Review Committee on the Intelligence and Security Services

CTIVD

BRIEF OUTLINE

Response of the CTIVD to the ISS Act 20 draft bill**

The CTIVD's response in brief outline

On 1 July 2015 the Review Committee for the Intelligence and Security Services (CTIVD) received the draft bill for a new Intelligence and Security Services Act (ISS Act) from the minister of the Interior and Kingdom Relations, also acting on behalf of the minister of Defence. The ministers gave the CTIVD the opportunity to comment on the draft. The CTIVD sent its response to the ministers on 3 September 2015. The following is a brief outline of this response.

Its core mandate, so the CTIVD holds, is to contribute by means of its independent oversight of the lawfulness of the conduct of GISS and DISS to finding the right balance between the interest of national security and the interest of protecting privacy. In its review reports the CTIVD in recent years identified several problem areas where, in its opinion, such a balance was not always found. It made recommendations on these issues to the ministers. The CTIVD notes, and appreciates, that many of these issues have been given a place in the draft bill and/or the explanatory memorandum.

The CTIVD will not express an opinion on the desirability or otherwise of the proposed extension of the powers of the services. That falls outside its task. It confines its response to the question whether, as a corollary of the extension of powers, the privacy safeguards will be sufficiently strengthened.

The chosen approach

The proposed draft bill extends the powers of the services in a number of areas. These include not only the extension of the powers of interception so as to include cable communications, but e.g. also an extension of the power to hack and the power to carry out data analysis. As also stated by the Dessens Committee in its evaluation report, such an extension of powers of GISS and DISS should be accompanied by strengthened independent oversight of how these powers are exercised in actual practice. This means that the oversight must be designed so as to constitute an effective, essential safeguard against possible unjustified privacy infringement. The basic principle must be that the more the services are permitted to infringe privacy in terms of quantity and sensitivity of the data they collect and process, the greater the importance of having such a safeguard in place.

The central theme of the CTIVD's response to the draft bill is therefore: **effective oversight as a safeguard against unjustified privacy infringement.**

There are two important factors that make for effective oversight: (1) the position of the oversight body; it must be independent and impartial, have access to all information at the services and have the means to intervene coercively when rules are infringed, and (2) a statutory standards framework that provides clear and tangible criteria, thus enabling the oversight body to review the actual conduct of the services for lawfulness. These requirements ensue from the European and international human rights framework for the supervision of intelligence and security services. In the context of assessing the draft bill the above translates into the following two questions: (1) **Will the position of the CTIVD as oversight body be sufficiently strengthened?** And (2) **Does the proposed framework provide an adequate basis for oversight?**

When the CTIVD examined the draft bill and the explanatory memorandum, it also came across issues which do not primarily concern effective oversight, but rather the protection of privacy in general. When considering these issues the CTIVD asked itself: (3) **In which areas are adequate safeguards for the protection of privacy still lacking?**

Will the position of the CTIVD as oversight body be sufficiently strengthened?

The answer to this question is, to put it briefly: no, the proposed powers of the CTIVD fall short of what is necessary. Current European and international human right standards show that there can be no effective oversight unless the position of the CTIVD is further strengthened beyond what is proposed in the draft bill. Its main weakness is the omission to grant the CTIVD power to give binding decisions when it reviews whether the services act lawfully when exercising their most infringing powers, such as the power to intercept and the power to hack. It could be argued that the oversight body as regulated in the draft bill lacks sufficient teeth.

The CTIVD bases this position among other things on a recent study by Leiden University commissioned by it (the report is attached to this reaction as an **appendix**).

The main focus of the draft bill in the area of oversight is on complaints handling. It proposes to give the CTIVD the position of an external complaints handler instead of an internal complaints advisory committee to the minister. The final, binding decision on complaints about activities of the services will thus come to lie with the CTIVD and therefore no longer with the minister, as is currently the case. That is without doubt a good development. However, with regard to overseeing the lawfulness of the activities of the services (which makes up 90% of the CTIVD's work) the position of the CTIVD is only changed very slightly. The infringing special powers of the services (e.g. telephone taps or hacking PCs) are made subject to an obligation to reconsider, meaning that the minister must reconsider his permission to exercise the power if the CTIVD has established that it is being exercised unlawfully. If the minister upholds his earlier decision, he must inform the Parliamentary Committee on the Intelligence and Security Services and the CTIVD of this decision. The opinion of the CTIVD is therefore not binding on the minister. The obligation to reconsider merely introduces a higher threshold for the ministers.

As the CTIVD sees it, this proposal ignores the real function of reviewing whether privacy-infringing secret powers are being exercised lawfully. In the Dutch system the CTIVD is the only external party that has full access to and insight into what the services are doing. This enables the CTIVD to review the activities of GISS and DISS against the frameworks imposed by law. In fact, its oversight serves as a substitute for the possibility for citizens to invoke a remedy against infringement of their privacy, since a citizen will usually not be aware or become aware of such infringement because of its secret nature. This means that this oversight in its entirety, and not only as regards complaints handling, must make up an "*effective remedy*" within the meaning of article 13 in conjunction with article 8 of the ECHR. If the CTIVD considers that a secret power is being exercised unlawfully, then this should, in its opinion, entail more than a higher threshold for the minister to cross; in that case the door must be shut. The CTIVD must also have the authority to order the operation to be terminated and the collected data to be destroyed.

Binding ex post review of lawfulness does not affect the minister's responsibility for or the parliamentary oversight of the activities or policies of the services. The oversight exercised by the CTIVD focuses on the legal assessment of the authorisation and the exercise of special powers, not on the effectiveness or efficiency of the policies adopted and their implementation. There are in fact other fields in which a minister can be restricted in the implementation of his policy due to review by independent authorities, while he remains fully responsible towards parliament for the implementation of his policy.

Does the proposed framework provide an adequate basis for exercising oversight?

The CTIVD has established that in some areas, the legal framework proposed for the exercise of special powers does not provide sufficient clarity for effective oversight. Most of the questions arise with regard to the rules on large-scale (bulk) interception. On the basis of the description of the proposed 'three-phase model' in the explanatory memorandum, the CTIVD wrote out a fictitious case to gain an understanding of how the system might work in practice. The CTIVD has established that on various points the draft bill provides insufficient clarity regarding the scope and the interconnection of the powers. There are no clear definitions, for example, of the different forms of technical searching and searching of content. Furthermore, it is not clear to the CTIVD what internal arrangements the services will make to substantiate the reasons justifying the selection of communications from the intercepted bulk at the level of persons and/or organisations. In the proposed system this no longer requires the minister's permission, while at present it does.

In which areas are adequate safeguards for the protection of privacy still lacking?

A central issue in this part of the CTIVD's response are the retention periods for the different types of data that have been collected. After the expiry of the retention period the data must be destroyed. The Court of Justice of the EU ruled in 2014 that a retention period for stored (personal) data may not be longer than is strictly necessary and that it must be determined on the basis of objective criteria. The CTIVD notes that the proposed retention periods – one year for data collected by targeted interception and three years for bulk – are long to very long. The reasons stated in the explanatory memorandum for the duration of the proposed retention periods are not convincing, given the requirements set by the Court of Justice of the EU.

Another important point is the extension of the power to hack. The CTIVD holds the opinion that the draft bill does not provide sufficient safeguards for the situation that the services gain access to a computerized device or system of a third party with the aim of collecting information about a target.

In addition to the issues discussed above, the CTIVD comments on the provisions on cooperation with foreign intelligence and security services, automated data analysis, the extension of the power to promote or take measures, and the provision on the destruction of data relating to informers and agents.