Summary of Report

Automated OSINT: tools and sources for open source investigation

CTIVD No. 74

CTIVD

Review Committee on the Intelligence and Security Services

Review Committee
on the Intelligence
and Security Services

CTIVD No. 74

SUMMARY OF REPORT

Automated OSINT: tools and sources for open source investigation

Summary

The Intelligence and Security Services Act 2017 (ISS Act 2017) permits the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) to collect and process publicly accessible data, including personal data. These activities are also referred to as open source investigation or OSINT, which stands for 'open source intelligence'. The Dutch legislator does not consider OSINT to be an intrusive intelligence method.

When open source investigation is automated using specialized software, it is referred to as 'automated OSINT'. In this report, a distinction is made between the tools that are used and the sources (datasets) that may be accessed using these tools. The tools include software equipped with functions for search and network analysis which can query a wide variety of sources. These tools may come from commercial providers or they can be developed by the services themselves.

Tools for automated OSINT offer two major advantages over conventional open source investigation using an ordinary web browser. The first of these is ease of use: a single search using an automated OSINT tool can query hundreds of sources simultaneously. The tool can then provide a visual representation of the results. The second major advantage of using such tools is that they give access to dedicated sources provided by the tool's vendor on a commercial basis. One example of this is leaked data from users of social media services. Vendors can aggregate these datasets as a single searchable source, which may contain billions of records.

Another example of commercial data that can be accessed through these tools consists of location data generated by advertisements shown to application users (i.e. mobile phones). Providers of commercial tools for OSINT can purchase advertising data - including location data - from data brokers and use their tool to make it available to clients, including intelligence and security services.

The volume, nature and range of personal data in these automated OSINT tools may lead to a more serious violation of fundamental rights, in particular the right to privacy, than consulting data from publicly accessible online information sources, such as publicly accessible social media data or data retrieved using a generic search engine.

From the explanatory memorandum of the ISS Act 2017, it can be concluded that the practices facilitated by automated OSINT were not taken into account by the legislator at the time. Automated OSINT undeniably goes well beyond classic investigative techniques such as checking telephone directories or using a search engine to access online data and will continue to develop in the near future. This report reflects the following reality: automated OSINT can provide simultaneous searchable access to hundreds of sources of various origins, including location data or data from leaked datasets.

The current practice of automated OSINT involves a more serious violation of privacy than was anticipated when the ISS Act 2017 was drafted.

This finding leads to recommendation 1:
Given the nature, diversity and volume of the data at issue, the Review Committee on the Intelligence and Security Services (CTIVD) recommends that the legislator creates a more foreseeable legal basis with sufficient safeguards governing the use of automated OSINT for both the tools themselves and the sources that can be accessed using these tools.

In the present report, the CTIVD's lawfulness assessment focuses primarily on the OSINT tools and the sources that can be accessed using these tools. How these tools and sources are used in actual cases does not fall within the scope of this report. The CTIVD considers it essential that the services know how the tools operate and which sources can be consulted prior to actual deployment. Only with this knowledge, a thorough assessment can be conducted to determine how the processing of this data with these tools relates to the general data processing provisions of the ISS Act 2017. Among other things, these provisions require that the processing of data by the services should be proportionate. This means that there must be an appropriate balance between the interests at stake in processing the data for the relevant intelligence investigation and the severity of the breach of the fundamental rights of the data subject.

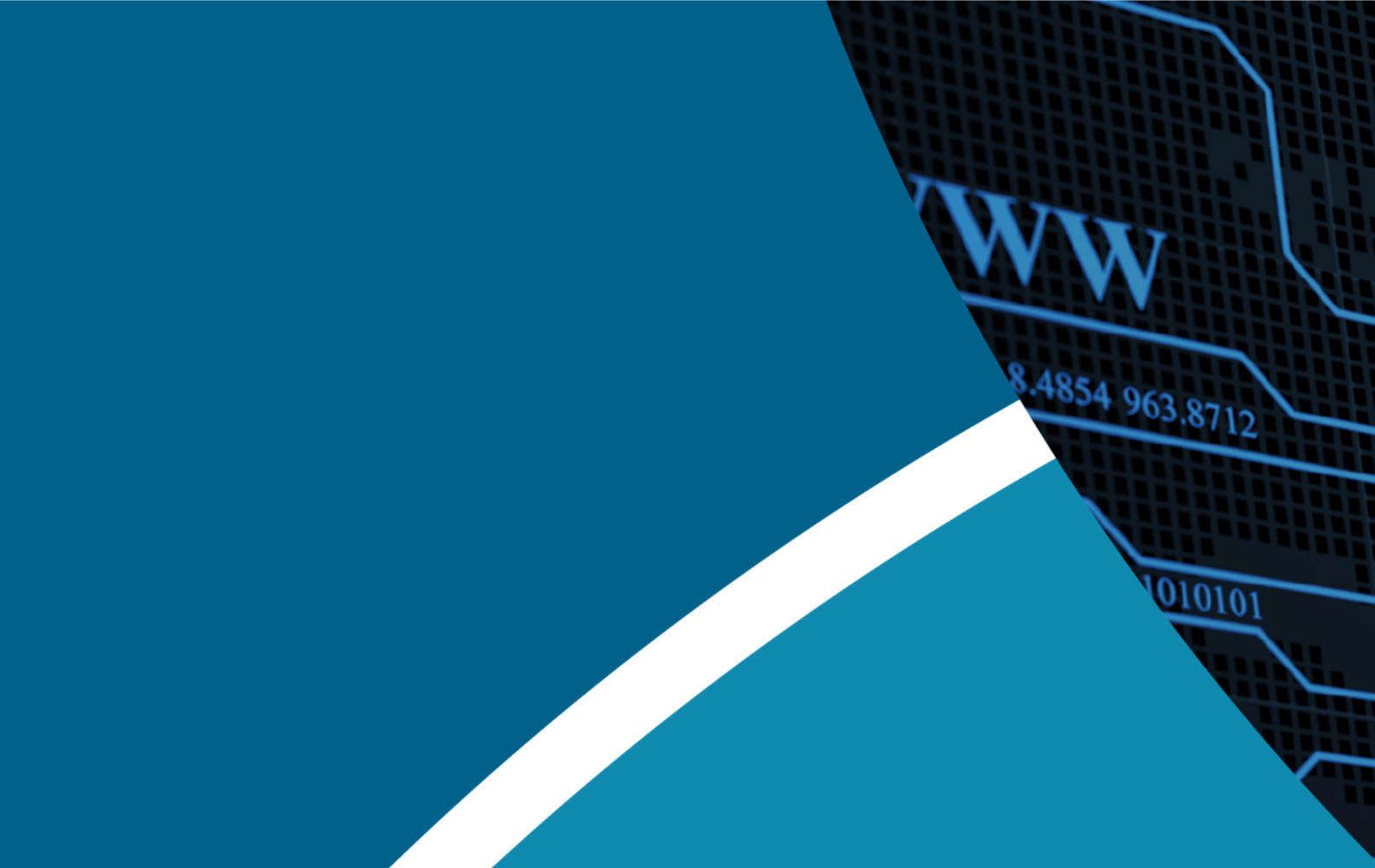
By conducting this review, the CTIVD aims to answer the following question:
Do the AIVD and the MIVD have a sufficient understanding of the operation of the automated OSINT tools and the origin and the nature of the underlying sources with a view to complying with the data processing provisions?

The answer to this question is that the AIVD's and the MIVD's understanding of the workings (the functionalities) of the automated OSINT tools and the origin and nature of the sources that can be consulted using these tools is insufficient to ensure compliance with the data processing provisions of the ISS Act 2017. The CTIVD notes that several improvements are needed before automated OSINT can be brought into compliance with the law. The services should identify (as thoroughly as possible) the workings (i.e. functionalities) and the underlying sources of the tools, and take mitigating measures in this regard to prevent unlawful conduct in the future.

This finding leads to recommendation 2:
When selecting and acquiring tools for automated OSINT (and thereby selecting the underlying sources), the AIVD and the MIVD should also aim to ensure lawful data processing. Preferably, the two services should work together to develop a joint policy framework with accompanying operational instructions.

In the interests of legal certainty, lawfulness and operational effectiveness on the part of the services, the CTIVD will enter into a dialogue with the services in order to arrive at a workable temporary assessment framework which the services will then translate into policy, procedures, and operational instructions. This temporary assessment framework should, among other things, address the establishment of a prior assessment in light of the data processing provisions, the criterion of a systematic approach to open source investigation and the handling of sources whereby the origin and accuracy of the data cannot be clearly established.

The use of OSINT is not exclusive to the domain of the intelligence and security services but also applies elsewhere in the national security domain (for example, at the National Coordinator for Security and Counterterrorism (NCTV)) and beyond (including other government bodies). The CTIVD therefore requests the Minister of the Interior and Kingdom Relations and the Minister of Defence to bring this report to the attention of other government bodies and, when forwarding the report, to ask Parliament to bring it to the attention of the House of Representatives' Standing Committee on Digital Affairs.



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

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