New surveillance legislation & intelligence oversight challenges: the Dutch experience

International Intelligence Oversight Forum, 11-12 October 2016

Hilde Bos-Ollermann, Secretary Dutch Review Committee on the Intelligence and Security Services

Introduction

Thank you for this opportunity to share with you some developments in The Netherlands. My name is Hilde Bos-Ollermann, I am the secretary to the Dutch Review Committee on the Intelligence and Security Services (CTIVD).

It always strikes me in conferences like this that although our legal systems and oversight structures vary in many ways, we are all faced with similar challenges. In this presentation, I will not elaborate on the details of the Dutch system. Do feel free to contact me in the break, should you have questions. What I will do, is briefly go into the plans for amending Dutch intelligence legislation and from there pinpoint some overarching issues, some of which you might also recognize in your own practice of intelligence oversight. I hope this will further stimulate our debate.

The way it is

- So to start with the way it is: the present law regarding the Dutch general and military intelligence and security services, was drafted in the nineties. Back then, administrative court cases led to the conclusion that the mandate and powers of the secret services were not foreseeable and that for individuals it was impossible to have an effective remedy against possible infringements on their rights. Although the government wasn't eager to draft a new law, parliament pressed through, which in 2002 led to the law that is still in place today.
- This intelligence and security services Act 2002 is indeed clear about what secret services can and cannot do. The special powers of the services laid down in the Act include for example various forms of interception, hacking and humint operations.
- The 2002 Act also introduced a specialized independent oversight committee, the CTIVD, with broad mandate and unrestricted access. This Committee was to review, retrospectively the legality of the activities of the secret services and to provide both parliament and the public with an understanding of a proper balance between national security and privacy.
- And this is what the CTIVD has been doing the past 14 years, intensively so, publishing over 50 in depth public reports, about topics such as humint, wiretapping and sigint operations and national and international exchange of data. The CTIVD does this on its

own accord but also in reaction to incidents and media scandals. Apart from this, the CTIVD also handles complaints.

- The Committee consists of 3 members, of which Marylène Koelewijn is present here today. I am the head of the staff bureau, today consisting of 10 investigators, advisors and administrative personnel.
- So far so good?
- Yes, but…
    - The special powers require some modernization. Untargeted powers in the 2002 Act are limited to satellite interception. In 2013, an evaluation committee concluded that the existing statutory powers were no longer sufficient and should therefore be extended.
    - This in turn calls for a reorganization of oversight, especially since oversight of the CTIVD is not binding and there is no independent body involved in the authorization process.

New surveillance legislation

- The amendment procedure took off in the Summer of 2015 with an internet consultation, allowing Dutch civil society, companies and the public in general an opportunity to react. In this draft proposal the powers of the secret services were to be extended and several working methods that had developed over the years, e.g. in the area of big data analytics, were to be codified. Oversight was to remain the same. The draft proposal led to a volume of responses that was unprecedented. There were many objections against the plan to allow the services to intercept cablebound communication in bulk. Questions were raised regarding the necessity of the new interception powers, adequate safeguards and the negative spin off for telecom providers and other commercial services. And many called for an independent ex ante binding check of the legality of interception powers.
- In the summer of 2016 a new draft proposal was sent to the Council of State for legal advice. In this new draft a number of concerns were addressed, amongst others by proposing to establish a new, independent committee consisting of former judges to authorize interception powers ex ante and binding.
- Right now, we are waiting for the ministers to send the draft bill to Parliament. They aim to do so by the end of this year.

Challenges

- In this period of time we are impressed by the increased threats and the legitimate call for effective intelligence and security services. But evaluating an old law and drafting a new one also demands of us to reflect upon a new, stable and futureproof balance between national security and privacy.
- Let's take a look at few challenges that will undoubtedly surface once the draft bill is discussed in Dutch Parliament. I will go into (1) bulk interception, (2) big data analytics, (3) international cooperation and (4) oversight.

1. How to make bulk interception privacy proof?

- As some of you might have experienced, it turns out to be very difficult to debate on the necessity of bulk communication interception. Secret services are often not willing to explain how they use these powers and why they need them. But it is evident that they have to keep pace with technology and have to be enabled to anticipate security threats. In the Netherlands, there seems to be a political majority for extending powers. Civil society, however, isn't convinced. It's worthwhile for the government to make the effort to explain WHY bulk powers are needed, if only to gain the trust the secret services will need further down the road.
- As an oversight body, de CTIVD concentrates on finding adequate safeguards for bulk interception. And there is disagreement in the Netherlands on what these safeguards should consist of. On the following issues, discussion is ahead of us.

A. Who should authorize bulk interception?
   - Should this be the minister who is to be held responsible for these activities?
   - Or should this be an independent judicial, expert or parliamentary institution?
   - ECHR caselaw shows a preference for the latter. But especially when this independent authorization is binding, this raises questions regarding the ministerial responsibility.
   - The CTIVD stresses the need for binding independent oversight, ex ante or ex post. And in any case the institution that is tasked to perform a role in the authorization of interception, has to be sufficiently specialized and staffed, to prevent it to become a rubber stamp.

B. What about dataminimalisation?
   - Do services indeed, like a dragnet, aim to collect as much bulk data as possible? Or are they looking for ways to target their interception activities? How foreseeable is this process?

- In any case, the capacity of the services to handle data will increase. To avoid the tendency to keep data "just in case", clear parameters should be set and procedures should be concrete.
- This can be done in different ways- focusing from the beginning onwards, using filters when intercepting data, assessing the relevance of data.
- And, most importantly: concrete retention periods. Lot of discussion about length retention periods; months or years? (In the Netherlands, there is no differentiation between content and meta-data, nor between data from Dutch citizens or foreigners.)
- We are all aware of the European court cases on the topic of retention. One thing is certain, if the Dutch government wants to have retention periods that are longer than intended by the European Court, it will have some explaining to do.
- Whatever the outcome of the debate, dataminimalisation in practice should not rely too much upon the good intent of the secret services and their staff. Where possible, it should be an automated process. This also enables more effective internal control and external oversight.

2. How to find suitable safeguards for big data analytics?

- One way or another, services are managing larger amounts of data. Bulk data can be acquired not only through interception or hacking operations, but also from other sources, such as government institutions or foreign partners.
- I dare say that when it regards bulk data, the real privacy infringement does not take place in the acquisition phase. It is what happens next that may seriously effect people's lives; the big data analytics through which links are established between people, profiles are applied, patterns uncovered and individuals are singled out.
- In this regard, having an independent body oversee or authorize the acquisition of bulk data is only the beginning. It's what happens next that requires safeguards. But how to protect personal data of innocent citizens in the process of big data analytics? On this aspect, the Dutch draft law fails to be future proof.
- Safeguards for big data analytics can't be achieved through traditional principles such as purpose limitation and proportionality. Data is used secondary, for another purpose than initially intended. And it is beforehand uncertain which patters will emerge, which purpose will be served, and whose rights will be infringed upon. Even the term "personal data" becomes problematic when data is continually qualified differently in the process of big data analytics and the distinction between normal data and personal data fades.

- Additional safeguards in the process of big data analytics may consist of applying a high standard of care for the quality of data, how it is stored and accessed. Also the quality of the tools for analysis, often automated processes using algorithms, should be established. These standards should be part of internal legal compliance (dataprotectionpolicy), which enables the oversight body to assess its results.

3. How to regulate international cooperation?

- For outsiders it might seem awkward, but there is no international legal framework for international cooperation between secret services.
- And also on a national level it tends to be underregulated. Cooperation criteria are often unclear and there is no independent body involved in authorizing e.g. the exchange of personal data.
- Yet possible consequences can be farreaching. Once data is exchanged, it is our of your hands. Foreign partners use your data for purposes you disagree of, e.g. illegal detention or targeting.
- The last years, secret services have intensified their international cooperation. The exchange of personal data takes place not only in bilateral contacts but increasingly also within a multilateral network, leading to databases and operational platforms. These development are essential to effectively combat international terrorism.
- But it does raise the question how one wants to regulate this. An international intelligence codex seems a bridge too far. As is international oversight. National security interests will at this juncture not allow this to be effective.
- Hence it is very important to start by setting national standards. And to allow national oversight bodies to assess this cooperation. In Dutch law and practice some steps have been taken in this regard.
- But even when this is realized, national oversight is limited, it can only investigate one part of the cooperation, it loses track once foreign services act upon data or data is used in international fora.
- For this reason, relations between national oversight bodies are very important. Not only to exchange experience and views, but also to identify cross border issues and discuss findings in similar investigations. All within the existing legal mandates.
- With a small group of oversight bodies, the CTIVD is presently experimenting with this on the theme of the exchange of data on foreign terrorist fighters. Steps are small, but it might be the most feasible approach to bridge the accountability gap of international cooperation of secret services.

4. What should be role of oversight?

- There is a large variety of possible oversight mechanisms. But we are all pondering about our expertise, our effectiveness and transparency.

A. How important is expertise?
   - To get to the bottom of the secret world of intelligence and security services an oversight body has to be granted time, resources and autonomy.
   - An oversight body should, also for the sake of independence, not rely on services to explain, but should be able to understand the intelligence practice autonomously.
   - The major challenge at this junction is technology. Like many of you, at the CTIVD we are legal scholars. The last years we have established a knowledge network experts from differ backgrounds, including the field of informationtechnology. And increasingly, we're including IT professionals in our staff.
   - And to take it one step further: wouldn't it be great to have technology be used to strengthen oversight? We aim to make part of our oversight automated, in line with my comments on big data analytics. We hope that this approach will find support in the legislative process.

B. What makes oversight effective?
   - Does it have to be binding or are there other ways to assure that the position of an oversight body is abided by? I'd like to hear your views on this.
   - Effectiveness of oversight also means that it creates awareness within the secret services of the proper balance between privacy and security, so that internal regulations are improved and privacy becomes more relevant in the daily work of the employees.

C. How transparent should an oversight body be?
   - If oversight bodies don't provide insight, journalists and whistleblowers will.
   - Oversight bodies have to be depended upon to verify, assess and explain when no one else can.
   - And transparency is possible, more than you would think at first instance.

Final remarks

Now to wrap up my presentation. The drafting of new legislation provides not only a time of reflection, it is also an opportunity for expectation management. To take away misconceptions and myths, to explain why and how special powers are used and how oversight can intervene.

This will enable a debate that is better informed and more realistic, which, I am convinced, in the end contributes to more public trust and a stronger system.

Thank you.