The CTIVD's View

On the ISS Act 20.. Bill

November 2016

Anna van Saksenlaan 50 | 2593 HT The Hague
T +31 (0)70 315 58 20 | **F** +31 (0)70 381 71 68
E info@ctivd.nl | www.ctivd.nl

CTIVD
Review Committee
on the Intelligence and
Security Services

Review Committee on the Intelligence and Security Services

THE CTIVD'S VIEW

On the ISS Act 20.. Bill

On 28 October 2016, the government sent the Bill for the new Act on the Intelligence and Security Services to the Dutch House of Representatives. The Review Committee on the Intelligence and Security Services (CTIVD) hereby presents its view of this Bill. As an independent oversight body, which has direct access to the AIVD and the MIVD, the CTIVD has the expertise and competence that enable it to appraise the substance of the Bill and the application thereof in actual practice. This view aims to provide points of reference for the purposes of the parliamentary debate on the Bill.

Balance Achieved?

Based on its experience and understanding of practice, the CTIVD wants to provide insight into the balance that - in its opinion - should be achieved in the new Act on the Intelligence and Security Services (ISS Act 20..). A balance between the powers necessary to enable a timely detection of threats to national security on the one hand, and safeguards that provide effective protection from unlawful infringements of our fundamental rights, including privacy, on the other hand. The CTIVD believes that this balance has not been achieved in the ISS Act 20.. Bill. The recommendations included in this view are aimed at clarifying the essential safeguards that are lacking. Statutory safeguards that ensure the protection of privacy now and in the future, make effective review possible, and do not impose any unnecessary restrictions on the AIVD and the MIVD in the implementation of the statutory task assigned to them.

Expansion and Modernisation of the Powers

The CTIVD's picture of the scope of the existing powers of the AIVD and the MIVD, related to the question of whether these services must still be deemed able to ward off current and future threats to national security in practice with these powers, confirms the necessity of the proposed expansion thereof. Not only changes in the nature and scope of these threats play a role in this context - measured by severity and probability - but also the technological and social developments in the past few years. Developments that pertain to the creation of a digitalised society at a rapid pace, with ever changing means and methods of communication, which have resulted and will continue to result in an exponential growth in communication and data traffic. A growth with correspondingly large amounts of data that are transported and stored worldwide. Data collections that may be decisive for services such as the AIVD and the MIVD to perform their tasks properly.

More than is the case now, expansion and modernisation of the powers imply that the services will gain access to ever increasing amounts of data. The strong increase in the international exchange of data further contributes to this increase. The origin and reliability of these data deserve constant attention. Necessarily, more and more techniques are being developed and used to enable automatic processing of these data, from collecting and analysing to the destruction thereof. Not only the amount of data, but also the complexity of data processing has increased as a result of this, and will increase in the future.

Strengthening of Safeguards and Oversight

The safeguards for the protection of privacy and other fundamental rights should follow the above-mentioned developments at the same pace. If larger amounts of data are being collected, received, and processed, there are, of course, also larger amounts of data of persons and organisations that are not the target of the services. This results in a larger risk of unlawful infringements of privacy. Complex and automated forms of data processing also involve risks that require additional safeguards against unlawful use thereof. The safeguards concerned in this context include those for the quality of systems that provide automated access to data collections on the basis of specific characteristics or for technical processes that single out data on the basis of behavioural patterns and profiles.

The Bill places strong emphasis on classic safeguards, such as prior authorisation (Minister) and assessment of the use of the powers (Assessment Committee on the Use of Powers (TIB)). Although these safeguards have been strengthened considerably compared to the current statutory regulation, these safeguards alone are no longer sufficient. Especially for the collection and further processing of large amounts of data (bulk data), in particular for the purpose of establishing unknown threats, it has limited meaning to require substantiation linked to authorisation and independent assessment at the beginning of the process, for it is often unclear in advance who or what is exactly sought. Such a system of safeguards in advance is meaningful, in particular, if powers are used in a targeted manner in case of a known threat that involves a person or an organisation that is already in the picture.

Classic safeguards alone are no longer sufficient

Especially for the processing of increasing amounts of data, additional and future-proof safeguards are necessary. These safeguards must pertain to that phase of the data processing in which privacy (or other rights) is/are actually infringed, i.e. during the automated processing, analysis, and use phase. Those safeguards must be adequate and assessable. Essential in this context is a statutory duty of care for automated data processing, which is currently lacking in the Bill. This duty of care should imply that the services give account of the quality of the automated processes for data processing by means of instruments laid down by law, and that this quality can be reviewed effectively. In this context, the operational reality with which the AIVD and the MIVD are confronted daily should not be disregarded. This means that the scope of the administrative burden imposed on the services must be taken into consideration.

Review Committee on the Intelligence and Security Services
THE CTIVD'S VIEW
On the ISS Act 20.. Bill

In the context of the above-mentioned developments, strengthening of the oversight is a necessary precondition. Effective oversight requires oversight that can make itself felt especially in those areas where the infringement of fundamental rights has the greatest impact. The oversight will consequently have to be aimed at both technological data-processing methods including the way in which these methods are embedded in the systems of the services and at the resulting effects on privacy and other fundamental rights. With the current proposals alone, where the emphasis has been placed on authorisation and assessment in advance, this effectiveness has not been achieved.

Addition and Tightening are Essential

In this view, the CTIVD will discuss five themes that are relevant for achieving an appropriate balance in the new Act between powers on the one hand and safeguards against unlawful use thereof on the other hand. Below is a brief summary of the parts of the Bill that the CTIVD believe require addition or tightening. In that context, it is important to note that following the CTIVD's recommendations will also require sufficient resources for the services to be able to develop and install additional safeguards and for the oversight body/bodies to review their operation. Without granting these resources, the safeguards will remain empty and the oversight will not be effective.

Effective oversight requires oversight that can make itself felt especially in those areas where the infringement of fundamental rights has the greatest impact.

Oversight

In the Bill, the oversight lacks sufficient effectiveness where it concerns the oversight of automated data processing. It is recommended to clarify the scope of the oversight in relation to the assessment by the TIB in order to prevent an oversight gap. Furthermore, the Bill does not provide safeguards for the purposes of uniform and consistent application of law, legal uniformity. The system of authorisation (Minister) and assessment (TIB or court) in advance, and review and complaints handling afterwards (CTIVD) as described in the Bill is stratified and complex. All above-mentioned players will be engaged in the same issues of law. It is important that uniform and consistent application of law is addressed in the new Act by assigning the TIB and the CTIVD the joint task of promoting legal uniformity. **(Annex I, paragraph 1)**

Interception

The interception system proposed, which is simply complex, does not yet include an adequate system of statutory safeguards. It is true that the Bill provides for considerable strengthening of authorisation and assessment of the use of bulk interception powers in advance, but the chosen system only addresses the risks to the protection of our fundamental rights involved in bulk interception to a limited extent. These risks can be limited by ensuring "responsible data reduction". The essence of this is that data should be collected in the most targeted manner possible, and that the data collected must be reduced as soon as possible to the data actually required by the AIVD and the MIVD to enable them to perform their tasks properly. Nothing more and also nothing less.

The interception system proposed, which is simply complex, does not yet include an adequate system of statutory safeguards.

Although the Bill and the explanatory memorandum thereto aim to give substance to this "responsible data reduction", the safeguards to this end are lacking or lack a clear provision in the Act. It is essential that the principle of "responsible data reduction" is substantiated further. On the one hand by including in the Act the provision that the use of powers must be "in the most targeted manner possible". On the other hand by embedding the purposiveness of data processing in concrete statutory obligations which ensure that interception and further processing are actually related to individual investigation assignments, that the storage of data is limited as a result, and that destruction of data takes place in a timely fashion, and also that all this can be reviewed effectively. **(Annex I, paragraph 2)**

Automated Data Processing

The use of automated processes involves risks. There is, for instance, the risk that - in the case of complex and large-scale data processing - it becomes increasingly less transparent or traceable for the services themselves and the oversight body which data are processed in which manner. A complicating factor in this context is that these automated processes can also fulfil important safeguard functions, such as the automated destruction of data if the retention period has lapsed or the discontinuation of collecting data if the relevant authorisation period has lapsed. In addition, automated analysis processes, such as Big Data Analysis, are used to an increasing extent. It is clearly of great importance that the services are able to guarantee that automated data processing does what it is expected to do, and that the oversight body is able to ascertain this. With the instruments provided for in the Bill, it is not possible to review these processes properly.

With the instruments provided for in the Bill, it is not possible to review automated data processing properly

The Act should therefore include a duty of care for the services in respect of automated data processing. This duty of care should extend to, among other things, the quality of data collection, of the data (files or otherwise) used, of the algorithms and models to be applied, and to the quality of the results of these processes. The services must be accountable for this (compliance). As a result, the oversight body will be able to assess effectively whether automated data processing is performed lawfully and to report on this to Parliament. In addition, it is necessary that more forms of automated data analysis are designated as investigatory powers, together with the appropriate safeguards. **(Annex I, paragraph 3)**

Review Committee on the Intelligence and Security Services

THE CTIVD'S VIEW
On the ISS Act 20.. Bill

Hacking

With regard to the power to hack via third parties, additional safeguards should be included in the Bill aimed at a limitation of the concept of 'third party' itself (there must be a direct technical relationship), at the use of this power (only when this is unavoidable), and at the (prompt) destruction of collected data that do not relate to the actual target. **(Annex I, paragraph 4)**

Cooperation with Foreign Services

The legal protection envisaged by the assessment based on the cooperation criteria requires considerable strengthening. It is, for instance, essential that the general framework for cooperation applies to all forms of data provision, and that arrangements - including adequate safeguards - are made for exceptional situations. The Act should also include additional cooperation criteria, and the transitional provision suspending the application of the cooperation criteria by two years should be deleted. It is furthermore important that the relevant Minister's responsibility for the cooperation with foreign services is clearly reflected in the authorisation of the framework for the cooperation and of cooperative activities that deviate from that framework. **(Annex I, paragraph 5)**

The legal protection in the cooperation with foreign services requires considerable strengthening

Finally

The CTIVD specifies these recommendations in **Annex I**, in which it discusses the essential safeguards that are currently lacking in the Bill. The essence of the CTIVD's considerations is set out by theme, and the CTIVD provides specific points of reference for the strengthening of safeguards and effective oversight. **Annex II** contains the proposals for quality improvements which are of a more legalistic or separate nature. In each of the annexes, the CTIVD provides suggestions for clarification or adjustment of the proposed legal provisions.