Research and Documentation Centre

Cahier 2023-12a

Police Hacking regulation abroad

A comparative law study into legal regulations and safeguards regarding the quality of data

Summary

Research and knowledge centre for
the Ministry of Justice and Security

Cahier 2023-12a

Police Hacking regulation abroad

A comparative law study into legal regulations and safeguards regarding the quality of data

Summary

J.J. van Berkel
A. van Uden
J.H. Goes

Cahier
This series comprises overviews of studies carried out by or for the WODC Research and Documentation Centre. Inclusion in the series does not mean that the sheet's contents reflect the viewpoint of the Minister of Justice.

Summary

The Dutch Computer Crime Act III (CCIII) came into effect on 1 March 2019. Among other things, this Act introduces the power of the police to carry out hacking operations. The new Sections 126nba, 126uba, 126zpa in the Code of Criminal Procedure will allow specially authorised investigating officers to covertly and remotely intrude into computer systems under certain conditions and investigate them. The police can carry out investigative actions using technical tools. In principle, a technical device must be inspected and approved by an independent inspection service (*de Keuringsdienst*) prior to its use, in order to guarantee the reliability, traceability and integrity of the evidence.

The Justice & Security Inspectorate (hereinafter Inspectorate) supervises the implementation of the hacking power. In its first Report in 2020, it concluded that the use of technical tools for hacking powers and the inspection of these tools were not yet proceeding as intended under the legal framework. In his response to the first Inspectorate Report, the then Minister of Justice and Security indicated that he would have an investigation into the safeguards of technical tools used by foreign police authorities. The present report is the result of this research. This report also supplements the previously published evaluation of the use of the hacking power in the Netherlands, carried out by the WODC.

Research question

The central research question for this study is as follows:

What safeguards govern hacking powers abroad, more specifically the use of technical tools, and how does this compare with the Dutch situation?

The central research question is answered on the basis of the following subquestions:

1 What countries allow 'authorised hacking' and on the basis of which legal ground can foreign police services carry out hacking operations in their own country?
2 What statutory conditions apply in other countries for police services to deploy the hacking power?
3 To what extent do other countries test technical tools and what has been laid down in legislation and regulations on this?
4 To what extent are there any other rules to ensure the reliability, traceability and integrity of data obtained with the use of technical tools?
5 How does the working method abroad compare with the Dutch working method regarding the approval of technical tools and any other safeguards to achieve data reliability, integrity and traceability?

Methods of research

We first made a broad inventory to map out which countries have legal hacking powers. To be able to speak of a hacking power, we assumed that the hacking power is carried out secretly and remotely. As part of the broad inventory, virtually all European countries were examined, with the addition of the United States, Canada and

Australia. Based on the broad inventory, a selection was made of five countries that were studied in more detail: Belgium, Germany, France, Sweden and Switzerland. Various research methods were used to answer the research questions: document study (laws and regulations and relevant (grey) literature), written questionnaires and interviews.

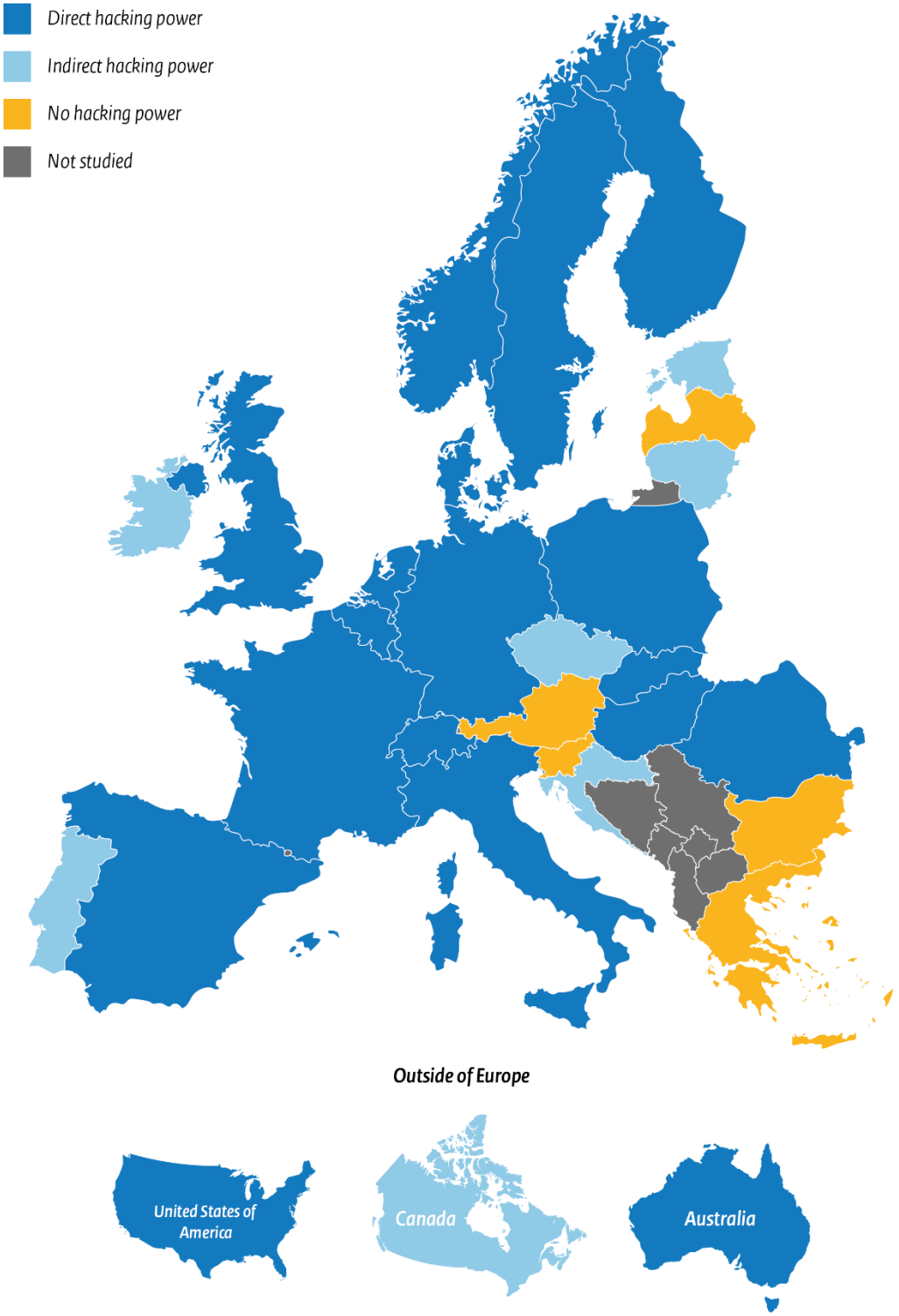
Broad inventory

Based on the broad inventory, a number of topics are discussed in this report. In this summary, attention is paid to the presence of a hacking power, the inspection of technical resources and the presence of an inspection body, the guarantees for documentation, storage and judicial supervision, and the notification obligation and the right of inspection.

Presence of hacking power

The figure on the next page features a map of all the countries included in this study. The figure indicates whether a country has set up a statutory power of the police to carry out hacking operations, and if so, whether this is a direct or indirect power. A direct power applies if the law explicitly refers to the possibility of covertly and remotely intruding into a computer system and undertaking one or more investigative actions within that system. An indirect power applies if the hacking power forms part of a general provision. Consider, for example, the power to intercept telecommunications, whereby the law text does not specifically mention the hacking power, though the power could be used for that purpose.

Country overview – hacking power



The maps are adaptations of works by Maix (Europe; CC BY-SA 3.0), Theshibboleth/Lokal_Profil (VS; CC BY-SA 2.5), Paul Robinson/Lokal_Profil (Canada; public domain) and Rycherr (Australia; CC BY-SA 4.0 and previous versions).

Inspection of technical tools and supervisory body

None of the countries has established an inspection by an independent inspection body in charge of testing the technical tools before they are deployed based on a comprehensive inspection protocol. Some countries do have a testing procedure, however, these procedures are not performed by an independent inspection body. Furthermore, for those other countries that do have an inspection or testing procedure, it is unknown what the procedure consists of. Germany constitutes an exception in this regard. Even in that country, it is not entirely clear what the inspection entails, but it is clear that it is based on an SLB guideline specifically designed for it. See Section 4.8.

In other countries, the supervision of hacking operations by an independent body is limited, thereby not including the trial court. Australia, Denmark, Norway, the UK and Sweden have independent bodies performing some level of supervision of the execution of the hacking power. Owing to its technical expertise, Germany has an authority that advises on the deployment and development of technical tools. France has a specific authority responsible for the design, supervision and implementation of technical tools used for hacking operations.

Safeguards regarding documentation, storage and judicial supervision

Almost all countries require some sort of documentation with regard to documenting and logging operative actions. As a minimum, they require an official report documenting all actions. Some countries take it a step further and require the logging of all actions. During our research, it remained unclear to what extent five countries have requirements to document and register operative actions.

There is judicial supervision in Belgium, France, Croatia, Portugal and Spain *during* the deployment of the hacking power. This means the police must provide interim updates on progress to the judge who issued the order. In some cases, the judge may withdraw the authorisation for the hacking operations based on those status updates. As far as we know, there is no interim judicial review in the remaining countries.

Twenty countries have included safeguards in their laws regarding the storage of data collected with the use of hacking powers. These safeguards include the sealed storage of data or the storage of data in a secure environment. In the case of the remaining countries, nothing is included in the law or it has not become clear to us whether countries have set formal or informal safeguards.

Trial and right to inspection

Thirteen countries have included a notification obligation in the law. This means that those persons whose computer system was hacked must be informed within a predefined term that this hacking power had been deployed. In half of these countries, notification can be deferred or sometimes even omitted if the interests of the investigation may be compromised. In nearly all countries, the suspect will be notified if the case is brought before the court. Seventeen countries have explicitly included the right to inspect obtained data in legislation. In many cases, the defence may receive a copy of the data obtained. Among the remaining countries, our inventory did

not show whether this hacking power is covered by a specific legal provision regarding the right to inspection.

In-depth country comparison

A number of countries have been studied in more depth. These countries have been compared with each other and with the Netherlands. Therefore we first describe the most important bottlenecks in the Netherlands. Then follows the country comparison.

Main issues and bottlenecks in testing technical tools in the Netherlands

For the introduction of the hacking power, the Dutch legislator opted to follow the inspection system of technical tools already set in place for existing (special) investigative powers. A separate decision was prepared for the authorised hacking titled 'the Decision on intruding into automated information systems (hacking)', hereinafter: the Decision. The Decision sets a number of requirements for technical tools, including requirements aimed at integrity, traceability and reliability of the data collected, hereinafter: quality. The Dutch National Commodity Inspectorate is tasked with testing the tools in the Netherlands, thereby applying an inspection protocol based on various articles from the Decision. In principle, the police must make use of technical tools that have been tested and approved prior to their use. This is subject to a number of exceptions: 1) a technical tool may be tested afterwards, 2) it is possible to switch to manual deployment or 3) the public prosecutor decides that the tool cannot be tested 'on account of its nature'.

The Reports from the Inspectorate of Justice and Security and the first evaluation report from the Research and Documentation Centre show that the testing and the use of technical tools do not always proceed as intended by law. Pre-approved technical tools are hardly ever deployed, and inspection is a major bottleneck for investigation practices. Different aspects play a role here:

- The turnaround time of an inspection takes a relatively long time, at least four months.[1] That timeframe does not always match the promptness that may be required within an investigation.
- Adjusting a technical tool that has not been approved always requires a new inspection and thus takes time.
- The Decision demands, and consequently so does the Dutch National Commodity Inspectorate, that technical tools must meet all requirements for the technical tool to be approved. Investigation practices, however, question the usefulness and necessity of all requirements and the compliance thereof.
- The deployment of technical tools takes place in an environment which Digit, the police team executing the power, cannot always control. For example, Digit cannot exercise any influence over what suspects do with their computer systems. Any action from the owner of the computer system can affect the quality of the data collected. Digit would prefer to focus more on making risk analyses with regard to the technical tool used and the evidential value of the data collected.
- A risk analysis focuses on the risk of data quality being compromised if a technical tool is used that does not meet all requirements.

[1] This time frame relates to the development of an (approved) technical tool. Several inspections usually take place during this time frame.

- Another consideration is the impact of using a technical tool that does not meet all requirements on the evidential value of the data collected. Especially, if the data only form part of the evidence collected.

The majority of police investigations in which hacking operations are carried out make use of a commercial product. Here, too, no pre-approved tools were used. In fact, the products were never submitted for testing, because the Digit public prosecutor decided that the nature of the tools preclude inspection. In so doing, the public prosecutor makes use of the Decision's ground for exception. Incidentally, these products can indeed not be approved under the current inspection regime. There are a number of factors that make a commercial tool inherently impossible to approve and/or never to be approved:

- Commercial tools are updated relatively often. The question then becomes, which version or versions should the Dutch National Commodity Inspectorate approve? If all the versions need to be approved, it would exceed the usual lead time needed for testing and approval in relation to the timeframe within which the police action must take place.
- Operation of these types of tools is a 'black box' for the users, which is why the Dutch National Commodity Inspectorate is not given access to the exact operation and can therefore not carry out a full inspection.
- Suppliers want to have access to their product at all times, to do things like perform maintenance, for example. As a result, the Dutch National Commodity Inspectorate is not given exclusive access to the tool, which it requires for its inspection. Not having exclusive access means no approval, as it cannot be ruled out that a party other than the suspect and the police had access to the data collected. This means that the reliability and integrity of the data cannot be fully guaranteed.

Failing to perform the inspection means that a majority of criminal investigations do not comply with a key safeguard with regard to the quality of the data collected. It should be noted, however, that additional technical and tactical safeguards are put in place in this situation to ensure the reliability of the evidence. These tactical safeguards are not included in the testing.

Comparison between countries

In our study, five countries have been studied in more depth: Belgium, Germany, France, Sweden and Switzerland. To compare the countries, a distinction has been made between three phases with regard to the safeguards during the deployment of the hacking power: the phase prior to deployment, during deployment and after deployment of the hacking power.

Safeguards prior to the deployment of the power

Except for Sweden, all countries have some form of inspection or testing of the technical tool to be used. However, the manner differs per country. The Netherlands has the most detailed described inspection of technical tools. The manner in which Germany has described the criteria appears closest to the way the Netherlands has done this. The German inspection is based on the SLB Guideline , which highlights the following themes: protection targets and security measures, work processes and procedures, suppliers, and test policy. Application of the guideline serves as a guiding principle; it is not a legal requirement. A risk analysis is used to identify which objects,

e.g. system components such as hardware and software, applications, organisational or personnel issues, pose a risk for these themes. The results of this risk analysis, the determination of the protection needs and the resulting consequences and implementation thereof are laid down in an IT security concept. Both software suppliers and users of the software must conform to this concept. It is not known what criteria comprise the inspections in the other countries.

The Dutch National Commodity Inspectorate carries out the inspection in the Netherlands. The Dutch National Commodity Inspectorate is an independent body, though it formally falls under the same organisational unit of the National Police Board to which the team carrying out the hacking operation belongs. In France, the testing is done by a specific government body called STNCJ. This government body is also responsible for the execution of the hacking power. In both countries, the way in which the tasks are assigned may raise the question of how independent the inspection is. This applies in particular to France, where it is actually the same organization that carries out the power and inspects the tools. The other countries have the police doing their own testing. It is interesting to note that both in France and Switzerland, the 'inspector' and the 'performing party' are one and the same party. These countries do not consider this to be problematic and proceed on the assumption that the parties act in a fundamentally trustworthy manner. As far as known, there is no formal inspection in Sweden. However, they often use standardised software at a later stage of the hacking process, i.e. once the data are placed on the police's systems. This standardised software, for example, involves software that has been certified by other police services such as the Dutch police.

Safeguards during the deployment of the hacking power

The safeguards that must be in place during deployment of the hacking power differ per country. Common safeguards at this stage are forms of logging, reporting, the use of a secured transport of data from the computer system and the storage of data in a secured environment.

There is judicial review in Belgium and France during the hacking operations. The judge granting authorisation for the deployment of the hacking power also supervises the execution thereof. If the execution of the hacking power does not take place in accordance with the conditions of the authorisation, the hacking operations may be terminated. It should be noted in this respect that the judge relies on the information that the police or the public prosecutor provides or may provide during the deployment. The question is thus whether this judicial oversight will actually ensure that a deployment can be terminated mid-term. The judicial oversight in these countries goes beyond the role of the Examining Magistrate in the Netherlands, who principally only oversees the hacking power prior to a deployment or its extension. However, the Netherlands still has the supervision by the Inspectorate of Justice and Security.

Safeguards after the deployment of the hacking power

The most common safeguards pertain to the notification of the deployment of the hacking power to the suspects or the data subjects, the substance of the case at the hearing and the suspect's right to inspection. Notification is not a guarantee in all countries, given that such notification may be omitted if it could compromise ongoing interests of the investigation. The law in Belgium always requires notification. France is

the only country in which a suspect does not need to be notified. It goes without saying that if the data hacked form part of the evidence, the suspect is indirectly notified by the inspection of the file. Not all countries have made it clear what information is included in the file, and to what extent the right to inspection extends. However, it does emerge that in most cases the defence receives a copy of the data collected by means of hacking operations or a collection thereof.

Based on information conveyed in interviews there is still little case law available that calls into question the quality of the data collected by means of hacking operations. This makes it difficult to answer the question of how extensively a session judge assesses the deployment and the data quality. The case law that is available mostly deals with cases where evidence is used based on data from the Encrochat communications service. The French authorities have been able to intercept these communications. Many countries have used Encrochat data as evidence. However, the main issue in these cases was whether this was legally obtained evidence rather than the quality of the data collected. As far as known, the quality of data has only been called into question in Sweden and France. In Sweden, the court dismissed relatively easily the objections raised regarding data quality. The court added that the data, in conjunction with other investigation data, show that 'the messages correspond well to the reality in terms of time and content'. More striking is an October 2022 ruling from France. In this ruling, the court concluded that in the absence of a certificate of truthfulness, it cannot be accepted that nothing is shared about how the evidence was obtained. However, this only applies if the collected data is encrypted. It is likely that the police use the authority to view decrypted messages (live). Therefore, in these cases a certificate is not required.

Another striking issue in terms of the safeguards at the end of deployment is the legal provision applicable in Switzerland that stipulates that it must be made possible to check the source code of the technical tool if so requested by the court. Prior to deployment, it must also be ensured that the supplier cannot access the data. Source code disclosure and access restriction stand out because both issues are a major obstacle in the Netherlands to testing and approving commercial tools. A relevant question, which unfortunately cannot be answered based on our research, is thus to what extent both requirements can ultimately be enforced in Switzerland.

Finally, it is worth noting that Sweden is the only one of five countries that has a specific supervisory body (SIN) that monitors the hacking power. SIN's role in relation to the use of technical tools for the hacking power is still evolving. For the time being, supervision is focused particularly on legal and process-related aspects of the power, such as the lawfulness. However, SIN also has the authority to check the technical tools themselves. While SIN's rulings are not binding, authorities generally follow SIN's rulings. SIN has partly similar tasks to the Inspectorate in the Netherlands, but it additionally oversees the lawfulness of the entire process and thus also the activities of both the police and the public prosecutor. SIN can furthermore issue public statements in individual cases. The suspect may also personally request this.

Scenario's

Based on our research, we have formulated three scenarios which could potentially complement the way in which the Netherlands deals with technical tools and data

collected by means of the hacking power. These scenarios are described in the text below.

Scenario 1: Source code and monitoring data access

Our research shows that it is required by law in Switzerland that it must be made possible to check the source code of the technical tool if so requested by the court. It must also be ensured that suppliers cannot access the data when these are being collected. These issues specifically form an obstacle in the Netherlands in inspecting commercially technical tools. It has not become clear to what extent the Swiss authorities have actually been able to fulfil both requirements. As far as is known, there has not yet been a case in which the source code was actually requested. In principle, suppliers do not benefit from giving access to their source codes. The software's working method is a well-kept secret. However, if Switzerland has succeeded in finding a workable solution, it is worth considering whether the police, public prosecutors and policymakers in the Netherlands can also achieve this in a similar manner. This could resolve two major bottlenecks in the testing procedure in the Netherlands.

Scenario 2: Changing supervisory role

During the Dutch legislative process, supervision during the exercise of the power has been an important point of discussion. Extra supervision would be necessary because judges would not always be able to properly assess the evidence collected. It was also expected that a (large) portion of the cases would never be trialled by a court. It has been suggested to set up a body comparable to the Supervisory Committee of the Intelligence and Security Services (CTIVD). Over the years, various authors have pointed to the importance of (additional) supervision or a different form of supervision. In the end, the legislator did not opt for a committee comparable to the CTIVD. Arguments for this were the existing supervision by an examining magistrate and supervision by the Central Review Committee of the Public Prosecution Service. Instead, the Justice and Security Inspectorate has been chosen, which supervises cases that are and are not submitted to the court.

Based on our research, we do not take a position on this discussion. However, it is worth noting that if the role of oversight for hacking power is explored further, there are a number of countries that have surfaced from the study that may provide guidance.

Firstly, it is relevant in this context that Belgium and France have examining magistrates overseeing the execution of the hacking power. The Examining Magistrate granting authorisation for the deployment of the hacking power also supervises the execution thereof. If needed, the Examining Magistrate may decide to terminate the hacking operations. This oversight goes beyond the role of the Examining Magistrate in the Netherlands, who principally only oversees the hacking power prior to deployment. The working method in Belgium and France solves the problem that part of the cases are not presented to court. As a side note, it should be noted that the examining magistrates rely on the information provided. The question is thus whether this judicial oversight actually results in a substantive review during deployment. It does however offer a perspective that deviates from the Dutch system in which the Examining Magistrate grants an authorisation prior to the deployment and thereafter generally no longer oversees the hacking operations.

Secondly, also relevant is the Swedish supervisor SIN. This supervisor specifically oversees the execution of the hacking power. It is therefore similar to the Committee modelled on the CTIVD as proposed by some authors. As yet, SIN's supervision is focused particularly on legal and process-related aspects of the power, such as the lawfulness and it oversees both the police activities as well as those of the Public Prosecution Service. As such, it distinguishes itself from the tasks of the Inspectorate in the Netherlands, which only oversees the police. SIN can furthermore issue public statements in individual cases upon request or on its own accord. Given that SIN focuses both on the legal and process-related aspects, this solves the issues raised earlier that not all cases are heard by a session judge and that the judge is not always sufficiently capable of properly assessing the evidence.

Scenario 3: Customised inspection

As previously discussed, the testing in the Netherlands constitutes an important safeguard in the deployment of technical tools and the quality of the data collected by means of the tools. Practice shows that the testing and the use of technical tools do not always proceed as intended by law. Technical tools that are mainly used are tools that are not pre-approved and technical tools that cannot be approved due to their nature. Notably, the safeguards relating to technical tools and the data quality are less detailed by law abroad than in the Netherlands. In that respect, it is easier to deploy the hacking power abroad. Another striking aspect is that there is little or no case law available that challenges the use of the hacking power in these countries. This incidentally does not mean that the evidence provided by the hacking power will always be readily accepted. In many countries, the hacking power is relatively new and its use and any opinions thereof will continue to develop. Therefore, it cannot be ruled out that future rulings may still ensue that will impact the current legal framework in these countries. This does not detract from the interesting fact that several countries have chosen not to check data quality in a way that is done in the Netherlands. And that the working method in those countries has, as yet, not resulted in any fundamental discussions in the courts. It is for this reason that we have included a third scenario which takes a more tailor-made approach to the inspection requirements, with attention to additional tactical and technical safeguards. This scenario explores a) the use of a risk analysis for the inspection and b) the question to what extent additional tactical and technical measures are adequately safeguarded.

Scenario 3a: Risk analysis in the inspection phase

Risk analyses form part of the decision to purchase and use technical tools in Germany. An SLB guideline addresses various themes that should be taken into consideration when it involves technical tools, such as the testing policy. A risk analysis identifies which objects pose a risk for these themes and what additional measures are needed. The different parties involved must conform to this. In the Netherlands, the performing party Digit indicates that the Dutch National Commodity Inspectorate, as well as the underlying inspection protocol, does not take sufficient account of the fact that it could also operate on the basis of a risk analysis, namely in terms of the measures it takes when deploying a technical tool. It is particularly this risk analysis that appears to have taken centre stage in Germany. Therefore, the working method in Germany could be further explored to see what lessons can be learned from it in terms of the Dutch situation.

Scenario 3b: Assurance of additional tactical safeguards in the Netherlands

As noted, the Netherlands currently mainly uses technical tools that, according to the Public Prosecutor, cannot be approved due to their nature. Tactical and technical measures are taken to safeguard the data quality in this situation. There are no indications at present that the use of commercial products will be terminated. The current Minister considers this to be a 'reality that we have to deal with', as evidenced by the committee debate on 7 July 2022. The use of risk analyses described in scenario 3a may serve as a guideline to take appropriate additional measures to ensure data quality. If the working method with commercial products remains the rule rather than the exception and the method will be continued by exactly the same token, it will also be important to review the role of the Public Prosecution Service with regard to the additional safeguards, tactical or otherwise. At present, the Public Prosecution Service is the only one checking these safeguards prior to a deployment. A tactical public prosecutor leading the criminal investigation is in principle ultimately responsible for the tactical safeguards. These are also reviewed by the Digit public prosecutor and the Central Assessment Committee of the Public Prosecution Service. Owing to the sole involvement of the Public Prosecution Service and no other independent bodies, it is useful to explore which other party can (additionally) verify the adequacy of these measures, especially when a case is not presented to court.

The WODC (Research and Documentation Centre) is the knowledge centre in the field of the Dutch Ministry of Justice and Security. The WODC carries out independent scientific research for policy and implementation purposes; it does so both by itself, and on the WODC's commission.

More information:

www.wodc.nl