Review report

On the deployment of virtual agents by the AIVD and the MIVD

CTIVD no. 79

Adopted on 25 July 2024

Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence
and Security Services

CTIVD no. 79

REVIEW REPORT

On the deployment of virtual agents by the AIVD and the MIVD

Contents

Review Committee
on the Intelligence
and Security Services

CTIVD no. 79

REVIEW REPORT

On the deployment of virtual agents by the AIVD and the MIVD

Summary

The General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) are authorised to deploy natural persons for the targeted acquisition of information on persons or organisations that may be relevant to the performance of these intelligence and security services' tasks. If these persons are being directed and instructed by the AIVD or the MIVD, this concerns special powers, and these persons are referred to by law as 'agents'. This power can also be used in a virtual environment. The agents are then referred to as 'virtual agents', regardless of whether or not they are employed by either of these intelligence and security services. This review report discusses the deployment of virtual agents by the AIVD and the MIVD (hereinafter referred to as 'the services'). The investigation by the Review Committee on the Intelligence and Security Services (CTIVD) shows that virtual agents are deployed for many of the services' different areas of interest, such as gathering data to protect national security from terrorism and extremism. The activities of virtual agents mainly take place on chat services, in online forums and on social media.

The CTIVD has previously already reported on the activities of persons employed and not employed by the AIVD who collected information on social media to support the AIVD in performing its tasks. At the time, among other things, a policy framework for the deployment of virtual agents was missing. Since then, a policy framework has been introduced that both services adhere to. Several aspects of the deployment of virtual agents have changed in practice, especially in relation to the acquisition of large amounts of personal and other data. When acquiring large amounts of personal and other data, this may be subject to far-reaching infringements of fundamental rights. This is especially the case when those data or data sets mostly concern records about persons or organisation that are not, or never will be, the subject of investigation by the services. We refer to these as 'bulk data sets'. This practice, which is subject to developments, was part of the reason why the CTIVD decided to carry out this lawfulness investigation. This investigation therefore looks at the question to what extent the services lawfully deploy virtual agents to obtain data, data sets and bulk data sets available online. Specifically, it looks at the deployment of virtual agents for (1) the acquisition of bulk data sets and (2) the acquisition of data on online trade forums.

During the investigation period from 1 January 2020 to 1 June 2023, the CTIVD reviewed the lawfulness of the use of the power to deploy agents with regard to five virtual agents of the services on a random basis. These virtual agents acquired bulk data sets in an online environment or acquired data via online trade forums. This concerned dozens of bulk data sets during the investigation period, in some cases concerning tens of millions of records. These bulk data sets generally do not concern personal or other records of residents of the Netherlands, but rather records of people in countries the services are investigating.

The general picture obtained by the CTIVD indicates that the services deploy virtual agents in a lawful manner. The policy in effect at both of these services provides for technical and organisational measures that are necessary to deploy a virtual agent. Additionally, the security of employees active as agents in an online environment is laid down in policy, as well as the method of maintaining records of the activities of these virtual agents. In practice both services adhere to the policy for the deployment of virtual agents. The investigation into the policy and application in practice shows that the duty of care regarding confidentiality of the services' sources is observed in a lawful manner. The duty of care to safeguard the security of persons with whose cooperation data are gathered is also observed in a lawful manner.

During the investigation period, the CTIVD identified three counts of unlawfulness and three counts of negligence in total. Two of the three counts of unlawfulness identified by the CTIVD concerned the deployment of virtual agents and related to the lack of a proper basis for the acquisition of bulk data sets on the one hand and the lack of permission for virtual agents committing criminal offences on the other (MIVD). One count of unlawfulness concerned the approval request for a virtual agent of the AIVD that the CTIVD was unable to retrieve. The counts of negligence identified in this report concerned the recording of considerations for data minimisation and the requests to use the power to deploy agents in an online environment by the services. They concerned shortcomings in the considerations regarding the proportionality and the focus of the requests for deploying virtual agents. These shortcomings were mostly of a procedural nature. Following on from the provisional findings of the CTIVD, the intelligence and security service has taken adequate mitigating measures to address the identified counts of unlawfulness and negligence.

During the investigation period, the MIVD deployed fewer virtual agents compared to the AIVD. The policy and the organisational embedding of the deployment of virtual agents were also different at the MIVD than at the AIVD. In one instance, the procedure based on the original policy at the MIVD resulted in unlawful actions; bulk data sets acquired by a virtual agent were registered under the general power to deploy informants instead of the special power to deploy agents, resulting in a longer retention period. The CTIVD brought these unlawful actions to the attention of the director of the MIVD and the Minister of Defence in an interim (classified) letter. In response to this letter, measures were taken to rectify the unlawfulness, and a promise was made to register the related bulk data sets on the correct legal basis and to destroy them if necessary.

In relation to the acquisition of data and data sets through the deployment of virtual agents, the CTIVD has established that, both in the acquisition of bulk data sets and in the acquisition of data on online trade forums, this is in general done lawfully. The CTIVD has established that, in all cases involving the acquisition of bulk data sets, an acquisition memorandum was drawn up, checking the necessity, proportionality and subsidiarity of the acquisition. However, it should be recorded more clearly whether an assessment has taken place of the possibility of data minimisation in relation to the acquisition of bulk data sets and what the outcomes are of this assessment.

CTIVD no. 79

REVIEW REPORT

On the deployment of virtual agents by the AIVD and the MIVD

1. Introduction

This review report discusses the deployment of virtual agents by the services. An agent is a natural person who is deployed by the services for the targeted gathering of data on persons and organisations relevant to the performance of tasks by these services. When the power to deploy agents in an online environment (the Internet) is used, this concerns the deployment of a virtual agent. A virtual agent can be either an employee of the services or an external party.

The power to deploy agents as set out in Section 41 of the ISS Act 2017 is a special investigatory power with regard to which – contrary to most other special powers – the Investigatory Powers Commission (TIB) does not issue a lawfulness decision. Pursuant to the ISS Act 2017, the Minister or on their behalf the director of an intelligence and investigation service should grant permission for the use of the power to deploy agents. In this case, a mandate regulation can be established for each intelligence and security service stipulating that an employee in a lower position than the director of the intelligence and security service may grant permission. The CTIVD can monitor the lawfulness of this deployment both during and after the use of the power to deploy agents.

Previously, the CTIVD had already confirmed that the AIVD deploys agents in an online environment for the performance of its tasks. For example, this involved gathering and further processing data in order to protect national security from jihadist terrorism. In review report no. 39 (2014), the CTIVD reported on the activities of persons employed and not employed by the AIVD who collected information on social media on the AIVD's behalf. At the time, among other things, a policy framework for the deployment of virtual agents was missing. In review report no. 55 (2017), the CTIVD made recommendations regarding clearly setting out which legal basis (open source, informant or agent) applies in which situation to the acquisition of bulk data sets made available by third parties on the Internet.

It was also recommended that a general policy framework be developed for the acquisition of (bulk) data.In the ten years following the publication of review report no. 39, there have been further developments in the deployment of virtual agents by the services, especially regarding the frequency and working methods of acquiring data, data sets and bulk data sets in an online environment. Bulk data sets are large collections of data, the vast majority of which concern organisations and/or people that are not, and never will be, the subject of investigation by the services.[1] This concerned dozens of bulk data sets during the investigation period, in some cases concerning tens of millions of records.

1 See Appendix I Assesment framework to review report no. 55 (2018) on bulk data sets made available by third parties online and review report no. 70 (2020) on collecting bulk data sets using hacking powers.

Most of these bulk data sets do not concern personal or other records of residents of the Netherlands, but rather records of people in countries the services are investigating. Gathering large amounts of data in bulk is an infringement of the fundamental rights of citizens and requires sufficient safeguards. In view of these developments, among others, the CTIVD believes there is cause to carry out a lawfulness investigation.

1.1 Scope of the investigation and research question

The following research question is the focus of this report:

> *To what extent do the services lawfully deploy virtual agents to obtain data, data sets and bulk data sets available online?*

To answer the main research question, it was divided into three subquestions:

1. Based on the provisions of the ISS Act 2017 relating to the deployment of virtual agents, can this deployment be said to be lawful?
2. Are virtual agents deployed lawfully for the acquisition of bulk data sets?
3. Are virtual agents deployed lawfully for the acquisition of data and data sets on online trade forums?

During the investigation period from 1 January 2020 to 1 June 2023, the CTIVD reviewed the lawfulness of the use of the power to deploy agents with regard to five virtual agents of the services on a random basis. These virtual agents acquired bulk data sets in an online environment or acquired data via online trade forums.

1.2 Methodology

In this report, the CTIVD reviews the lawfulness of the deployment of virtual agents against the review framework (section 2.1). This review is based on the provisions of the ISS Act 2017 that apply to the power to deploy agents.

A verdict of 'unlawfulness' indicates a conflict with laws or regulations. These laws and regulations concern the Intelligence and Security Services Act 2017 (ISS Act 2017), case law and recommendations from previous CTIVD review reports adopted by the relevant Minister. In cases where actions are taken that are at odds with the working instructions, policy or processes of an intelligence and security service and this can be rectified, for example, by providing additional justification, this is referred to as 'negligence' in this report.

Over the course of this investigation, which was announced on 23 May 2023, the CTIVD interviewed 17 employees in total, working for different units of both services. The internal documents of the services were examined as well, along with requests and approvals for the use of the power to deploy agents, the policy and the operation reports on the activities of virtual agents. The CTIVD has also received an overview of all bulk data sets acquired by virtual agents during the investigation period and has investigated the documentation and reporting on the acquisition of data on online trade forums.

Care of duty aspects relating to the mental health of virtual agents were not considered in this investigation. This will be included in a different investigation into the duty of care regarding the mental health of agents in a broad sense, which has already been announced.

1.3 Classified appendix

This report has a classified appendix. This appendix does not list any instances of unlawfulness that are not also described in the public report. However, the classified appendix contains more detailed information reveals the services' procedure relating to subquestion 3 and for that reason had been marked 'classified'.

1.4 Structure of the report and reading guide

This report is structured as follows. In section 2, the CTIVD reviews several general aspects of the power to deploy agents, in part based on an overview and the follow-up to the main recommendations from relevant previous review reports. This mainly concerns the records maintained by the services when deploying virtual agents, policies and working instructions, requests for approval and criminal offences committed. In section 3, the CTIVD reviews the lawfulness of the acquisition of the data and data sets in an online environment. In particular, this section looks at the lawfulness of the acquisition of bulk data sets (section 3.1) and the acquisition of data on legal and illegal online trading forums (section 3.2). The report concludes with section 4, which sets out the conclusions and recommendations. The report has a glossary as an appendix.

2. The deployment of virtual agents

Virtual agents are agents that collect data in a virtual environment in order to allow the services to perform their tasks. The intelligence and security agencies' tasks mainly involve investigations into persons or organisations that, either because of their objectives or their activities, represent a threat to national security.[2] Additionally, virtual agents are deployed in the interest of national security to carry out investigations into other countries.[3] The CTIVD's investigation shows that virtual agents are deployed for many of the services' different areas of interest. For example, this includes gathering and further processing data in order to protect national security from terrorism and extremism. Virtual agents are mainly active on chat services, in online forums and on social media.

In this chapter, the CTIVD answers the subquestion of whether, based on the provisions of the ISS Act 2017 relating to the deployment of virtual agents, this deployment can be said to be lawful. Section 2.1 looks at relevant previous reports discussing the deployment of virtual agents. It also describes the recommendations from previous reports that have been adopted by the services. Section 2.2 provides an outline of the deployment of virtual agents by the services based on the recommendations from previous review reports that have been incorporated into the policies of the services and the legal requirements for the deployment of virtual agents. Section 2.3 draws an interim conclusion to answer the first subquestion.

2.1 Relevant previous reports on the deployment of virtual agents

In previous review reports, the CTIVD described the legal framework for deploying agents in an online environment.[4] These review reports also discussed the process of maintaining records when exercising investigatory powers.[5] This section contains a summary of the review framework previously set out by the CTIVD.

In review report no. 39 (2014), the CTIVD reported on the activities of persons employed and not employed by the AIVD deployed on social media. Whereas deployment of *people not employed* by the AIVD on social was carefully considered and thought through, the CTIVD was critical of the deployment of AIVD employees as agents on the Internet. At the time, the CTIVD concluded that the reporting of activities of employees operating as agents on the Internet was lacking and therefore had to be considered unlawful.[6] The CTIVD recommended bringing the reporting of ongoing operations in line with the usual standards within the intelligence and security service without delay. It also recommended carefully recording the online identities of agents, as this is also in the interest of the agent's security and the operation's verifiability. The CTIVD furthermore recommended developing a policy framework for the deployment of virtual agents.

2 This concerns the so-called 'a task' in Section 8(a) ISS Act 2017 for the AIVD.
3 See Section 8(d) ISS Act 2017 and Section 10(e) ISS Act 2017.
4 See the assessment framework accompanying review report no. 39 (2014) on the lawfulness of the AIVD's investigation on social media, review report no. 55 (2018) on bulk data sets made available by third parties online and review report no. 74 (2021) on Automated OSINT by the AIVD and the MIVD.
5 Section 31 ISS Act 2017.
6 Review report no. 39 (2014) on the lawfulness of the investigation on social media by the AIVD, p. 36.

In review reports by the CTIVD and the legislative history of the ISS Act 2017, it has been determined that, when *an employee of the intelligence and security service* enters the closed portions of social media networks using an assumed identity, such as a fake profile, the power to deploy agents set out in Section 41 of the ISS Act 2017 is applicable.[7] In the context of the open source investigation, the power to deploy agents is appropriate if an employee is attempting to befriend a target using a 'fake account', thereby gaining access to data in a profile on a social media service that are not available to the general public and only to the target's 'friends'.[8] This involves interaction. The CTIVD has previously indicated that *interacting* with the provider of a bulk data set involves more than just registering or paying. For example, interaction may involve communication regarding a specific method of payment.[9]

Review report no. 55 describes a situation in which a bulk data set is made available on the Internet, with an employee of the intelligence and security service having made an account with an assumed identity to buy the bulk data set based on the informant power. The relevant employee did not use an existing VA profile and did not have a role as a virtual agent. It is not described as such in review report no. 55. Since then, the deployment of virtual agents has been further developed and embedded in policy. In the context of this investigation, the CTIVD considers it important that the information acquired by a virtual agent is considered information acquired pursuant to Section 41 of the ISS Act 2017, regardless of whether the information has been provided by another person on a voluntary/ unsolicited basis.

In addition to employees of the services, *people not employed* by the services can provide information using an online assumed identity to the services. The informants regulation in Section 39 of the ISS Act 2017 is in this case misused if the *person not employed* by the services is being 'directed' by these services. As soon as the intelligence and security service starts directing the external person, this concerns the use of the investigatory power to deploy agents, in this case virtual agents, as this concerns an online environment.

With regard to 'bulk data sets made available online by third parties', the CTIVD made the following three recommendations in review report no. 55 (2018): (1) when acquiring bulk data sets, the services should make it clear in internal policy which legal basis (regarding the deployment of a power) applies in which situation, (2) the services should assess, in the context of data minimisation, immediately following the acquisition, whether all data or all types of data in the bulk data set are actually necessary to achieve the goals set out in the justification and (3) a written justification for the acquisition of bulk data sets should be drawn up.

As with the deployment of agents in a physical environment, virtual agents may commit criminal offences in an online environment. In review report no. 39 (2014), the CTIVD described how agents may be instructed to commit criminal offences subject to strict conditions. At the time, attention had already been paid to committing speech offences in the context of the deployment of agents in radical or terrorist online environments, such as insults or sedition. In the acquisition of data by virtual agents, different criminal offences are important, such as the 'acquisition or publication of private data' as described in Section 139e of the Criminal Code. When permission is requested to commit criminal offences, the virtual agent must be given an explicit instruction and follow this.[10]

7 See review report no. 39 (2014) on the lawfulness of the AIVD's investigation on social media, Review report no. 55 (2018) on bulk data sets made available by third parties online and review report no. 74 (2021) on Automated OSINT by the AIVD and the MIVD and *Parliamentary Papers II* 2016/17, 34588, no. 3, p. 63.
8 Appendix I assessment framework to review report no. 74 (2021) on Automated OSINT by the AIVD and the MIVD, p. 11.
9 Appendix I assessment framework to teview report no. 55 (2018) on bulk data sets made available by third parties online, p. 12.
10 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 66.

2.2 Lawfulness decision provisions regarding the deployment of virtual agents

Maintaining records/reporting

Records must be maintained of the activities of virtual agents and the assignments issued to gather data on a target.[11] Reporting must make it possible for the CTIVD to discover how data was obtained using the power to deploy agents. The CTIVD's recommendation from Revew Report no. 39 (2014) was to bring the reporting of ongoing operations, when the power to deploy agents is used in an online environment, in line with the usual standards within the intelligence and security service. This recommendation was then adopted by the Minister of the Interior and Kingdom Relations.[12]

The general provisions regarding data processing, including a review of the necessity and proportionality, also apply to the acquisition and further processing of data.[13]The policy of the services takes account of these legal provisions, and the method through which virtual agents have acquired data is retraceable for the CTIVD. The requirement in Section 31 of the ISS Act 2017 to maintain records of the use of a power was therefore complied with in a **lawful** manner during the investigation period.

Policy and working instructions

In the decade following the publication of review report no. 39, the AIVD in particular has further developed this intelligence-gathering method and given it a place within the organisation. Policy and support for the deployment of virtual agents is present at both services, on both technical and organisational level, and is complied with in practice. In it, the services have paid attention to, among other things, duty of care aspects that apply to confidentiality regarding sources when deploying virtual agents. In this way, technical and organisational measures are taken to protect the identity of those who are active as agents in online environments. Both services have also drawn up policies regarding criminal offences committed by virtual or other agents.

In doing so, they are implementing the duty of care regarding confidentiality of their sources from which they have gathered information, in a **lawful** manner, as set out in Section 23 ISS Act 2017. The duty of care to safeguard the security of persons with whose cooperation data are gathered is also observed in a **lawful** manner.

During the investigation period, the MIVD deployed fewer virtual agents compared to the AIVD. The policy, the definitions and the organisational embedding of the deployment of virtual agents were also different at the MIVD than at the AIVD. In one instance, the working policy based on the original policy at the MIVD resulted in **unlawful** action. This was because, according to the MIVD's policy, data supplied by a virtual agent on a voluntary basis that were furthermore not acquired under the MIVD's instruction were registered based on the power to deploy informants (for more details, see section 3.1).

Recommendation:

The services should align their policies for the deployment of virtual agents, to ensure there is no difference between the definitions used and the translation of the legal obligations into the use of the power to deploy agents in an online environment by both services.

11 Section 31 ISS Act 2017.
12 *Parliamentary papers* 2013/14, 29924, no. 114, p. 3.
13 Section 18 ISS Act 2017.

Requests for approval, Section 41 ISS Act 2017

Pursuant to the ISS Act 2017, use of Section 41 ISS Act 2017 requires approval from the relevant Minister or from the director of an intelligence and security service on their behalf. In this case, a mandate regulation can be established for each intelligence and security service stipulating that an employee in a lower position than the director of the intelligence and security service may grant permission. With regard to requests for approval for the use of the power to deploy agents, the CTIVD believes the necessity and subsidiarity of the special power must be sufficiently justified in the request. In all five cases, it was clear for what investigation assignments the virtual agent would look for data in an online environment, which activities should take place to that end and why this was necessary for the services to perform their tasks. In four of the five cases, approval to use the power to deploy an agent was granted at the correct level. The actions taken in these cases were therefore **lawful**. In one case, the CTIVD was unable to find the initial approval for the deployment of a virtual agent, because this approval had not been registered in line with the services' policies. In this case, the AIVD therefore acted **unlawfully**. For the subsequent extensions in that same dossier, however, the approvals were registered.

With regard to the power to deploy agents, the proportionality check is not always sufficiently justified by the services. The director of the intelligence and security service or the minister granting approval for the deployment of an agent to acquire data sets must carefully weigh up the necessity of gathering data and the associated infringement of fundamental rights when carrying out the proportionality check (see section 3 for more details). The CTIVD has determined that the infringement of fundamental rights, especially the right to protection of privacy, required further justification in four of the five requests for the use of the power to deploy agents. This working method was **negligent**, since further investigation has shown that this requirement was actually met in practice. Following the investigation period, the CTIVD provided feedback on this to the services. The services have indicated with regard to the proportionality check that they will refer in future to the written check carried out with the acquisition and further processing of bulk data sets (for more details, see section 3.1), which looks at the proportionality of the acquisition of data sets in a **lawful** manner.

The request for the power to deploy agents set out in Section 41 ISS Act 2017 must furthermore describe how the working method will be made as specific as possible.[14] The services did not actually test this requirement in all five cases. This working method is also **negligent**. Even though this requirement was insufficiently elaborated in the justification of the request, the instructions and the description of the intended activities show that a sufficient framework is provided within which the agent is to gather data. The services have amended the request form for the use of the power to deploy agents, ensuring the specificity requirement is tested more explicitly.

Committing criminal offences

Virtual agents may be instructed by the services to commit criminal offences in the process of gathering data or data sets that are necessary for the services to perform their tasks.[15] These instructions must be recorded in writing pursuant to the ISS Act 2017. It is important not only to record the fact that such an instruction was issued verbally to the agent, but also what the instruction entailed (Section 41(7) ISS Act 2017).

14 This was required pursuant to Section 5, Policy rules, ISS Act 2017 up to and including 8 July 2021. As of 9 July 2021, this requirement has been enforced by Section 26 ISS Act 2017. See Bulletin of Acts and Decrees 2021, 117 and 119.
15 See Section 41(4) ISS Act 2017.

Instructions to agents or virtual agents to commit criminal offences may only be issued if this is necessary for the intelligence and security service to effectively perform its tasks or if this is necessary for the security of the natural persons involved.[16] For the acquisition of bulk data sets or the acquisition of data on an online trading forum (whether or not illegal), this may involve the offences 'acquisition of non-public data' or 'handling stolen data', for example.[17] The National Public Prosecutor for Counterterrorism (*Landelijk Officier van Justitie en Terrorismebestrijding*, hereinafter: LOvJ) works at the Public Prosecution Service as a liaison and provides advice to the services regarding which criminal offences may be applicable. The services for the most part comply with the procedure for granting approval for committing criminal offences and requesting advice from the LOvJ.

For the deployment of a single agent by the MIVD, wrongly no approval was granted for them to commit punishable offences. The initial request for deployment of this agent did result in approval for committing criminal offences being granted, but this approval was later not extended. This agent then gathered data by committing a criminal offence (computer intrusion as set out in Section 138ab of the Criminal Code), without approval for this having been obtained. The MIVD did not realise this at the time, accepted the gathered data and processed them further for the performance of its tasks. In the present case, approval was granted retroactively in the summer of 2023 for the criminal acts committed, and advice on this was acquired from the LOvJ. The virtual agent has now been granted permission to gather data and data sets for multiple investigation assignments. The lack of approval for a virtual agent of the MIVD to commit criminal offences is **unlawful**.

***Recommendation*:**
If a virtual agent commits a criminal offence for which approval was not granted or that was not covered by the instruction for committing a criminal offence, the services should reconsider whether the use of the power to deploy agents in the relevant case should continue, and if so, subject to what conditions and supplementary approvals.

16 See Section 41(4)(6) ISS Act 2017 and review report no. 39 (2014) regarding AIVD investigations on social media, p. 21 and Appendix I assessment framework to review report no. 55 (2017) on the acquisition of bulk data sets made available by third parties online, p. 15.
17 Section 138c and 139g of the Criminal Code.

3. Acquisition of data or data sets by virtual agents

The aim of this section is to answer the following subquestions:
- Are virtual agents deployed lawfully for the acquisition of bulk data sets?
- Are virtual agents deployed lawfully for the acquisition of data and data sets on online trade forums?

In this section, the CTIVD reviews the lawfulness of the acquisition of data and data sets by five virtual agents of the services. In doing so, it differentiates between the acquisition of bulk data sets and the acquisition of data on targets by a virtual agent on online trade forums (whether illegal or otherwise). Section 3.1 looks at the lawfulness of the acquisition of bulk data sets by virtual agents during the investigation period. It also discusses the written test that should accompany the acquisition of bulk data sets by the services, and the process of data minimisation following acquisition of bulk data sets. To conclude, the CTIVD looks at a specific situation at the MIVD concerning the basis for the acquisition of a bulk data set. Section 3.2 looks at the lawfulness of the actions of virtual agents when acquiring data on online trade forums.

3.1 Lawfulness decision regarding the acquisition of bulk data sets

During the investigation period from 1 January 2020 to 1 June 2023, virtual agents of the services gathered dozens of data sets, largely concerning tens of millions of records. Many of these data sets are (or were) accessible to anyone with access to the Internet. These bulk data sets generally do not concern personal or other records of residents of the Netherlands, but rather records of people in countries the services are investigating. These can be user data, for example, such as user names, full names, email addresses and address details.

Approval through acquisition memorandums

Prior to processing a bulk data set, the services will draw up a so-called acquisition memorandum. According to the policies of the services, this acquisition memorandum should already be drawn up before the actual acquisition of a bulk data set. For technical or operational reasons, this is not always the case. The acquisition memorandum functions as a written check of the necessity, proportionality and subsidiarity of the acquisition of the bulk data set, regardless of the basis on which acquisition of the bulk data set is approved. During the investigation period, an acquisition memorandum was in all cases drawn up for the acquisition of bulk data sets by virtual agents. The Minister of the Interior and Kingdom Relations (AIVD) or the Minister of Defence (MIVD), or the director of the intelligence and security service on their behalf, in each case approved the acquisition of the bulk data set.

Justification of the acquisition

The acquisition memorandums in each case included a check of the necessity, proportionality and subsidiarity of the acquisition. The CTIVD considers this check and its registration important safeguards. The necessity of the acquisition of the data to protect national security and subsidiarity was in all cases sufficiently justified. In each case, it was indicated which information need would be met by acquisition of the bulk data set.

Occasionally, the services gave insufficient weight to the severity of the infringement of fundamental rights (in particular the right to privacy) when carrying out the proportionality check. The fact that data are accessible to anyone (for a short time) does not mean that the infringement of the right to privacy for those involved is limited. The quantity and nature of the data in the bulk data sets, which, despite being accessible to anyone, largely originate from the internal systems of companies and institutions, mean that they are subject to repeated infringements of privacy.[18] In practice, in accordance with the ISS Act 2017 Temporary Regulation on further processing of bulk data sets (*Tijdelijke regeling verdere verwerking bulkdatasets*), necessity, proportionality and subsidiarity are again checked before a bulk data set is subjected to further processing by the services. During the investigation period, the CTIVD noticed the quality of the acquisition memorandums improved. Regarding the drafting of the acquisition memorandums, the services therefore acted **lawfully** when acquiring bulk data sets.

Data minimisation

The services should more emphatically check whether data minimisation of a bulk data set is possible. It is not always clear in advance what data are contained in the bulk data sets. As soon as this is clear, a data minimisation check should be performed. This check can be derived from the provisions on proper data processing.[19] Data minimisation also plays a role in the proportionality check and the implementation of the specificity criterion in acquiring a bulk data set. After all, removing data in a bulk data set affects the balance between the necessity and the infringement of privacy carried out with the acquisition and further processing of the data. The CTIVD believes that the services insufficiently implemented the previous recommendation to assess, following acquisition, whether all data or all data types in the bulk data set were actually necessary to achieve the goals set out in the justification and to destroy all unnecessary data. After all, it was insufficiently clearly recorded whether an assessment had taken place and what the outcomes of the assessment were. This was **negligent**.

Basis for the acquisition

For storing bulk data sets acquired through the power to deploy agents, the MIVD in certain cases used the power to deploy informants (Section 39 ISS Act 2017) as a basis. This is unlawful, as the bulk data sets were acquired through the use of the power to deploy agents (Section 41 ISS ACT 2017). This unlawfulness may be subject to an undesirable legal consequence, as data from bulk data sets acquired based on Section 39 ISS Act 2017 only need to be removed once they are no longer of significance. Data in bulk data sets that were gathered based on the special power in Section 41 ISS Act 2017 should be assessed on their relevance as soon as possible – within a year – with the possibility of a six-month extension. The director of the MIVD and the Minister of Defence were notified of these unlawful actions on 15 November 2023 by means of an interim (classified) letter. In response to this letter, the MIVD adjusted its policy and took measures to rectify this unlawfulness. The related bulk data sets have been destroyed.

Recommendation:

If virtual agents are instructed to acquire bulk data sets, this must be recorded in the request for the use of the power to deploy agents in which the object of the deployment is described. Moreover, following the acquisition of a bulk data set, regardless of the method of acquisition, it must be assessed whether all data or all types of data are necessary to achieve the objects set out in the justification, and this consideration must be recorded so it can later be verified that this actually took place. Data that are not necessary must be destroyed.

This recommendation has a wider scope than just the investigation into virtual agents.

18 See also review report no. 74 (2021) on Automated OSINT, p. 21.
19 See, among others, Section 18 ISS Act 2017.

3.2 Lawfulness decision regarding the acquisition of data on online trade forums

The classified appendix contains an elaboration of the working method for acquiring data on online trade forums. The CTIVD investigation has revealed that the services apply a **lawful** working method.

4. Conclusions and recommendations

Virtual agents are agents that collect data in a virtual environment in order to allow the services to perform their tasks, regardless of whether or not they are employed by either of these services. This investigation by the CTIVD shows that virtual agents are deployed by the services for many different areas of interest, such as gathering data to protect national security from terrorism and extremism. The activities of virtual agents take place on chat services, in online forums and on social media.

This report focuses on answering the main research question:

> *To what extent do the services lawfully deploy virtual agents to obtain data, data sets and bulk data sets available online?*

To answer the main research question, it was divided into three subquestions:

1. 1Based on the general provisions of the ISS Act 2017 relating to the deployment of virtual agents, can this deployment be said to be lawful?
2. Are virtual agents deployed **lawfully** for the acquisition of bulk data sets?
3. Are virtual agents deployed lawfully for the acquisition of data and data sets on online trade forums?

During the investigation period from 1 January 2020 to 1 June 2023, the CTIVD reviewed the lawfulness of the use of the power to deploy agents with regard to five virtual agents of the services. These virtual agents acquired bulk data sets in an online environment or acquired data via online trade forums.

Lawfulness decision general provisions regarding the deployment of virtual agents

The general picture obtained by the CTIVD indicates that the services deploy virtual agents in a lawful manner. Policy and support for the deployment of virtual agents is present at both services, on both technical and organisational level, and is complied with in practice. Through this policy, the legal requirement to maintain records of the use of a special power is implemented in a **lawful** manner. The duty of care regarding confidentiality of sources of the services and the security of persons with whose cooperation data has been gathered, as set out in Section 23 ISS Act 2017, is also implemented in a **lawful** manner.

During the investigation period, the MIVD deployed fewer virtual agents compared to the AIVD. The policy and the organisational embedding of the deployment of virtual agents were also different at the MIVD than at the AIVD. In one instance, the working policy based on the original policy at the MIVD resulted in **unlawful** action. This was because the MIVD's policy stipulated that data supplied by an agent on a voluntary basis that were furthermore not acquired under the MIVD's instruction should be unlawfully registered based on the power to deploy informants. The director of the MIVD and the Minister of Defence were notified of these unlawful actions on 15 November 2023 by means of an interim (classified) letter. In response to this letter, they have taken measures to rectify this unlawfulness, and a promise was made to register the related bulk data sets on the correct basis and to destroy them. The related bulk data sets have since been destroyed.

***Recommendation*:**
The services should align their policies for the deployment of virtual agents, to ensure there is no difference between the definitions used and the translation of the legal obligations into the use of the power to deploy agents in an online environment by both services.

Requests for approval of the deployment of virtual agents

With regard to requests for approval for the use of the power to deploy agents, the CTIVD believes the necessity and subsidiarity of the special power must be sufficiently justified in the request. In all five cases, it was clear for what investigation assignments the virtual agent would look for data in an online environment, which activities should take place to that end and why this was necessary for the services to perform their tasks. In almost all cases, the director of the intelligence and security service or the minister had granted approval for the use of the power to deploy agents. The actions taken in four out of five cases were therefore **lawful**. In one case, the initial approval for the deployment of the virtual agent was not registered in accordance with the AIVD's policy. This means the AIVD acted **unlawfully** in the initial deployment of the virtual agent in this case. The approvals for extension of the deployment of this virtual agent were subsequently registered, however.

With regard to the requests for approval, the CTIVD notes that the infringement of fundamental rights, especially the right to privacy, required further justification in four of the five requests for the use of the power to deploy agents. This working method was **negligent** according to the CTIVD, and not unlawful, since further investigation has shown that this requirement was actually met in practice. The services did not in all five cases sufficiently explicitly check the specificity requirement. Even though this requirement was insufficiently elaborated in the justification of the request, the instructions and the description of the intended activities of the agent clearly show what the agent was to focus on when gathering data. This working method was **negligent**. The services have amended the request form for the use of the power to deploy agents, ensuring the specificity requirement is checked more explicitly.

Criminal offences committed by virtual agents

Virtual agents may be instructed by the services to commit criminal offences in the process of gathering data or data sets that are necessary for the services to perform their tasks. The services in most instances comply with the procedure for granting approval for committing criminal offences and requesting advice from the LOvJ. For the deployment of a single agent by the MIVD, no approval was granted for them to commit punishable offences, despite criminal offences then being committed. This was **unlawful.**

***Recommendation*:**

If a virtual agent commits a criminal offence for which approval was not granted or that was not covered by the instruction for committing a criminal offence, the services should reconsider whether the use of the power to deploy agents in the relevant case should continue, and if so, subject to what conditions and supplementary approvals.

The use of the power to deploy agents to acquire data or data sets

Virtual agents may be instructed by the intelligence and security service to gather data or data sets that are necessary for the services to perform their tasks. It must be possible to find these instructions again in a request to use the power to deploy agents as set out in Section 41 ISS Act 2017. When these data or data sets largely concern records relating to organisations and/or people that are not, and never will be, the subject of investigation by the services, this means they are bulk data sets.

Acquisition of bulk data sets by virtual agents

During the investigation period, virtual agents of the services gathered dozens of data sets, often with records on tens of millions of people. These bulk data sets largely contain data on people from countries the services are investigating. These can be so-called user data, for example, such as user names, full names, email addresses and address details. Prior to processing a bulk data set, the services will draw up an acquisition memorandum. The memorandum functions as a written check of the necessity, proportionality and subsidiary and is carried out before the data in bulk data sets are taken into use. This acquisition memorandum is drawn up regardless of the legal basis on which the bulk data sets are acquired. During the investigation period, an acquisition memorandum was in all cases drawn up for the acquisition of bulk data sets and checked for necessity, proportionality and subsidiarity. The CTIVD considers this check and the registration important safeguards ensuring lawful implementation of the acquisition of bulk data sets by virtual agents. The necessity of the acquisition of the data to protect national security and subsidiarity was in all cases sufficiently justified.

However, the CTIVD argues that the possibility of data minimisation of a bulk data set should be checked more emphatically. The CTIVD believes that the services insufficiently implemented the previous recommendation to assess, following acquisition, whether all data or all data types in the bulk data set were actually necessary to achieve the goals set out in the justification and to destroy all unnecessary data. After all, it was insufficiently clearly recorded whether an assessment had taken place and what the outcomes of the assessment were. This was **negligent**.

Recommendation:

If virtual agents are instructed to acquire bulk data sets, this must be recorded in the request for the use of the power to deploy agents in which the goal of the deployment is described. Moreover, following the acquisition of a bulk data set, regardless of the method of acquisition, it must be assessed whether all data or all types of data are necessary to achieve the goal set out in the justification, and this consideration must be recorded so it can later be verified that this actually took place. Data that are not necessary must be destroyed.

This recommendation has a wider scope than just the investigation into virtual agents.

Acquisition of data on online trade forums

The services apply a lawful working method when deploying virtual agents who acquire data on online trade forums.

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

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl