquired from foreign services if there are concrete indications that the data has been obtained by torture. It is only in highly exceptional emergency situations that the services may (or even must) deviate from this rule. In practice, however, it proves to be virtually impossible for the services to ascertain in concrete cases whether data provided by a foreign intelligence or security service was obtained by torture. This is due to the fact that intelligence and security services maintain strict secrecy about their information sources and methods in their reciprocal dealings. Moreover, a service will never say it has obtained information by torture. However, this lack of certainty may not result in any and all forms of cooperation with certain foreign services being completely ruled out in advance. In this connection, moreover, it is all the more important that a service carefully assesses, prior to cooperating with a foreign intelligence and/or security service, to what extent the human rights situation in a country stands in the way of cooperating with the relevant service of that country. In addition, as a cooperation relationship continues or takes different forms, GISS or DISS will also have to reconsider what is the maximum level at which they may cooperate with such a service.[261]

Foreign services usually provide data on a request from GISS or DISS or on the basis of agreements. In the legislative history of the Act it was considered that foreign services that perform services for GISS or DISS will have to duly observe the legislation and regulations applicable to them, since the same applies in the reverse situation. This means that when these foreign services acquire data they must do so with due observance of the legal parameters applying to them.[262] Although the foreign service has a responsibility of its own to assess a request for data from a Dutch service, this does not mean that the Dutch services are free to address any request they deem advisable to foreign services. A request for data addressed to a foreign service must be necessary for the performance of its tasks by the Dutch service and it must satisfy the standards of proper and due care (article 12 ISS Act 2002).

VI.4 Technical support and other forms of support

In addition to exchanging data, there are other ways in which the services cooperate with foreign services. Operational cooperation, for example, may take the form of carrying out joint operations which usually involves the exercise of special powers. The services exercise these powers (in part) for the purpose of performing their own tasks, to which the general rules regarding data processing embodied in the ISS Act 2002 apply, including the provisions regarding the deployment of special powers.

Article 59 ISS Act 2002 provides for the possibility for GISS and DISS to cooperate with other services in certain cases without the Dutch services promoting their own interests thereby.

---

[261] For a discussion of this subject with regard to GISS see: CTIVD review report no. 22a on the cooperation of GISS with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), section 5.1, available at www.ctivd.nl.
[262] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 62.

Within the context of maintaining relations with foreign intelligence and security services the Dutch services may, pursuant to article 59(4) ISS Act 2002, give technical and other forms of support to foreign services for the purpose of the interests served by these foreign services. Giving technical and other forms of support is subject to similar conditions as those imposed on the provision of data in the interest of the foreign service. Support may only be provided insofar as the interests served by the foreign service are not incompatible with the interests served by the Dutch service (under a), and the proper performance of the tasks by the Dutch service is not incompatible with providing the support (under b).

By way of example of a situation in which the proper performance of its statutory tasks by the Dutch service is incompatible with providing support to a foreign service the legislative history mentions the case that giving support would frustrate ongoing operations of GISS or DISS itself. It is also pointed out that the type of support requested is relevant, too. It must, among other things, fit within the legal parameters which the services must observe. If a specific form of support is incompatible with those parameters, giving the support notwithstanding would be contrary to the proper performance of tasks.[263]

According to the legislative history, the expectation is that requests for support will usually concern the exercise of specific special powers, such as shadowing and surveillance actions. These must be exercised with due observance of the statutory regulations applying to the special powers.[264] This means among other things that GISS or DISS must satisfy the criterion of necessity (article 18 ISS Act 2002). Any support given by deploying special powers must also satisfy the requirements of proportionality and subsidiarity embodied in articles 31 and 32 ISS Act 2002. The Committee notes that giving support in the interest of the foreign service can be readily assumed to be necessary on the basis of the duty of the Dutch services to maintain relations with eligible foreign services and on the basis of the principle expressed in the legislative history that the services should take a positive approach to requests from friendly services.[265] In addition, the Dutch service must weigh the proportionality and the subsidiarity of deploying a special power for support purposes in the sense that it must assess whether the means is proportional to the intended purpose and whether using a less infringing means will not be sufficient.

Pursuant to Article 59, paragraphs (5) and (6), ISS Act 2002 support may only be provided with the permission of the minister concerned. The minister may mandate this power to grant permission but exclusively to the head of the service and only with respect to requests of an urgent nature (for example cross-border shadowing and surveillance activities), subject to the condition that the minister must be informed immediately of any permission granted. The power to give permission for providing technical and other forms of support is vested at this (high) level on account of the potential political aspects inherent to providing support.[266] The support is subsequently provided by the service which falls under the minister and is carried out under the responsibility of the minister concerned.[267]

Every independent action of a foreign service within the territory of the Netherlands constitutes infringement of Dutch sovereignty and will usually pose a threat to national security. This is the interest which the Dutch services have in taking action against such

[263] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 64.
[264] *Parliamentary Papers II* 1999/2000, 25 877, no. 9. p. 38.
[265] *Parliamentary Papers I* 2001/02, 25 877, no. 58a, p. 24.
[266] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101 and no. 9, p. 37.
[267] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 38.

practices. It is not permitted to authorise foreign services to carry out independent operations within the territory of the Netherlands.[268] Foreign services may only deploy legitimate activities within Dutch territory if the minister of the Interior and Kingdom Relations or the head of GISS has given them permission to do so and if they do so under the supervision and responsibility of GISS.[269] Responsibility for activities involving places in use by the Ministry of Defence lies with the minister of Defence and DISS.[270].[271]

The reverse situation is also possible: GISS or DISS may request a foreign service to provide (technical) support. To the extent foreign services do provide support to GISS or DISS they will have to do so with due observance of the regulations that are applicable to them. Foreign services must duly observe the statutory parameters when they exercise intelligence means within their own territory.[272] The possibility of requesting a foreign service to provide support is not regulated under the ISS Act 2002. This does not alter the fact that the Dutch services cannot simply request any and all forms of support from a foreign service. In an earlier report the Committee concluded that a request for support made to a foreign service involving an activity that qualifies as a special power under the ISS Act 2002, must satisfy the applicable requirements of necessity, proportionality and subsidiarity.[273] Furthermore, the Dutch services may not use requests to foreign services to "circumvent" the ISS Act 2002 and the special powers for the collection of data the Act confers on them, a construct that is sometimes referred to as sidestepping legal restrictions. For example, the Dutch services may not request a foreign service to collect data which they cannot acquire themselves because the ISS Act 2002 does not permit them to do so. On the other hand the services may request other countries to supplement their own (technical) capacity. According to the legislative history, this is precisely the purpose of international cooperation between services. The ISS Act 2002 and the legislative history do not expressly state that the services may not use the construct of sidestepping legal restrictions. But this does follow from the ISS Act 2002 interpreted as a whole, given the fact that article 2 ISS Act 2002 provides that the services perform their tasks in accordance with the law. In addition, the ISS Act 2002 provides for a closed system of (special) powers to collect data and furnish such data (to external parties). It follows from these provisions that the services are not permitted to use intelligence means and methods not regulated in the ISS Act 2002, and consequently they are also not permitted to do so in the context of cooperating with foreign services.

Thus adopted at the meeting of the Committee held on 5 February 2014.

---

[268] *Idem*.

[269] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 62-65; *Parliamentary Papers I* 2001/02, 25 877, no. 58a, p. 25.

[270] The Act also provides for the possibility of DISS exercising special powers in spaces not in use by the Ministry of Defence, provided permission has been granted in consultation with the Minister of the Interior and Kingdom Relations. See section III.

[271] *Parliamentary Papers I* 2001/02, 25 877, no. 58a, p. 25.

[272] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 62.

[273] CTIVD review report no. 22a on the cooperation of GISS with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), section 2.2, available at www.ctivd.nl.