

APPENDIX II

Assessment Framework

To the review report on bulk data sets collected using the hacking power and their further processing by the AIVD and the MIVD

CTIVD no. 70

[adopted on 19 August 2020]



Review Committee
on the Intelligence and
Security Services

APPENDIX II

To the review report on bulk data sets collected using the hacking power and
their further processing by the AIVD and the MIVD

Table of contents

1.	Introduction	3
2.	Introduction to the hacking power	7
2.1	Section 45 of the ISS Act 2017	7
2.2	Automated device or system	8
2.3	Exploration	10
2.4	Entry	10
2.5	Inherent investigatory powers after entry	14
3.	General framework for data processing	17
3.1	General requirements for data processing	17
3.2	Duty of care	18
3.3	Bulk data sets	19
4.	Requirements for exercising the hacking power	22
4.1	Authorization and assessment	22
4.2	Requirements for the use of general and special investigatory powers	23
4.3	Description of technical risks	25
4.4	Reporting	28
4.5	Clean-up obligation	29

5.	Safeguards for the further processing of bulk data from the hacking power	30
5.1	Requirement for data reduction	30
5.2	Safeguards for bulk data sets	31
5.3	Reporting	32
6.	Summary of legal requirements	33

APPENDIX II

To the review report on bulk data sets collected using the hacking power and their further processing by the AIVD and the MIVD

1. Introduction

It can be necessary for the AIVD and the MIVD to collect bulk data sets, from an operational perspective. Bulk data sets are large collections of data, the majority of which concerns organizations or people who are not the subject of investigation by the services, nor ever will be. In other words, data of people or organizations who are not under investigation. The ISS Act 2017 does not rule out the possibility of the services collecting bulk data sets based on their general and special investigatory powers.

The hacking power is one of the special investigatory powers which the AIVD and the MIVD can employ to collect bulk data sets. This is a special investigatory power with which to explore and enter an automated device or system and copy the data stored there (Section 45 of the ISS Act 2017). The use of the hacking power to collect bulk data is the focus of this investigation. This investigation ties in with other investigations by the CTIVD into the use of general investigatory powers when collecting bulk data, such as report no. 55 on bulk data sets on the internet and the investigation into passenger data.¹

As context and background, this legal framework first looks at the main characteristics of the hacking power. The requirements that apply to exercising this special investigatory power are then addressed. The CTIVD opted to restrict the current investigation to a number of elements of the hacking power that are new in the Act.² These elements are laid down in the Act to provide more legal protection and to mitigate certain concerns that exist in society about the use of this investigatory power. In specific terms, these are:

- The requirement of a lawfulness assessment by the Investigatory Powers Commission (TIB) of the authorization given by the minister for the use of the hacking power.
- The requirement of a description of the technical risks in the authorization request.
- A 'clean-up obligation' of technical aids once the use of the hacking power has ended.

¹ See review report no. 55 (published February 2018) on the acquisition by the AIVD and the MIVD of bulk data sets offered on the internet by third parties, *Parliamentary Documents II* 2016/17, 29 924, no. 155 (appendix); the investigation into passenger data (review report no 71).

² CTIVD has already conducted a broad review of the exercise of the hacking power in its review report no. 53 (published in April 2017) on the use of the hacking power by the AIVD and the MIVD, *Parliamentary Documents II* 2016/17, 29 924, no. 149 (appendix), available at HYPERLINK "<http://www.ctivd.nl>" www.ctivd.nl. The corresponding legal framework includes an extensive description of this investigatory power under the ISS Act 2002.

- Keeping records on the use of the hacking power, including logging of actions (Section 33 of the ISS Act 2002 (former) already stipulated that a written report must be made of the exercise of a special investigatory power; logging of actions is a recommendation in the CTIVD report no. 53 that was adopted by the ministers³).

These elements also serve as a safeguard where it concerns the collection of large amounts of data and careful conduct in that respect, although the scope is not limited to that.

The subsequent focus of the investigation is on the further processing of bulk data sets obtained with the hacking power. The hacking power is a severe infringement of the fundamental rights of people whose personal data is processed. Therefore it is essential that the fundamental rights of those involved who are not, nor ever will be, under investigation by the services be protected to a sufficient degree. The ISS Act 2017 does not contain any specific regulation for this, with the exception of bulk data from investigation-related interception, for which the ISS Act 2017 has a specific regime.⁴ Both the AIVD and the MIVD use their own safeguards when accessing and using bulk data sets. These extra safeguards stem from the general obligation to ensure data is processed properly and carefully (Sections 18-24 of the ISS Act 2017). The requirements and safeguards that apply to the processing of bulk data are discussed in this legal framework.

The legal framework in this appendix is based on the ISS Act 2017 and the Policy Rules, parliamentary history, previous relevant CTIVD review reports and the recommendations outlined in them, in so far as adopted by the ministers and relevant policy of the services. Where relevant and unchanged under the ISS Act 2017, this assessment framework mainly builds on the CTIVD review report no. 53 (April 2017) on the use of the hacking power under the ISS Act 2002 (former) by the AIVD and the MIVD⁵ and review report no. 55 (February 2018) on the acquisition by the AIVD and the MIVD of bulk data sets offered on the internet.⁶

The legal framework is structured as follows:

- A diagram of the legal process concerning the use of the hacking power under Section 45 of the ISS Act 2017 when collecting bulk data sets and the further processing of this information.
- S2: Discussion of the key characteristics of the hacking power under Section 45 of the ISS Act 2017 (compared with the ISS Act 2002 former).
- S3: Description of the general framework that applies to data processing, based on Section 18 (general requirements for data processing) and Section 24 of the ISS Act 2017 (duty of care for data processing). This also applies to the use of the hacking power and the further processing of data collected by that means. And a description of the term bulk data sets.

³ In their policy response to report no 53 (25 April 2017) the Minister of the Interior and Kingdom Relations and the Minister of Defence wrote that 'all recommendations by the CTIVD will be adopted, albeit that the retention periods and automated recording and logging in the new ISS Act 20xx, which is currently being debated in the Senate, have been addressed and will then be implemented.' (*Parliamentary Documents II* 2016/17, 29 924, no. 149).

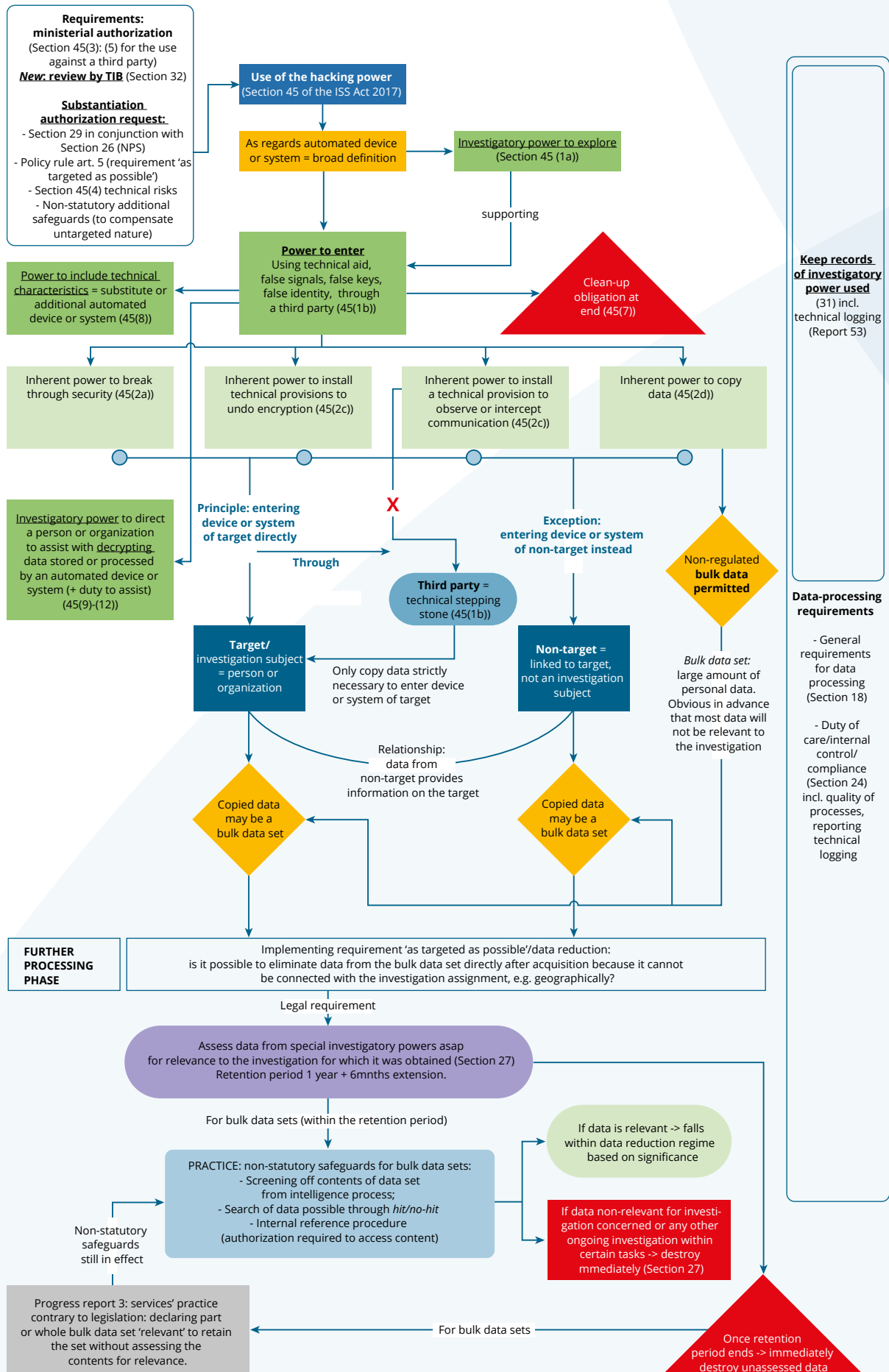
⁴ After the ISS Act 2017 entered into force on 1 May 2018, the CTIVD conducted an investigation into the application of filters and selection in investigation-related interception, see CTIVD review report no. 63 on the application of filters in investigation-related interception by the AIVD and the MIVD, *Parliamentary Documents II* 2018/19, 29 924, no. 188 (appendix) (Sept. 2019) and the CTIVD review report no. 64 on the application of selection in investigation-related interception by the AIVD and the MIVD (*Parliamentary Documents II* 2019/20, 29 924, no. 192 (appendix) (Oct. 2019).

⁵ CTIVD review report no. 53 (published in April 2017) on the use of the hacking power by the AIVD and the MIVD, *Parliamentary Documents II* 2016/17, 29 924, no. 149 (appendix), available at www.ctivd.nl.

⁶ CTIVD review report no. 55 (published February 2018) on the acquisition by the AIVD and the MIVD of bulk data sets offered on the internet by third parties, *Parliamentary Documents II* 2016/17, 29 924, no. 155 (appendix).

- S4: Description of the requirements for the use of the hacking power, such as the requirements of authorization and substantiation and keeping records on the exercise of this investigatory power.
- S5: Requirements and safeguards for the further processing of bulk data sets obtained by hacking.
- S6: Summary of the legal requirements

A diagram of the legal process concerning the use of the hacking power when collecting bulk data sets and the further processing of this data.



2. Introduction to the hacking power

2.1 Section 45 of the ISS Act 2017

The hacking power, as it is known, is a special investigatory power of the AIVD and the MIVD with which to collect data. It is regulated by Section 45 of the ISS Act 2017. This investigatory power was already in existence under the former ISS Act 2002, regulated by Section 24 of that former Act. The hacking power is also referred to as '*computer network exploitation*' (CNE).⁷

Section 45 of the ISS Act 2017 contains the investigatory powers to explore and enter automated devices or systems (subsection 1). When entering an automated device or system, the services have the following four 'inherent' investigatory powers, referred to in subsection 2:

- Breaking through the existing security of the device or system
- Installing technical provisions to undo encryption of data.
- Installing technical provisions to enable the exercise of certain other special investigatory powers, i.e. observing or intercepting communication of a target.
- Copying of data

The section contains a number of safeguards and requirements relating to the authorization requirement (2.3), the authorization request (2.4), access to a third-party device or system (2.5), direction of specialized staff to actually exercise the hacking power (2.6) and the obligation referred to as the clean-up obligation (2.7). The section further contains a power to include additional technical characteristics under the authorization (2.8) and, under certain conditions, a duty to cooperate with decryption (duty to decrypt) (2.9-2.12).

Section 45 of the ISS Act 2017 has been significantly expanded compared with Section 24 of the ISS Act 2002 (former). Unchanged in terms of wording are the investigatory powers to enter, to undo security, to install a technical provision to undo encryption and copy data. The ISS Act 2002 (former) also contained an obligation to cooperate with undoing encryption.

Section 45 of the ISS Act 2017 sets out a number of common operational practices and a number of new requirements, listed below:

- The investigatory power to *explore* the technical characteristics of an automated device or system, such as the digital environment of a subject of the investigation, including the exploration to detect any vulnerabilities (Section 45(1)(a) of the ISS Act 2017).⁸
- The investigatory power to enter through the automated device or system of a third party (Section 45(1)(b) of the ISS Act 2017). The same requirements (authorization and substantiation) apply as to entering that of a target (Section 45(5) of the ISS Act 2017). The application of the investigatory power to install a technical provision that enables that third-party to be observed and intercepted is expressly ruled out (Section 45 (5) of the ISS Act 2017).

⁷ Parliamentary Documents II 2016/17, 34 588, no. 3, p. 68.

⁸ Parliamentary Documents II 2016/17, 34 588, no. 3, p. 75.

- The investigatory power to install a ‘technical provision’ in an automated device or system *to support the exercise of certain other subsequent special investigatory powers*, such as observing and intercepting communication of a subject of the investigation using their automated device or system (Section 45 (2)(c) of the ISS Act 2017).
- The investigatory power to also allow the entry into automated devices and systems that *take the place of or that are an addition* to the automated device or system of a person (not only a target, also a third party) or the organization for which the original authorization to enter was given (Section 45(8) of the ISS Act 2017).
- The obligation for the AIVD and the MIVD, after ending the entry using a technical aid, to *remove that aid* and if that is not possible, to draw up a report on this (clean-up obligation) (Section 45 (7) of the ISS Act 2017).
- The *requirement of ministerial authorization* to use the investigatory power to explore and enter (Section 45(3) of the ISS Act 2017).⁹
- Specific, additional (above and beyond Section 29 of the ISS Act 2017) *requirements to authorization requests* for exploring and entering (the former ISS Act did not contain these) (Section 45(4) of the ISS Act 2017).
- The requirement of ministerial authorization and additional requirements (above and beyond Section 29 of the ISS Act 2017) to the authorization request for the investigatory power to compel someone to help in undoing encryption (Section 45 (10 and 11) of the ISS Act 2017).
- In addition to the law, a policy rule (article 5) stipulates that special investigatory powers should be exercised in *as targeted a way as possible*.

Although the hacking power was described in detail in the legal framework to report no. 53, the changes in the ISS Act 2017 justify discussing the main points of Section 45 of the ISS Act 2017 again in this legal framework, mainly as a means to provide context and background to the investigation. The requirements and safeguards that apply to the exercise of this special investigatory power are discussed in Sections 3 and 4. Those elements are assessed in the investigation. The requirements and safeguards that apply to the further processing of copied bulk data are discussed in Sections 3 and 5. These are also assessed in the investigation.

2.2 Automated device or system

Just as was the case under the ISS Act 2002 (former), the term automated device or system in the ISS Act 2017 follows the definition in criminal law, i.e. the description in Section 80sexies of the Criminal Code. However, this provision was redefined by the Act to amend the Criminal Code and the Code of Criminal Procedure which entered into force on 1 March 2019 in connection with improving and strengthening criminal investigation and prosecuting computer crime, better known as the Computer Crime Act III.¹⁰

⁹ Based on the ISS Act 2002 (former) the AIVD could, for physical hacks, suffice with the authorization of a Director of the AIVD; a remote hack needed the authorization of the minister. In its review report no. 53, the CTIVD recommended – in anticipation of the new legislation, in which this was included in the bill – submitting all authorization requests for hacks at ministerial level. This recommendation was adopted. At the time, the MIVD had to submit initial requests for hacking to the minister but extensions were put to the deputy director of the service. In this case also, the recommendation was, in anticipation of the new legislation, to submit all extension requests to the minister. This recommendation was adopted. CTIVD review report no. 53 on the use of the hacking power by the AIVD and the MIVD, pp. 23-24, *Parliamentary Documents II* 2016/17, 29 924, no 149 (appendix), accessible on www.ctivd.nl.

¹⁰ Computer Crime Act III of 27 June 2018, Bulletin of Acts and Decrees 2018, 322. Decree implementing the Computer Crime Act, Bulletin of Acts and Decrees 2019, 67. *Parliamentary Documents II* 34 372.

The legislative history to the ISS Act 2017 explicitly states that harmonization is sought as soon as that Act becomes effective.¹¹ An 'automated device or system' in the ISS Act 2017 is therefore – in accordance with the new Section 80sexies of the Criminal Code – taken to mean “a device or group of interconnected or related devices, of which one or more automatically processes computer data based on a program.”

The term automated device or system thus gained broader meaning.¹² An essential requirement in the description of the term is the phrase 'automatically processes computer data using a program'. The explanatory memorandum to the Computer Crime Act III states that the change was prompted by technological developments resulting in more and more devices with features that were previously only reserved for computers and with autonomous functions independently processing data based on a program, without these devices being part of a network. The new definition fits in with the terminology of the Convention on Cybercrime. The definition covers 'computers, servers, modems, routers, smartphones and tablets', but may also include 'technical devices connected to a network, such as navigation systems, televisions, digital cameras with WIFI compatibility or pacemakers'.¹³ That makes it clear that Internet of Things devices also fall under the heading automated device or system.

The legislative history to the ISS Act 2017 looks at the scope of the term automated device or system, partly in the light of the developments that have taken place since the ISS Act 2002 (former) entered into force and those expected in the future. The legislative history considers that it is inherent to the broad definition used for automated device or system that the development of devices and systems that meet the definition automated device or system thereby also fall under the scope of the hacking power. That can mean that the services could hack smart devices, such as refrigerators, watches, cars, etc. that have computer functionalities – where that is necessary, proportional and subsidiary – because according to the government it cannot be ruled out that these smart devices will, at some point, process information that could be necessary for the services to properly perform their tasks. From the viewpoint of establishing a future-proof regulation, the government feels it is not appropriate to formulate restrictions in this respect.¹⁴ Certain medical devices inserted in the body, such as pacemakers, may fall also under this definition. However in terms of physical integrity, the government considers that it 'cannot conceive of any situation, now or in the near future, in which the services would seek to use this investigatory power in a way that would affect the physical integrity of people, in the context of collecting data.'¹⁵ The ministers explicitly rule out this use.

Conclusion:

The term 'automated device or system' has a broader meaning than that in the ISS Act 2002 (former): “a device or group of interconnected or related devices, of which one or more automatically processes computer data using a program.” That can include smart devices that have computer functionalities (Internet of Things). Hacking them must be possible, under circumstances.

¹¹ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p.76 (Explanatory memorandum to ISS Act 2017) and no. 18, p. 69 (note on the report on the ISS Act 2017).

¹² *Parliamentary Documents II* 2015/16, 34 372, no. 3, p. 85 (Explanatory Memorandum to Computer Crime Act III).

¹³ *Parliamentary Documents II* 2015/16, 34 372, no. 3, pp. 85-86.

¹⁴ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 76 (Explanatory Memorandum to ISS Act 2017).

¹⁵ *Parliamentary Documents II* 2016/17, 34 588, no. 18, pp. 64-65 (note on the report on the ISS bill 2017).

2.3 Exploration

The hacking power in Section 45 of the ISS Act 2017 now explicitly includes the investigatory power to explore the technical characteristics of an automated device or system, linked to a communication network (Section 45(1)(a) of the ISS Act 2017). That might be necessary to achieve an overview of the digital environment of the subject of the investigation and to explore the operational automated device or system for any vulnerabilities.¹⁶ This investigatory power is supportive in nature compared with the investigatory power to enter an automated device or system (Section 45(1)(b) of the ISS Act 2017).

‘To explore’ means the use by the AIVD and MIVD of technical applications such as IP and portal scanning software and means of registration with which to obtain a picture of the characteristics of the automated devices connected to communication networks.¹⁷ It may also acquire a ‘semi-continuous character’ when the digital infrastructure needs to be identified, for example in the context of a military operation. When exploration is aimed at examining the feasibility of entering an automated device or system, it is short-term in nature.¹⁸

Although ‘exploration’ in Section 24 of the ISS Act 2002 (former) was not explicitly included, it did prove to be the services’ common practice (conducting preliminary investigations). The CTIVD described this in previous investigations.¹⁹ By laying down this investigatory power in Section 45 of the ISS Act 2017, the legislator has also expressed an opinion on the demarcation of the preliminary investigation. Legislative history indicates that an automated device or system is not yet entered at that stage. The CTIVD concurs. In its review report no. 53 on the hacking power in the ISS Act 2002 (former), the CTIVD at that time used a broader definition of preliminary investigation, based on its review report no. 38, i.e. until the moment that the content of the data is accessed.

Conclusion:

- *Exploring or conducting a preliminary investigation was already common practice but has now been enshrined in the law. The investigatory power to explore supports the investigatory power to enter but exploration does not entail entering the automated device or system.*
- *During exploration, technical applications are used to attempt to gain a picture of the characteristics of automated devices or systems connected to communication networks. This may be short-term in nature if exploration is aimed at examining the feasibility of entering an automated device or system. Alternatively it may also acquire a semi-continuous character when the digital infrastructure needs to be identified.*

2.4 Entry

Entry into an automated device or system is regulated by Section 45(1)(b) of the ISS Act 2017 as a separate investigatory power. This investigatory power had already been laid down in the ISS Act 2002 (former). It concerns the investigatory power to enter an automated device or system whether or not by using a technical intervention, false signals, false keys, false identity or through the automated device or system of a third party.

¹⁶ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 75.

¹⁷ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 77.

¹⁸ *Ibid.*

¹⁹ See Appendix II (legal framework) to CTIVD review report no. 53, Section 4.1.

Exploiting known or unknown vulnerabilities can be part of the exercised investigatory power to enter.²⁰

As under the ISS Act 2002 (former), the definition of entry is that the AIVD or the MIVD obtains access to an automated device or system against the undisputable will and/or without authorization of the entitled party. That will may be expressed in both words or deeds. An example of the first is the notification that unauthorized access is prohibited. An example of the second is the case where an automated device or system is secured against such entry.²¹ In other words, obtaining access to a screened off or not publicly accessible part of the automated device or system.²²

Investigatory power to include technical characteristics

Section 45(8) of the ISS Act 2017 stipulates that a ministerial authorization to enter an automated device or system of a target or third party also gives the power – for the duration of the authorization granted – to enter another automated device or system of this person or organization if this is done instead of or in addition to the automated device or system for which the authorization was originally granted.

This investigatory power to include technical characteristics is explained in more detail in the legislative history of the ISS Act 2017. Two situations are distinguished:

1. A target or third party may start to use *another* automated device or system (belonging to him) *instead of* the original automated device or system for which authorization to enter has been given. In that case, fresh authorization is not required to enter that new automated device or system. The following example is given: 'if a target uses a smartphone and, during the period for which authorization has been granted, starts to use another smartphone, entering that new smartphone is then also permitted.'²³ A third party may be 'a provider who, because of a defect [or expansion, but that is situation 2], starts to use a new automated device or system. In those exceptional cases that entering a target's automated device or system takes place through the automated device or system of an individual citizen, the same situation can be imagined: a defective automated device or system is replaced.'²⁴
2. *As well as* the automated device or system for which authorization has been granted, a target or third party may *in addition* start to use another automated device or system (belonging to him).²⁵ In that case, fresh authorization is not required to enter that new automated device or system. Two scenarios are sketched: The target or third party will at some point make '*additional* use of another smartphone, tablet, laptop or digital device, as well as the automated device or system for which the authorization was granted.' The target or third party may already be using an additional digital device but this characteristic is only discovered through the device already falling under the authorization.'²⁶

Targeted use

The legislative history to the ISS Act 2017 explains that the power to enter an automated device or system is targeted in nature. The use of the special investigatory power will generally be aimed at an automated device or system being used by a subject of the investigation (target) of the AIVD or the

²⁰ *Parliamentary Documents I* 2016/17, 34 588, C, p.12 and E, p. 4.

²¹ Appendix II (legal framework) to CTIVD review report no. 53, Section 3.2.

²² Cf. Section 138ab of the Criminal Code (computer intrusion); under criminal law, entry is when the automated device or system is accessed by breaking through security using a technical intervention, by false signals or a false key or by assuming a false identity.

²³ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 81 and repeated in *Parliamentary Documents I* 2016/17, 34 588, C, p. 16.

²⁴ *Parliamentary Documents II* 2016/17, 34 588, no. 3, pp. 81-82.

²⁵ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 81 and repeated in *Parliamentary Documents I* 2016/17, 34 588, C, p. 16.

²⁶ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 81.

MIVD.²⁷ The law provides for the possibility of investigating both people and organizations.²⁸ When hacking, the services use various technical capabilities, whereby the services can take advantage of known vulnerabilities in the security used by the subject of the investigation.²⁹

If it proves impossible to enter the target's automated device or system directly, there are two possibilities – under certain circumstances – to do so, by entering the device or system of the target using an automated device or system of a third party (technical stepping stone) or by entering the device or system of a non-target and collecting data on the target in that way.

Entry through the device or system of a third party

A new element in the ISS Act 2017 of the investigatory power to enter is the explicit addition of 'through the automated device or system of a third party' (Section 45(1)(b)). This was already existing practice under the former ISS Act 2002.³⁰ Legal grounds were provided for this practice to remove doubts about its permissibility and to subject this investigatory power to certain requirements and safeguards.³¹

Legislative history shows that the services should first try to enter the target's automated device or system directly and only when that proves impossible may alternatives be devised including entry through the automated device or system of a third party.³² The TIB, tasked with assessing the lawfulness of the authorization granted by the minister for the use of the hacking power, does not always consider that realistic in practice. The TIB is of the opinion that 'if it has been sufficiently substantiated that in specific cases the direct hack of a target is not possible because of compelling operational reasons, it can be lawful, under circumstances, to conduct a hack through a third party without first attempting a direct hack.'³³ If the same data can also be obtained in another way, entry of the automated device or system through that of a third party must be abandoned.³⁴

Technically linkable party

A 'third party' in this context is a party who can be related technically to the target. This includes a party who connects a network, provides a service, supplies software or technological knowledge. In most cases that third party will not be an individual citizen, but for example, a provider, intermediate supplier or service provider.³⁵

In 'exceptional circumstances' it may refer to an individual citizen. This may 'only be the case when alternative, less intrusive methods of entry are unsuccessful or have proved impossible'.³⁶ This must be substantiated in the request for authorization.

²⁷ *Parliamentary Documents II* 2016/17, 34 588, no. 3, pp. 78-79 and no. 18, p. 67.

²⁸ The term 'organization' is taken to mean 'a permanent cooperative partnership with a joint objective and the awareness of that joint objective by the members of the organization', see CTIVD review report no. 53, Appendix II (legal framework), Section 4.2.1.

²⁹ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 78.

³⁰ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 78 and *Parliamentary Documents I* 2016/17, 34 588, C, p. 15.

³¹ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 79 and *Parliamentary Documents I* 2016/17, 34 588, C, p. 15.

³² *Parliamentary Documents II* 2016/17, 34 588, no. 3, pp. 78-79 and no. 18, p. 67.

³³ TIB 2018/2019 annual report, p. 11, www.tib-ivd.nl.

³⁴ *Parliamentary Documents II* 2016/17, 34 588, no. 3, pp. 79 and no. 18, p. 65.

³⁵ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 78; *Parliamentary Documents II* 2016/17, 34 588, no. 18, p. 67 and *Parliamentary Documents I* 2016/17, 34 588, C, pp. 11-12.

³⁶ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 78 and no. 18, p. 70, and *Parliamentary Documents I* 2016/17, 34 588, C, p. 11.

The exact number of technical intermediaries and links which can still be defined as a direct technical relation depends on the circumstances of the case, and is for the minister and TIB to assess.³⁷

Copying data from a third party

The explanatory memorandum to the ISS Act 2017 states that where it concerns a third party, any use of the hacking power must entail the smallest possible infringement of that third party's privacy. A consideration is that 'no data may be collected other than that which is strictly necessary to enter the automated device or system of the target',³⁸ for example, passwords.

Entry of the device or system of a non-target

It is standard practice that under certain circumstances, the AIVD and the MIVD use special investigatory powers, such as the hacking power, against parties that are known as non-targets.³⁹ This is not included in the law or legislative history. The aim of the use is to increase the information position of the service in relation to the target.⁴⁰

Non-targets are not the subject of investigation by the services but have some sort of personal or business relationship with a target. If it proves impossible to enter a target's system or device, for instance because they are very security conscious, attempts can be made to obtain information about the target through the communication or actions of a non-target. A non-target can also be an organization or service provider.⁴¹

In previous reports relating to the former ISS Act 2002, the CTIVD underlined that the use of investigatory powers against a non-target is a serious measure that must be used sparingly.⁴² The CTIVD worded three conditions as follows:

1. The request for authorization must state that the hack concerns a non-target, so that this is clear to those assessing the request.
2. If the use of the investigatory power is to be proportionate, the services will have to demonstrate that the operational interest leading to the infringement of the non-target's privacy is so great that it justifies that infringement. The non-target's privacy is given greater weight because, as stated, the non-target has not given rise to an investigation by the services. In order to outweigh this, the interest that the services have to use this special investigatory power against a non-target must be correspondingly greater than usual. Examples of such compelling operational interests are situations in which there are one or more specific indications of a direct threat to national security.
3. The request for authorization states that data that does not or cannot provide any information on the target may not be processed further and must be removed and destroyed.

These conditions are not enshrined in the ISS Act 2017 or legislative history. With the introduction of the ISS Act 2017, the lawfulness assessment of the minister's authorization for the use of the hacking power has been placed with the newly founded TIB, that issues a binding decision (Section 32 in conjunction with Section 36 of the ISS Act 2017, see Section 4). The introduction of an independent lawfulness assessment prior to a special investigatory power being exercised is an important safeguard for the legal protection of citizens.

³⁷ *Parliamentary Documents II* 2016/17, 34 588, no. 18, pp. 65 and 68 and *Parliamentary Documents I* 2016/17, 34 588, C, p. 11.

³⁸ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 79.

³⁹ CTIVD review report no. 53, Section 4.2.3 (non-targets), Section 4.2.4 (third parties).

⁴⁰ See also review report no. 10, Section 5, review report no. 19, Section 6.2.2, review report no. 47, Sections 7 and 8.

⁴¹ TIB 2018/2019 annual report, p. 13, www.tib-ivd.nl. The TIB remarks in this respect that in the case of service providers considered non-targets, information can be obtained on a large scale, 'including information that for the majority relates to people who are not the focus of the service.'

⁴² CTIVD review report no. 53, Section 4.2.3 (non-targets); see also CTIVD review report no. 19 on the application by the AIVD of Section 25 of the former ISS Act 2002 (communication interception) and Section 27 of the former ISS Act 2002 (selection of random wireless telecommunication), *Parliamentary Documents II* 2008/09, 29 924, no. 29 (appendix), p. 28.

Conclusion:

- *Entry means that the AIVD and the MIVD gain full or partial access, against the indisputable will and/or without authorization by the entitled party, to an automated device or system that is screened off or inaccessible to citizens. This may be done using a technical intervention, false signals, false keys, false identity or through the automated device or system of a third party.*
- *The investigatory power to enter is targeted. Its use should be aimed at an automated device or system being used by a subject of the investigation (target) of the AIVD or the MIVD. That can be both people or organizations. If the device or system of a subject of the investigation cannot be entered directly, there is an option, under circumstances, to enter the device or system of a non-target in order to collect data concerning the target or to enter the device or system of the target through the automated device or system of a third party.*

2.5 Inherent investigatory powers after entry

Section 45(2) of the ISS Act 2017 regulates four investigatory powers that fall under the investigatory power to enter. It states that the investigatory power to enter an automated device or system also includes the investigatory power to (under a) break through security, (under b) install technical provisions to undo any encrypted data stored or processed in the automated device or system, (under c) install technical resources in connection with the use of the investigatory power as referred to in Section 40(1) and Section 47(1) as well as (under d) copy data stored or processed in the automated device or system. The request for authorization must contain substantiation for this (Section 45(4) of the ISS Act 2017).

The investigatory powers referred to under a, b and d were already included in Section 24 of the former ISS Act 2002. The legislative history of the ISS Act 2017 does not address the existing legal investigatory powers. These were explained in the legal framework to review report no. 53 and briefly put, these investigatory powers come down to the following:

"The investigatory power to break through security must be understood as entering an automated device or system via a path that the existing security does not secure or secure sufficiently, and where it is irrelevant if that opening is inherent in the system or caused by the intruder.⁴³ Encryption includes all conceivable methods to make data inaccessible to a third party. In all events this includes encryption, scrambling or steganography. Consequently, undoing that means that the data is again made accessible to third parties.⁴⁴ Copying data from the entered automated device or system means copying the data found there. To constitute copying, the data must be recorded permanently. This may be done by printing or storing the data on a data carrier. Only calling up the data onto the person's own screen does not constitute copying."^{45 46}

⁴³ ECLI:NL:HR:2011:BN9287, paragraph 2.4.

⁴⁴ *Parliamentary Documents II* 1998/99, 26 671, no. 3, p. 28

⁴⁵ *Parliamentary Documents II* 1998/99, 26 671, no. 3, p. 28.

⁴⁶ CTIVD review report no. 53, Section 3.3 (cracking security), Section 3.4 (copying information), Section 3.5 (undoing encryption).

The Act does not regulate which data may be copied after entry. Thus legislation leaves scope to obtain by ‘untargeted’ means large amounts of data using the hacking power. In other words, at the time of collection it is not yet possible to specify to whom or what the data relates. The CTIVD already described that fact in its report no. 53.⁴⁷

During the legislative procedure of the ISS Act 2017 and afterwards in the context of the investigatory power to break through security (Section 45(2)(a) of the ISS Act 2017), there was debate on using vulnerabilities that are unknown in general and to the manufacturer – referred to as zero day or unknown vulnerabilities – and in particular about whether or not to report them.⁴⁸ This topic was discussed in the context of report no. 53, in which the CTIVD recommended that the services develop policy and procedures on responsible disclosure of unknown vulnerabilities (zero days). As part of the follow-up to that report, the CTIVD will inform the House of Representatives separately on this issue.

A new element is the inherent investigatory power defined under c to install, after entering an automated device or system of a subject of investigation, certain technical provisions that support the exercise of the special investigatory powers to observe the target and intercept their communication, in brief, switching on the camera or microphone of the automated device or system.⁴⁹ This possibility is explicitly ruled out where it concerns entering an automated device or system belonging to a third party, because it is not considered necessary in that circumstance⁵⁰ as the third party’s device is only a technical resource used to enter the device of a target.⁵¹

The explanatory memorandum to the ISS Act 2017 clarifies, where this investigatory power is concerned, that automated devices or systems, such as laptops and desktop computers, are nowadays almost always fitted out with cameras and microphones. By installing technical provisions, such as certain software, these can be activated remotely and used as a technical aid, for example to the investigatory power to observe (Section 40(1) of the ISS Act 2017) or to record a conversation in a certain room (Section 47(1) of the ISS Act 2017).⁵² To do so requires the authorization prescribed based on those Sections; observations inside a house and intercepting communication requires authorization by the minister and assessment by the TIB. Furthermore, authorization is required to exercise the investigatory power to enter, included in Section 45(1)(b). If necessary, a combined request for authorization may be made.⁵³

⁴⁷ CTIVD review report no. 53, Appendix I (legal framework), Section 5.1; see also CTIVD review report no. 55, Appendix I (legal framework), Section 2.4.

⁴⁸ The parliamentary debate on this topic dates from before the legislative procedure of the ISS Act 2017; a brief description of this can be found in review report no. 53, Appendix II (legal framework), Section 3.3. For the most recent state of affairs, see: *Parliamentary Documents II* 2016/17, 26 643, no. 428; *Parliamentary Documents I* 2016/17, 34 588, C, p. 12; *Parliamentary Documents I* 2016/17, 34 588, E, p. 4; AIVD and MIVD policy on handling ‘unknown vulnerabilities’ 2018 (via www.aivd.nl); private member’s Bill Zero Days assessment process of 19 July 2019 and the advisory opinion from the Council of State of 13 December 2019, file 35 257.

⁴⁹ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 81.

⁵⁰ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 81.

⁵¹ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 78.

⁵² *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 79.

⁵³ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 80.

Investigatory power to decrypt and duty to assist

In addition to the investigatory power under b (installing technical resources to decrypt data stored or processed in the automated device or system), Section 45 of the ISS Act 2017 also contains the investigatory power of the services to instruct a party to assist with decrypting stored data. The law lays down a duty to assist for that party. This is regulated by Section 45(9)-(12) of the ISS Act 2017. This investigatory power and the duty to assist already existed under the ISS Act 2002. What is new is that the minister must authorize its use (subsection 10). Subsection 11 contains several additional requirements for the request for authorization.

Conclusion:

- *The investigatory power to copy data from the entered automated device or system means copying the data found there. To constitute copying, the data must be recorded permanently. This may be done by printing or storing the data on a data carrier. Only calling up the data onto the person's own screen does not constitute copying."*
- *The Act does not regulate which data may be copied after entry. Thus legislation leaves scope to obtain, by 'untargeted' means, large amounts of data using the hacking power. That means that at the time of collection, it is not yet possible to specify to whom or what the data relates.*

3. General framework for data processing

3.1 General requirements for data processing

The ISS Act 2017 defines ‘data processing’ or the ‘processing of data’ as: “every act or set of actions relating to data including in any case collecting, recording, arranging, storing, updating, altering, retrieving, consulting or using data, disseminating data by means of forwarding, distributing data or any other form of making available of data, and the assembling, interrelating, protecting, deleting or destroying of data”.⁵⁴

When the services process data within the context of the performance of their duties, the general requirements for data processing of Section 18 of the ISS Act 2017 apply. These requirements include that data should only be processed for a certain purpose and only in as far as necessary for the AIVD and the MIVD to properly perform their tasks (purpose limitation and necessity requirement).

That means that the services must have an objective that is detailed in advance and is in line with the services’ legal tasks. The purpose of the data processing must also be set out in the substantiation for a request to use an investigatory power.⁵⁵ The services should be confident that this purpose can be achieved by processing the data and they must be able to substantiate that.⁵⁶

Section 19 of the ISS Act 2017 sets out an exhaustive list of the categories of persons whose personal data may be processed. This corresponds with the services’ tasks. For example, it concerns those people suspected of being a threat to the national security or people who granted authorization for a security screening. For the purposes of this current investigation, it is important that the hacking power – as a special investigatory power with which data may be collected – may only be used for a number of the specific tasks that the services have, i.e. the intelligence and security tasks (Section 28 of the ISS Act 2017⁵⁷) and not for other tasks such as conducting security screenings or the security enhancing task. Relevant also is subsection 5 of Section 19 of the ISS Act 2002. This is discussed in more detail in Section 3.3.

Section 18 of the ISS Act 2017 further stipulates that data should be processed properly and carefully.⁵⁸ The propriety criterion is linked to the performance of the proportionality requirement.⁵⁹ Compliance with the propriety requirement means that the restriction of fundamental rights that occurs when data is processed must be proportionate to the intended objective.⁶⁰ In this respect it is important how much personal data is collected, its use and the weight of operational interests.

⁵⁴ Section 1(f) of the ISS Act 2017.

⁵⁵ Section 29(2)(e) of the ISS Act 2017.

⁵⁶ See report no. 56 (2018) on the multilateral exchange of data on (alleged) jihadists by the AIVD, Appendix II, p.2.

⁵⁷ For the AIVD these are the A and D tasks (Section 8(2) of the ISS Act 2017); for the MIVD the A, C and E tasks (Section 10(2) of the ISS Act 2017).

⁵⁸ See Section 18(2) of the ISS Act 2017. In its report no. 56 (2018) the CTIVD specifies in greater detail what the safeguards of necessity, propriety and due care entail in the provision of data to foreign partners. See also report 65 (2019).

⁵⁹ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 32.

⁶⁰ See also report no. 56 (2018), p. 11.

Careful data processing also relates to the accuracy and current relevance of the data that is processed.⁶¹ The data that is to be processed must contain an indication of the level of reliability of the data or a reference to the document or source from which the data derives.⁶² The indication of reliability can also be helpful in assessing data derived from, for example, a data analysis or data aggregation.⁶³ These requirements must be taken into account when disclosing data on the services' digital infrastructure. The reliability assessment must be recorded.

The general requirements for data processing serve as a starting point for collecting bulk data sets using the hacking power and further processing those sets. In order to exercise the hacking power, a number of additional specific requirements apply – in contrast to the use of the general investigatory powers to collect data – because it concerns a special investigatory power. These are discussed in Section 4.

Conclusion:

Data processing is broadly defined: it comprises all actions that may be taken with data. Data processing must in general comply with the requirements of purpose limitation, necessity, propriety and due care. These requirements also apply as a starting point for collecting bulk data sets with the hacking power and their further processing.

3.2 Duty of care

The duty of care that the AIVD and the MIVD have to ensure data is processed lawfully is part of the general framework of data processing. Based on Section 24 of the ISS Act 2017, the heads of the AIVD and the MIVD have a duty to ensure that the technical, staffing and organizational measures relating to data processing comply with the provisions under or pursuant to the law. Part of this is promoting the quality of data processing, including the algorithms and models used. This aspect of the duty of care is a new element compared with the former ISS Act 2002, which already included the duty of care.

The duty of care explicitly requires more from the AIVD and the MIVD than simply implementing the legal requirements imposed on them for collecting, analyzing and actual use of the data by service staff.⁶⁴ The duty of care means that both services continuously monitor how they process data and ensure that this data processing is and remains in accordance with the applicable legal requirements (*compliance*). Policy, process descriptions and work instructions may have a contributory role, with a view to assigning positions and responsibilities.

Continuously being in control requires the services to use a number of instruments that provide (central) overview of the functioning of processes and systems of data processing and that enable them to identify risks and take measures promptly. The entire processing procedure must be set up in such a way that internal control and effective external review are possible (Section 24 of the ISS Act 2017).

⁶¹ Section 24(2)(a) of the ISS Act 2017. See also CTIVD report no. 56 (2018). The data must not be superseded by more other, more recent data.

⁶² Section 18(3) of the ISS Act 2017.

⁶³ See also CTIVD report no. 57 (2018).

⁶⁴ See also CTIVD report no. 59 (2018), p.7.

Conclusion:

The AIVD and the MIVD have a duty of care for the lawfulness and quality of the data they process. This means that they are continuously in control of their data processing and that they are able to identify risks and take measures in time. The duty of care means that the services have policy, process descriptions and work instructions that are an interpretation of the legal requirements in practice. The entire processing procedure must be set up in such a way that internal control and effective external review are possible.

3.3 Bulk data sets

The term bulk data sets refers to large collections of data, the vast majority of which concern organizations or people who are not the subject of investigation by the services, nor ever will be. That means that these data sets contain a lot of data concerning people or organizations who are not under investigation by the services.⁶⁵ Given the nature and volume of data to be acquired, an estimate can often be made in advance that the majority of the bulk data will contain information that is not related to any targets of the services and therefore is irrelevant to the services' performance of tasks.⁶⁶ These types of bulk data sets have immense operational value for the services, particularly from the perspective of identifying 'unknown threats'. For example, the data may help to identify new targets and establish connections between people and/or organizations. In that way a bulk data set can be distinguished from a large amount of data that can be related in its entirety to a target of the service, for example data from the target's computer, but which can still contain mainly non-relevant data.

The fact that the ISS Act 2017 allows scope to collect bulk data sets is not a matter of debate. This appears from Section 19 of the ISS Act 2017 which sets out an exhaustive list of the categories of people whose personal data may be processed by the services. A newly inserted subsection 5 stipulates that the services may also, in addition to the categories of persons stated above, process data on other people if that data is a logical and inextricable part of the data files which the services have acquired or will acquire. The consideration when inserting this subsection was that when collecting data files, data is also collected from people who are not the focus of the services, from the perspective of their tasks. Under the ISS Act 2002 (former) the legal basis for this was sought in 'persons whose data is necessary to support the proper performance of tasks' (Section 13(1)(e) of the ISS Act 2002 (former), currently Section 19(1)(e) of the ISS Act 2017) As far as doubts could arise about the permissibility of processing this type of personal data, and therefore for the sake of legal certainty, the decision was made to regulate this separately. The Explanatory memorandum refers to the Privacy Impact Assessment (PIA) of the bill for the ISS Act 20xx. The PIA concluded, particularly with regard to the investigatory powers by which large amounts of data (bulk) are collected, that this is problematic given the risks to the privacy of people whose data is collected unfoundedly and given the ECHR requirement that the category of people who may be subjected to covert data collection must be defined. However, according to the PIA it is difficult to describe the category of people in any more detail than was done in subsection 5. The PIA did note that compensating measures were necessary, for example the obligation to remove non-relevant data as soon as possible.⁶⁷

⁶⁵ CTIVD review report no. 55 (February 2018) on the acquisition by the AIVD and the MIVD of bulk data sets offered on the internet by third parties, Parliamentary Documents II 2016/17, 29 924, no. 155 (appendix) accessible on www.ctivd.nl; VGR III, no. 66 (published 3 December 2019), p. 8, *Parliamentary Documents II* 2019/00, 34 588, no. 85 (appendix).

⁶⁶ Review report 39 on the lawfulness of the investigation on social media by the AIVD (2014) p. 13, *Parliamentary Documents II* 2013/14, 29 924, no. 114 (appendix), accessible on www.ctivd.nl.

⁶⁷ *Parliamentary Documents II* 2016/17, 34 588, no. 3, (Explanatory Memorandum to ISS Act 2017) p. 34.

Collecting and further processing bulk data sets constitutes a serious infringement of fundamental rights which must be offset by adequate safeguards. This is also something that the CTIVD infers from case law by the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU).⁶⁸ Storing personal data such as this in large quantities to combat terrorism, for example, is only permitted under certain circumstances, such as an advance assessment of necessity and proportionality, with detailed rules on aspects such as the duration of storage, the use of data by authorized staff, measures to safeguard the integrity and reliability of the data and procedures for the destruction of data.⁶⁹ A caveat is appropriate here, that case law as such makes no distinction between the processing of data in general and the processing of data to protect the national security of states. That case law is still being developed. The Grand Chamber of the ECHR will be ruling in last instance on two cases in which the subject is bulk data.⁷⁰ However it does serve as an incentive to implement possible safeguards which the AIVD and the MIVD should take into account when processing data from bulk data sets.

The ISS Act 2017 does not – contrary to bulk from investigation-related interception – contain any specific safeguard regime for collecting and further processing bulk data sets. As far as the current investigation is concerned, specific legal requirements apply to the collection of a bulk data set using the hacking power because it concerns a special investigatory power. These requirements are discussed in Section 4. When further processing bulk data sets, the starting point, given the lack of any more specific legal regulations, is that the data should be processed properly and carefully in accordance with the general requirements of Section 18 of the ISS Act 2017 and the duty of care in Section 24 of the ISS Act 2017. The services have implemented this by formulating certain safeguards for accessing and using bulk data sets.⁷¹ These are discussed in more detail in Section 5. This section also looks at the legal retention period in Section 27 of the ISS Act 2017 for data obtained using special investigatory powers. Under this provision, data must be assessed for relevance as soon as possible, but in any event within one year. After that term the data that has not been assessed must be destroyed immediately. This is an important safeguard for the protection of the fundamental rights of people whose data is being processed. However, this safeguard is at odds with the character (size and operational importance) of bulk data sets.

⁶⁸ See also the Assessment framework to report no. 55 (2018) on bulk data sets offered on the internet by third parties.

⁶⁹ In particular see ECHR 4 December 2008, no. 30562/04 and 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. and Marper vs. United Kingdom*), ECHR 30 January 2020, no. 50001/12, ECLI:CE:ECHR:2020:0130JUD005000112 (*Breyer vs. Germany*) and HvJEU 21 December 2016, C-203/15 and C-698, ECLI:EU:C:2016:970 (*Tele2 Sverige AB vs. Post- och telestyrelsen and Secretary of State for the Home Department vs. Tom Watson et.al.*).

⁷⁰ 19 June 2018, no. 35242/08, ECLI:CE:ECHR:2018:0619JUD003525208 (*Centrum för Rättvisa vs. Sweden*) and ECHR 13 September 2018, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch et.al. vs. United Kingdom*) (both currently before the Grand Chamber).

⁷¹ ECHR See the notice 'Working with large data sets' on aivd.nl and the 'AIVD and MIVD policy on the acquisition and processing of bulk data sets' of 1 May 2018, also accessible on aivd.nl. The authorization requests for the use of the hacking power show that there are specific safeguards relating to an inner box/outer box procedure.

Conclusion:

- *Bulk data sets are large collections of data, the vast majority of which concern organizations and/or people who are not the subject of investigation by the services, nor ever will be.*
- *Bulk data sets have immense operational value for the services.*
- *Collecting and further processing a bulk data set means a severe infringement of the fundamental rights of those not the subject of investigation. That must be compensated with sufficient safeguards. Aside from investigation-related interception, the law does not make provisions for this. The services themselves apply certain additional safeguards in the context of proper and careful data processing.*

4. Requirements for exercising the hacking power

In addition to the general framework for data processing, the ISS Act 2017 sets a number of specific requirements to exercising the hacking power because of the fact that this is a special investigatory power. Some of those requirements concern the hacking power specifically and are included in Section 45 of the ISS Act 2017, whereas others apply to all special investigatory powers. The requirements are discussed below.

4.1 Authorization and assessment

Minister

A new element in the ISS Act 2017 is that the relevant minister must grant authorization to use the hacking power. This is the Minister of the Interior and Kingdom Relations where it concerns the AIVD and the Minister of Defence where it concerns the MIVD. The law does not contain provisions for extending the mandate. The ministerial authorization requirement applies to exploring and entering automated devices or systems (Section 45(3) of the ISS Act 2017), entering the automated device or system of a third party (Section 45(5) of the ISS Act 2017) and the duty to decrypt (Section 45(10) of the ISS Act 2017). Thus authorization has been assigned to a higher level than under the former ISS Act 2002. But under the former ISS Act 2002, it was already the services' practice to request authorization from the relevant minister, partly in response to the recommendation made in report no. 53 (April 2017).⁷² Authorization is granted for a period of no more than three months (Section 29(1) of the ISS Act 2017).

TIB

A further new element in the ISS Act 2017 is the requirement of a lawfulness assessment by the TIB of the authorization given by the minister for the use of the hacking power. The TIB's assessment includes whether the authorization complies with the requirements of necessity, proportionality, subsidiarity, and being as targeted as possible (these requirements are explained in more detail in Section 4.2). The TIB also looks at the technical risks of the use of the hacking power (see Section 4.3) and a description of the result when requesting an extension. The TIB issues a binding decision. The investigatory power may only be exercised following a positive assessment by the TIB. The independent review by the TIB is an important new safeguard (Section 32 in conjunction with Section 36 of the ISS Act 2017).

The ISS Act 2017 does not contain provisions for transitory law. That means that the provisions of the new law applied immediately after the Act entered into force on 1 May 2018. The Minister of the Interior and Kingdom Relations said the following in the letter dated 25 April 2018: "Requests to use special investigatory powers, for which the ISS Act 2017 prescribes authorization by the Investigatory powers Commission (TIB) or by the Court of The Hague, will be submitted to the TIB or the court as soon as possible after the Act enters into force. The most sensitive warrants will be submitted first. After the ISS Act 2017 enters into force, the term required by that Act will apply. For that matter, the requests authorized under the ISS Act 2002 may run for a maximum of three months."⁷³

CTIVD

Although the CTIVD is not involved in the process of granting authorization, it does review the lawfulness of the hacking power exercised. The CTIVD's review is not restricted to this investigatory power, its lawfulness review covers all of the services' conduct.

⁷² CTIVD review report no. 53, Section 5; the recommendation was adopted by the relevant ministers, see the ministers' policy response, 25 April 2017, *Parliamentary Documents II* 2016/17, 29 924, no. 149.

⁷³ Letter from the Minister of the Interior and Kingdom Relations to the president of the House of Representatives of the States General regarding undertakings and motions ISS Act 2017 1 May 2018, 25 April 2018.

4.2 Requirements for the use of general and special investigatory powers

The use of either a general or special investigatory power by the AIVD and the MIVD to collect data must be reviewed against the general requirements that apply to the collection of data under Section 26 of the ISS Act 2017. These general requirements are proportionality (the means is proportionate to the infringement) and subsidiarity (selecting the least invasive means).⁷⁴

As a rule, a special investigatory power may only be used in so far as this is necessary for the proper performance of the AIVD's task, as referred to in Section 8(2)(a) and (d) of the ISS Act 2017, and the MIVD's tasks, as referred to in Section 10(2)(a), (c) and (e) of the ISS Act 2017 (Section 28(1) of the ISS Act 2017).

Based on Section 29(2) of the ISS Act 2017, the authorization request for the use of a special investigatory power must include a description of the intended objective (under e) and the reason why that use is considered necessary (under f). It is generally accepted that the requirement of necessity in this section also includes an assessment regarding the requirements of proportionality and subsidiarity, as described in Section 26 of the ISS Act 2017. The Bill amending the ISS Act 2017 which is pending in the House of Representatives since July 2019 proposes to explicitly include these two requirements in Section 29(2) of the ISS Act 2017.⁷⁵ Based on the adopted Motion Recourt,⁷⁶ which was established in a policy rule to the ISS Act 2017,⁷⁷ the authorization must also be substantiated in terms of how the requirement of 'as targeted use of the special investigatory power as possible' will be implemented. The aforementioned bill amending the ISS Act 2017 includes a proposal to set out this requirement explicitly in Section 29(2) as well as – applicable to all investigatory powers to collect data – in Section 26(new subsection 5) of the ISS Act 2017.⁷⁸

The requirements of necessity, proportionality, subsidiarity and being as targeted as possible can be seen as the four locks on the door to using the hacking power. Failure to comply with one or more of these requirements means that the exercise of the hacking power is unlawful. It is up to first the minister and then the TIB to assess compliance.

Necessity

The necessity requirement means that the use of a general or special investigatory power to collect data serves a certain objective and intends to contribute to achieving that objective. Once the objective has been achieved, the use of the investigatory power must be stopped immediately.

That requirement is included in Section 18 of the ISS Act 2017, which contains the general requirements for processing data (see Section 3.1), in Section 26 (1) and (4) of the ISS Act 2017, in Section 28(1) of the ISS Act 2017 which states that special investigatory powers may only be used if necessary for the services' security and intelligence tasks and finally Section 29(2)(f) of the ISS Act 2017 which stipulates

⁷⁴ The requirement 'as targeted as possible' currently only applies to the use of investigatory powers, see Section 5 Policy Rules of the ISS Act 2017. The Bill amending the ISS Act 2017 (introduced in the House of Representatives in July 2019) proposes to have the requirement 'as targeted as possible' apply to all investigatory powers in the context of collecting data and to explicitly set this out in Section 26(5) (new) of the ISS Act 2017, *Parliamentary Documents II* 2018/19, 35 242, no. 3, p. 4.

⁷⁵ *Parliamentary Documents II* 2018/19, 35242, no. 3, p. 4 (introduced in the House of Representatives in July 2019).

⁷⁶ *Parliamentary Documents II* 2016/17, 34 588, no. 66.

⁷⁷ *Parliamentary Documents II* 2017/18, 34 588, no. 76 (appendix); Section 5 of the Policy Rule states: "The use of special investigatory powers by the services must be as targeted as possible. The request for authorization as referred to in Section 29 of the Act to use a special investigatory power must clarify expressly how the requirement to exercise the special investigatory power in the most targeted way possible will be implemented."

⁷⁸ *Parliamentary Documents II* 2018/19, 35 242, no. 3, p. 4 The requirement 'as targeted as possible' currently only applies to the use of investigatory powers, see Section 5 Policy Rules of the ISS Act 2017. The Bill amending the ISS Act 2017 proposes to have the requirement 'as targeted as possible' apply to all investigatory powers in the context of collecting data and to explicitly set this out in Section 26(5) (new) and in Section 29(2) of the ISS Act 2017.

the requirements that the authorization request must meet in order to use a special investigatory power to collect data.

Proportionality

Proportionality means that an assessment must be made of the objective that is being sought and the disadvantage to the party involved, generally the corresponding infringement of fundamental rights (Section 26(2) of the ISS Act 2017). The use of the investigatory power should be proportionate to the intended objective (Section 26(3) of the ISS Act 2017).

The party involved referred to in Section 26 of the ISS Act 2017 means the person against whom the investigatory power is used. That does not mean that the interests of third parties are not part of the assessment. The legislative history considered that these are part and parcel of the review prescribed in Section 26(3) of the ISS Act 2017 that the use of an investigatory power must be proportionate to the objective it serves.⁷⁹

The CTIVD stated in previous reports that certain situations call for an ‘increased proportionality assessment’. That is the case, for example, when the hacking power is used against a non-target or when large amounts of data (bulk) are copied in an untargeted way, which means that it is not specifically clear beforehand to what the data relates and whose data it concerns. The fact that much of the data concerns information from people or organizations who are not a target for the services counts heavily.⁸⁰ The CTIVD determined that the services must then indicate why their operational interests should outweigh the interests of the people or the organizations whose information appears in the data. Compelling operational interests may be situations in which there are one or more specific indications of a direct threat to national security.⁸¹ Under the ISS Act 2017, the TIB is the body that reviews before special investigatory powers such as the hacking power are used, if the proportionality requirement has been met. This is an important safeguard for legal protection. The TIB’s 2018/2019 annual report (published on 25 April 2019) shows that the threshold for bulk hacks is high – the operational interests have to be compelling (p. 22). The TIB refers to the above extract from the CTIVD report no. 53.

Subsidiarity

Subsidiarity means that the investigatory power is exercised that causes the least disadvantage to the party involved (Section 26(1) of the ISS Act 2017). Furthermore the use of the investigatory power must be ceased immediately once the objective has been achieved or when using a less invasive investigatory power is adequate (Section 26(4) of the ISS Act 2017).

As targeted as possible

Article 5 of the Policy Rules of the ISS Act 2017 sets out – pursuant to the adopted Motion Recourt⁸² – that the use of special investigatory powers by the AIVD and the MIVD must be as targeted as possible. A further stipulation is that the request for authorization as referred to in Section 29 of the ISS Act 2017 must show expressly how the requirement to exercise the special investigatory power in the most targeted way possible will be implemented.⁸³ The Policy Rule or the explanatory memorandum do not give an interpretation or definition of this criterion.

⁷⁹ *Parliamentary Documents I* 2016/17, 34 588, C, p. 12.

⁸⁰ CTIVD review report no. 53, Appendix II (legal framework), Section 5.1 (copying data).

⁸¹ CTIVD review report no. 53, Appendix II (legal framework), Section 5.1 and Section 4.2; this definition is repeated in CTIVD review report no. 55, Appendix I (legal framework), Section 3; previously established in CTIVD review report no. 38, p. 39 and CTIVD no. 39, pp. 14 and 26.

⁸² *Parliamentary Documents II* 2016/17, 34 588, no. 66.

⁸³ *Parliamentary Documents II* 2017/18, 34 588, no. 76 (appendix).

The Bill amending the ISS Act 2017 proposes to lay down the requirement ‘as targeted as possible’ for the use of investigatory powers in the context of collecting data in the ISS Act 2017.⁸⁴ The government concurs with the criterion used by the TIB in its assessment in cases where ‘as targeted as possible’ plays a role, i.e. “to what extent is the data that is not strictly necessary for the investigation minimized on acquisition, given the technical and operational circumstances of the case.”⁸⁵ The government considers this a suitable criterion and specifies the term ‘as targeted as possible’ in the notes as clearly as possible:

“In their authorization request, the services must as far as reasonably possible (and where applicable) include the requirement ‘as targeted as possible’ by demarcating the data to be obtained: geographically, by time, by data/traffic type, by object/target, by conduct or otherwise. They must also take into account the intelligence context in which the as yet unknown threat is to be examined, including the stage of the investigation, the necessity to falsify, the time element and realistic technical possibilities.”⁸⁶

The government points out that in certain circumstances the above criterion leaves scope to collect data in a broader and less targeted way, owing to, for example, operational considerations such as preventing the identification of a hack of an automated device or system or of the specific data which the service is focusing on. In their request the services will have to substantiate convincingly why they cannot conduct the investigation if they reduce the amount of data collected (a part of which is therefore not required for the investigation itself in terms of content), when that additional data is not actually necessary for their investigation. Although this use involves collecting a great deal of data about people and bodies who are not the subject of any investigation by the services, it is sometimes necessary to collect the data in that form. Operational arguments, such as preventing identification, is one of them. The same elements can be taken into consideration when implementing the requirement of ‘as targeted as possible’ as those discussed above about the requirement of as targeted as possible. The request will also have to describe which measures will be taken to protect the data that is not necessary, in terms of content, for the investigation.⁸⁷

The requirement ‘as targeted as possible’ does not preclude the collection of bulk data sets on the condition that the authorization request contains a sound substantiation and lists the additional safeguards (see Section 5).

4.3 Description of technical risks

On top of the general requirements which Section 29(2) of the ISS Act 2017 lays down for the authorization and extension requests to use a special investigatory power, a request and extension to explore or enter an automated device or system, as regulated by Section 45(1) of the ISS Act 2017, must meet other specific requirements (Section 45(4) of the ISS Act 2017). That element is new in the ISS Act 2017, as the ISS Act 2002 (former) sets no specific requirements to requests.⁸⁸ The additional requirements apply equally to a request to enter the device or system of a third party (Section 45(5) of the ISS Act 2017) and consist of the following three elements:

⁸⁴ *Parliamentary Documents II* 2018/19, 35 242, no. 3, p. 3.

⁸⁵ *Ibid.*

⁸⁶ *Ibid.*, p. 5.

⁸⁷ *Ibid.*, p. 6-7.

⁸⁸ CTIVD review report no. 53, Section 4.2.

- a. a description of the technical risks associated with the use of the relevant investigatory power;
- b. which, if any, investigatory powers as referred to in (2) will be applied when exercising the investigatory power referred to in (2) under b;
- c. where it concerns the exercise of the investigatory power referred to in (1) under b, a number, a technical characteristic or other indication by which the automated device or system may be identified.

The authorization request must contain a description of the technical risks anticipated for the use of the investigatory power to explore or enter an automated device or system.

The explanatory memorandum sets out the following where it concerns the rationale behind including the requirement to describe the technical risks in the authorization request for the use of the investigatory power to explore or enter an automated device or system:

“In the internet consultation various respondents pointed out that exploiting the vulnerabilities present in the software, or installing technical aids (such as malware) to gain access to an automated device or system can create great risks for other users of the automated device or system but also for users of the same software containing the vulnerability detected by the services. If the services are able to identify those kinds of vulnerabilities, others will too; furthermore, third parties may even exploit the malware which the services themselves have installed. The use and misuse of these vulnerabilities may, depending on the systems, have a significant societal impact. This may raise questions, partly in light of government policy regarding cyber security [...]. We are aware of this tension but the interest of national security should, under certain circumstances, prevail. However in order to be able to consider the authorization request carefully, the technical risks associated with the use of the investigatory power (in so far as these can be estimated) must first be identified [...]”⁸⁹

Where the use of the investigatory power to enter an automated device or system entails exploiting a vulnerability, the authorization request must show that fact, along with the technical risks involved, so that the TIB can include these in its lawfulness assessment.⁹⁰ This requirement also applies to entering the device or system of a third party (Section 45(5) of the ISS Act 2017). Legislative history shows that if these risks mean that the use of the investigatory power against a third party should be abandoned, authorization will be denied. When entering a newly identified automated device or system of a third party (option to include, Section 45(8) of the ISS Act 2017), records will be kept in accordance with the provisions of Section 31 of the ISS Act 2017. Records will also be kept, based on Section 45(4)(a) of the ISS Act 2017, of the assessment of the technical risks associated with the use of that investigatory power in that case.⁹¹ The assessment of the technical risks is not only made to protect the interests of that third party, but also of the services themselves, who have a substantial interest in successfully entering unnoticed.⁹²

⁸⁹ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 80

⁹⁰ *Parliamentary Documents I* 2016/17, 34 588, E, p. 4.

⁹¹ *Parliamentary Documents I* 2016/17, 34 588, C, pp. 15-16.

⁹² *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 82; *Parliamentary Documents I* 2016/17, 34 588, C, pp. 15-16

How the technical risks are to be described is not regulated by law or legislative history. The law does recognize that the actual exercise of the hacking power requires specialist knowledge and must therefore only be placed in the hands of qualified staff (Section 45(6) of the ISS Act 2017). These employees are therefore primarily the ones to provide input for the description of the technical risks.⁹³

Section 45(4) of the ISS Act 2017 stipulates, among other things, that an authorization request for exploring or entering an automated device or system of a target or non-target or third party must contain a description of the technical risks associated with the use of the relevant investigatory power (under a). This is in addition to the general requirements that Section 29(2) of the ISS Act 2017 sets for the use of a special investigatory power.

Legislative history distinguishes various risks. Firstly, there are risks linked to the use of vulnerabilities in software to gain access to an automated device or system, both for users of that automated device or system on which that software operates and for other users of that software. In addition third parties could take advantage of these vulnerabilities. Secondly, these risks also exist for the services when introducing technical aids to gain access to an automated device or system. Weighing these risks is in the services' own interest in order to enter unnoticed.

The various related elements may be deduced from this description. The TIB lists these elements in its 2018/2019 annual report and distinguishes the following risks:

- "Risks to the availability and integrity of computer systems. The TIB provides examples of systems in vital infrastructures or of service providers that should be designated 'non-targets' or third parties.
- The risk that third parties will misuse the resources installed by the services, for example to also gain access to the systems with these resources on them.
- Risks associated with the use of known and unknown vulnerabilities. The TIB must include that use in its lawfulness assessment. In addition, exploiting vulnerabilities runs the risk of being identified by third parties.
- The risk that is linked to a hack being identified, for example because this could lead to reprisals."

As the TIB noted, the exploitation of vulnerabilities must be clearly stated in authorization requests, including a description of the associated technical risks.

The CTIVD points out that describing the technical risks is not a one-time exercise, but should be repeated when requesting an extension. It is conceivable that the technical risks cannot be fully foreseen on the initial request and that the picture only becomes clear or needs to be changed when the hack is being conducted. This demands an on-going assessment process of the technical risks which, if an extension request is made, must be expressed therein and the considerations in this respect recorded internally in accordance with Section 31 of the ISS Act 2017. In this context it is important to list the technical risks of keeping access to the automated device or system open.

⁹³ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 236

Conclusion:

Section 45(4) of the ISS Act 2017 stipulates, among other things, that an authorization request for exploring or entering an automated device or system of a target or non-target or third party must contain a description of the technical risks associated with the use of the relevant investigatory power (under a). This is in addition to the general requirements that Section 29(2) of the ISS Act 2017 sets for the use of a special investigatory power.

4.4 Reporting

Section 31 of the ISS Act 2017 stipulates that a record must be kept of the use of an investigatory power, also referred to as reporting. Firstly the assessments on the use of the hacking power must be set out in the authorization requests, so that the minister and then the TIB can include them in the review of the request or the granted authorization. Moreover, recording the assessments made is important for internal control purposes and for the CTIVD to be able to conduct effective review.

Legislative history considers that keeping records covers the entry of newly identified automated devices or systems, in particular those of a third party. Based on Section 45(4)(a) of the ISS Act 2017, records will also be kept of the assessment of the technical risks associated with the use of that investigatory power in the case concerned,⁹⁴ because the assessment of the technical risks is made not only to protect the interests of that third party, but also to protect the interests of the services themselves, who have a substantial interest in successfully entering unnoticed.⁹⁵

The legislator leaves open the manner of reporting. Consequently, methods other than written records are possible.⁹⁶ In its review report no. 53, the CTIVD recommended the services to start logging (i.e. the continuous automated and comprehensive recording of data) the hacking power exercised and the related technical actions taken.⁹⁷ The CTIVD's recommendations were adopted by the ministers involved.⁹⁸ The CTIVD considers its recommendations, if and insofar as adopted by the minister(s) concerned, including in communications to Parliament, as part of the legislation and regulations applicable to the AIVD and the MIVD.⁹⁹

Conclusion:

Section 31 of the ISS Act 2017 stipulates that a record must be kept of the use of an investigatory power. This includes recording the assessments made when exercising the hacking power, newly identified or substitute automated devices or systems of a target, non-target or third party, and the assessments regarding the technical risks associated with the use of that investigatory power in the case concerned. In its review report no. 53, the CTIVD recommended the services to start logging (i.e. the continuous automated and comprehensive recording of data) the hacking power exercised and the related technical actions taken. The ministers adopted this recommendation at the time.

⁹⁴ *Parliamentary Documents I* 2016/17, 34 588, C, pp. 15-16.

⁹⁵ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 82; *Parliamentary Documents I* 2016/17, 34 588, C, pp. 15-16.

⁹⁶ *Parliamentary Documents II* 2016/17, 34 588, no. 3, p. 50.

⁹⁷ CTIVD review report no. 53, Section 6 (implementation).

⁹⁸ *Parliamentary Documents II* 2016/17, 29 924, no. 149 (policy response)).

⁹⁹ CTIVD review report no. 51 on the implementation of the obligation to notify by the AIVD and the MIVD, Section 2.1.2 (p. 11), *Parliamentary Documents II* 2016/17, 29 924, no 146 (appendix), accessible on www.ctivd.nl; CTIVD review report on the provision by the AIVD and the MIVD of unevaluated data to foreign services, Appendix II (legal framework), Section 5.3.2, *Parliamentary Documents II* 2019/20, 29 924, no. 193 (appendix).

4.5 Clean-up obligation

Based on Section 45(7) of the ISS Act 2017, the principle applies that a technical aid used to enter an automated device or system, for example malicious software (malware) or a 'backdoor', must be removed if possible after the hacking power exercised has ended (referred to in this appendix and the report as 'clean-up obligation').¹⁰⁰ If an automated device was entered through that of a third-party, this obligation not only applies to that third party but also to the target. The clean-up obligation is a new element in the ISS Act 2017.

The aim is to prevent abuse of the technical aids used by the service that could lead to large-scale damage to the owner and/or users of the automated device or system.

A best-efforts obligation was selected in this case because in certain cases the removal of malware could disproportionately harm the third party or the compelling operational interests of the services. In the event that the technical aid cannot be removed, this must be recorded.¹⁰¹

Conclusion:

New to the ISS Act 2017 is a clean-up obligation for technical aids after the use of the investigatory power to enter has ended. It is a best-efforts obligation, meaning that non-compliance with this obligation could be legitimate. A report must be drafted in those cases.

¹⁰⁰ Parliamentary Documents II 2016/17, 34 588, no. 18, p. 67.

¹⁰¹ Parliamentary Documents II 2016/17, 34 588, no. 3, p. 79.

5. Safeguards for the further processing of bulk data from the hacking power

ECHR case law suggests that storing and further processing personal data constitutes an infringement of the right to privacy.¹⁰² The ECHR developed factors in its case law relating to data processing that are important when weighing the severity of the privacy infringement. Briefly put, based on this case law the following must be taken into account: (1) the context in which the data is collected, (2) the nature of the data and (3) the way in which that data is further processed and used.¹⁰³ A further processing of personal data means a more severe infringement of privacy.¹⁰⁴ If the right to privacy is infringed upon, Article 8 of the ECHR requires that this is provided for by law. In other words, privacy infringement must be grounded in national legislation.¹⁰⁵ Furthermore, the quality of the legislation must be such as to safeguard against misuse.¹⁰⁶

The requirements and safeguards that apply after bulk data has been copied using the hacking power are set out below.

5.1 Requirement for data reduction

One important safeguard for the legal protection of citizens in the ISS Act 2017 when processing data collected using special investigatory powers is the requirement of continuous data reduction, of which a key element is the obligation to assess the data for relevance as soon as possible and to destroy non-relevant data (Section 27 of the ISS Act 2017). The law provides for a retention period of 1 year (with a possible six-month extension). Data collected by investigation-related interception falls outside this regulation and is subject to a maximum retention period of three years. The requirement that the assessment for relevance must take place 'as soon as possible' does not apply in that case. Conversely, this system includes additional safeguards that do not apply to the other special investigatory powers, such as tiered authorization for the various components of the further data processing, division of job roles and tasks and a special regime for automated data analysis.

Generally speaking, data that has lost its significance, given the purpose for which it is processed, must be removed and destroyed unless legal rules on storage preclude this (Section 20 of the ISS Act 2017). To this end a periodic evaluation must be made of the significance of the data.

¹⁰² See ECHR 18 February 2000, no. 27798/95 (*Amann vs. Switzerland*), Section 65, ECHR 4 May 2000, no. 28341/95 (*Rotaru vs. Rumania*), Section 43, ECHR 28 January 2003, no. 44647/98 (*Peck vs. the United Kingdom*), Sections 63-63, ECHR 17 July 2003, no. 63737/00 (*Perry vs. The United Kingdom*), Sections 38 and 40-41 and the ECHR 17 December 2009, no. 16428/05 (*Gardel vs. France*), Section 62.

¹⁰³ ECHR 4 December 2008, no. 30562/04 and 30566/04 (*S. and Marper vs. The United Kingdom*), Section 67.

¹⁰⁴ See ECHR 28 January 2003, no. 44647/98 (*Peck vs. The United Kingdom*) Sections 62-63 and ECHR 2 September 2010, no. 35623/05 (*Uzun vs. Germany*), Section 45: "Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that is normally foreseeable", and ECHR 13 September 2018, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch et al. vs. The United Kingdom*).

¹⁰⁵ Although the ECHR does not prescribe that this be a formal Act, Section 10 of the Constitution does.

¹⁰⁶ See ECHR 25 September 2001, no. 44787/98 (*P.G. & J.H. vs. The United Kingdom*), Sections 44 and 61, ECHR 1 July 2008, no. 58243/00 (*Liberty et al. vs. The United Kingdom*), Section 62, ECHR 2 September 2010, no. 35623/05 (*Uzun vs. Germany*), Section 61 and ECHR 21 June 2011, no. 30194/09 (*Shimovolos vs. Russia*), Section 68.

Conclusion:

Data from special investigatory powers, such as the hacking power, must be assessed for relevance within a year (with the option to extend for a further six months) for the investigation for which it was required or other ongoing investigations. After that term, the data that has not been assessed as relevant must be destroyed immediately. As soon as data has been assessed as non-relevant, it must be destroyed immediately. Relevant data is made available to the services' full range of tasks. There is no legal retention period for this type of data. The law does require that data which has lost its significance must be removed and ultimately destroyed.

5.2 Safeguards for bulk data sets

The severe privacy infringement connected with processing bulk data sets is a reason to apply safeguards when the data is processed further. It ensues from the general requirements for data processing that this should be done properly and carefully (Section 3.1). Moreover, the services have a legal duty of care for the lawfulness and quality of the data they process (Section 3.2).

In its review report no. 53 (April 2017), the CTIVD pointed out that the data copied by the service in a hack must be made available to the operational teams to assess this data for its relevance for the task performance (now regulated in Section 27 of the ISS Act 2017). The CTIVD defined two safeguards to limit the access to as yet unassessed data in order to keep the infringement of fundamental rights and interests of the people involved within acceptable boundaries:

1. The condition that staff only have access to as yet unassessed data, where necessary for the proper execution of their designated tasks (*need-to-know*). This includes the use of internal systems and applications that are secured and screened off, and not accessible to internal third parties without separate authorization and an authorization policy to access the data so that only those staff members who need access based on their work activities are given it.¹⁰⁷
2. If the as yet unassessed data has been copied in an untargeted way and is expected to consist mainly of data that is not relevant to the services' proper task performance, the further condition of a division of job roles and tasks applies. This prerequisite must be apparent in the authorization request. The purpose is to prevent, as much as possible, data on people and organizations who are not targets ending up in the operational process. One example of how to achieve this is to restrict full and direct access to the unassessed data to a select group of technical staff and to ensure that only directly involved operational staff – after authorization – have access and can inspect the data based on references and queries (whereby staff from other operational teams may only have access on a hit/no hit basis and subsequently inspect the contents of a hit after internal authorization by a head of team or a head of bureau).¹⁰⁸

Partly following on from the recommendations in review report no. 53 and review report no. 55 (February 2018) about the acquisition of bulk data sets offered on the internet by third parties, the services have set out in public policy, published on their website, that they use certain safeguards when processing bulk data¹⁰⁹ Essentially this means that data that has been collected but not yet assessed for relevance is not accessible to every staff member. Service staff members must submit a separate request to gain access to the data in a bulk data set and they must substantiate why they need that data to perform their tasks. In other words, staff must be granted authorization to gain access to the

¹⁰⁷ CTIVD review report no. 53, Section 7.2 (making accessible).

¹⁰⁸ Ibid.

¹⁰⁹ www.aivd.nl.

data. More specifically this concerns the 'inner box/outer box procedure' and authorization policy. These safeguards are included in the requests for 'bulk hacks' in the investigation period.

In its Progress Report III (December 2019) the CTIVD established that the services subject themselves to these safeguards regarding the use of whole or partial bulk data sets from the hacking power. That prevents the data from automatically becoming available to the operational teams and being used in the operational process. Bulk data sets are not accessible to just anyone but may be searched by staff of operational teams using references. When a reference yields results, internal authorization must first be sought before the data in question can be inspected.

In this context, the CTIVD found that, although it was positive that both services have imposed additional safeguards on themselves when using bulk data sets, it does not mean this is sufficient. Compare this to the investigatory power of investigation-related interception with which data can also be collected in bulk – the safeguards for the legal protection of citizens are far stricter in that respect. In the case of investigation-related interception, including the investigatory power to select, external authorization and independent assessment prior to accessing and analyzing the data have been introduced and the data must be destroyed if it has not been declared relevant within three years. In the case of bulk data sets, no external authorization or independent assessment prior to the use of the data have been introduced. More importantly, as a result of declaring whole or partial bulk data sets relevant, the final destruction term for the data has ceased to apply while the data has not been assessed on its content. Nor are there any other safeguards that provide adequate legal protection.¹¹⁰

5.3 Reporting

Based on the general requirements for data processing, the AIVD and the MIVD must process data properly and carefully (see Section 3.1). Moreover, the services have a legal duty of care for the lawfulness and quality of the data they process (Section 3.2). This means that they are continuously in control of their data processing processes and that they are able to identify risks and take measures in time.

A service is unable to comply with this without careful internal reporting of how the data was processed. The reporting must be accurate enough to be able to establish compliance with the provisions regarding data processing in the ISS Act 2017. This requirement ensues from the regular data protection legislation that still holds as a guideline for the AIVD and the MIVD, except the restrictions in connection with the exceptional nature of these services.

Where the manner of reporting is concerned, the CTIVD has set out in its report no. 55 (2018) in the context of careful data processing of bulk data sets offered on the internet by third parties, that actions relating to bulk data sets must be recorded by logging and that automated reports must be drafted on that basis for internal control purposes of the services and external control purposes of the CTIVD.¹¹¹


¹¹⁰ VGR III, no. 66 (published 3 December 2019), p. 8, *Parliamentary Documents II* 2019/00, 34 588, no. 85 (appendix), pp. 8-11.

¹¹¹ See report no. 55 (2018), pp. 18 and 22.

6. Summary of legal requirements

Based on the assessment framework, the CTIVD has defined the following requirements for the collection of bulk data sets using the hacking power and the further processing of those data sets:

- Generally speaking, the services must observe purpose limitation when processing data and the data processing must be necessary for them to perform their tasks. This must also be done in a proper and careful manner (Sections 18 and 19 of the ISS Act 2017).
- Moreover, the AIVD and the MIVD have a duty of care for the lawfulness and quality of the data they process (Section 24 of the ISS Act 2017).
- The hacking power may only be exercised after authorization by the minister involved and after a positive assessment by the Investigatory Powers Commission (TIB). This independent lawfulness assessment by the TIB is an important new safeguard in the ISS Act 2017. The TIB assesses the substantiation of the legal requirements of necessity, proportionality, subsidiarity and as targeted as possible (Sections 26 in conjunction with 29(2) of the ISS Act 2017 in conjunction with Article 5 of the Policy Rules of the ISS Act 2017).
- A special investigatory power may only be used for the benefit of the services' intelligence and security tasks (Section 28 of the ISS Act 2017).
- The request for authorization must contain a description of the technical risks involved in the use of the hacking power (Section 45(2)(a) of the ISS Act 2017).
- Records must be kept of the hacking power exercised (Section 31 of the ISS Act 2017). That may be done in writing and through automated logging.
- Once the use of the hacking power (entering) has ended, the services have a best-efforts obligation to remove any technical aids they used, unless operational or technical interests preclude this. A report must be drawn up if the duty to clean up was not performed (Section 45(7) of the ISS Act 2017).
- The bulk data sets copied using the hacking power must be assessed for relevance as soon as possible, but no later than one year. After that term (including the option to extend a further six months) the data that has not been assessed must be destroyed immediately (Section 27 of the ISS Act 2017). Relevant data that has lost its significance, given the purpose for which it is being processed, must be removed and destroyed unless legal rules on retention preclude this (Section 20 of the ISS Act 2017). To this end, a periodic evaluation must be made of the significance of the data.
- Because of the privacy-sensitive nature of the bulk data sets, further safeguards for access and use of that kind of data must apply. Due to the lack of specific legal regulations in this area, these safeguards follow from the requirement of proper and careful data processing (Section 18 ISS Act 2017) and the duty of care that the services have (Section 24 ISS Act 2017). To this end the services use an 'inner box/outer box procedure' and authorization policy.
- The processing of bulk data sets must be carefully recorded internally (Section 18 in conjunction with Section 24 of the ISS Act 2017), not only to ensure continuous internal control but also to enable effective external review.



Oranjestraat 15, 2514 JB The Hague
P.O.Box 85556, 2508 CG The Hague

T T 070 315 58 20
E info@ctivd.nl | www.ctivd.nl