dialogic

Onderzoek voor *onderbouwd* beleid.

De strafzaak

Strafrechtelijk onderzoek en onderwijs

Summary

Evaluation Criminal Procedure Innovation Act

Pilots Data after Seizure (GNB), Audiovisual Registration (AVR), Assistant Public Prosecutor (hOvJ)

Authors

mr. dr. Bas de Wilde

Max Boiten MSc

Melvin Hanswijk LLM MSc

Sophia Stone MSc

ir. Tommy van der Vorst

Summary

Evaluation Criminal Procedure Innovation Act

Pilots Data after Seizure (GNB), Audiovisual Registration (AVR), Assistant Public Prosecutor (hOvJ)

Authors

mr. dr. Bas de Wilde
Max Boiten MSc
Melvin Hanswijk LLM MSc
Sophia Stone MSc
Ir. Tommy van der Vorst

Commissioned by:

Wetenschappelijk Onderzoek- en Datacentrum (WODC)

Publication number:

2023.099-2435

Date:

9th of September 2024

Image cover:

iStock, Jacob Wackerhausen (licenced)

Table of Contents

List of Abbreviations

	Dutch	English
amvb	algemene maatregel van bestuur	general administrative order
AVR	audiovisuele registratie (in dit onderzoek: alle registraties van beeld en/of geluid)	audiovisual recording (in this study: all recordings of images and/or sound)
BOD	bijzondere opsporingsdienst	special investigative service
BT	Basisteam (politie)	Basic Team (police)
DR	Districtsrecherche (politie)	District Investigation Service (police)
DRR	Dienst Regionale Recherche (politie)	Regional Investigation Service (police)
FIOD	Fiscale inlichtingen- en opsporingsdienst	Fiscal Information and Investigation Service
GDAS	Generieke Dienst Automatische Spraakverwerking	Generic Service for Automatic Speech Processing
GNB	Gegevens na Beslag (aanduiding pilotproject)	Data after Seizure (project designation)
ILT-IOD	Inlichtingen- en opsporingsdienst van de Inspectie Leefomgeving en Transport	Human Environment and Transport Inspectorate's Intelligence and Investigation Service
KMar	Koninklijke Marechaussee	Royal Marechaussee
MvT	memorie van toelichting	explanatory memorandum
NLA-IOD	Inlichtingen- en opsporingsdienst van de	Intelligence and Investigation Service of the Dutch Labour Authority
NVWA	Nederlandse Arbeidsinspectie Nederlandse Voedsel- en Warenautoriteit	Netherlands Food and Consumer Product Safety Authority
OvJ	officier van justitie	public prosecutor
pv	proces-verbaal	police report
RC	rechter-commissaris	examining judge
Sv	Wetboek van Strafvordering	Code of Criminal Procedure
WODC	Wetenschappelijk Onderzoek- en Datacentrum	Scientific Research and Documentation Centre

1 Introduction

On the 1st of October 2022, the Criminal Procedure Innovation Act (in Dutch: Innovatiewet Strafvordering) came into effect. This law, which introduced Articles 556-570 of the Code of Criminal Procedure (in Dutch: Wetboek van Strafvordering, or Sv), aims to allow for the acquisition of experience with powers and methods that are intended to be regulated in the new Criminal Procedure Code. The Criminal Procedure Innovation Act has led to five pilot projects, which have been evaluated on behalf of the WODC (Scientific Research and Documentation Centre). This report presents the results of the study on three of the pilot projects, namely the Data after Seizure (in Dutch: Gegevens na beslaglegging, or GNB), Audiovisual Recording (in Dutch: audiovisuele registratie, or AVR), and Assistant Public Prosecutor (in Dutch: hulpofficier van justitie, or hOvJ) pilots. In total, eight sub-pilots can be distinguished within these pilots.

Regarding the three pilot projects being studied, the following research questions have been answered:

1. What is the content of current law, the law based on the Innovation in Criminal Procedure Act, and the proposed Code of Criminal Procedure concerning the pilots under examination?
2. What were the objectives behind the creation of the legal framework within which the pilot takes place? What were the objectives of the pilot itself?
3. In what way(s) has the pilot been implemented? To what extent have the conditions for implementing the pilot as described in the evaluation framework been met? What adjustments have been made during the pilot?
4. How do the involved parties evaluate the implementation process of the pilot, including the collaboration between organizations? What goes well and what can still be improved?
5. What results and effects have been observed during the implementation of the pilot concerning the evaluation indicators formulated for each pilot project, and how do these relate to the methods followed before the start of the pilot?
6. Does the pilot's method, based on its implementation, achieved results, and observed effects, result in an improvement of criminal procedure?
7. Is it advisable to adjust the method of the pilot?
8. Is it recommended to apply the legal framework to cases other than those covered by the pilot projects, and if so, under what conditions and with what implementation consequences?
9. Is it advisable to supplement or adjust the equivalents of the provisions from the Criminal Procedure Innovation Act in the draft Code of Criminal Procedure?
10. Is supplementary policy necessary or desirable if the method of the pilot continues?
11. Based on the findings from the pilot, what can be said about the expected—both structural and incidental—financial implementation consequences that would result from the possible introduction of the legal framework?

Many partners within the criminal justice chain are involved in the pilot projects: the police, the Public Prosecution Service (in Dutch: Openbaar Ministerie, or OM), the Judiciary, the Royal Marechaussee (in Dutch: Koninklijke Marechaussee, or KMar), the Rijksrecherche, and the special investigative services FIOD (Fiscal Information and Investigation Service), ILT-IOD (Human Environment and Transport Inspectorate's Intelligence and Investigation Service), NLA-IOD (Dutch Labour Authority's Intelligence and Investigation Service), and NVWA

(Netherlands Food and Consumer Product Safety Authority). The involvement of different organisations varied considerably per (sub)pilot. In each pilot, the application of powers and methods was registered to a greater or lesser extent. The registered data were analysed. Various types of documents were also included in the study, such as reports from intervision sessions. Interviews were conducted with employees from all the aforementioned partners within the criminal justice chain. Lawyers were also questioned. In the hOvJ pilot, an assessment of the hOvJ's requisitions to provide data was conducted, aimed at examining the quality of the issued requisitions.

2 Pilot Data after Seizure (GNB)

2.1 Articles 556 en 557 Sv

Content of the pilot

Article 556 of the Code of Criminal Procedure (Sv) grants the authority to view and record data stored on a device (such as a smartphone or laptop) after its seizure. Article 557 Sv states that after seizure, it is permissible to investigate data stored on an automated work located elsewhere (often in the cloud). This is referred to as a network search. For both authorities, the investigative officer is only empowered when a public prosecutor (OvJ) has issued an order, following the issuance of authorization by an examining judge (RC). Only data present on the seized device or the investigated network within a timeframe specified in the order, counting from the moment of seizure, may be examined. The initial period is 3 days. If the urgency of the investigation requires it, this period can be extended incrementally up to a maximum of 6 months. Before the Criminal Procedure Innovation Act came into force, there was no specific legal basis for these authorities. Occasionally, a public prosecutor would request an examining judge to carry out investigative actions, after which the examining judge would instruct an investigative officer to conduct the requested investigation.

Number of applications

The extent of the use of the pilot authorities varies slightly by period but has remained fairly stable. For the application of Article 556 Sv, approximately 16-18 orders per month were issued, and for the use of Article 557 Sv, approximately 24-29 orders per month were carried out. There are significant differences among chain partners. By far, the majority of applications were made by the police, followed by the FIOD and the Rijksrecherche. The powers were seldom used by the Royal Marechaussee (KMar), ILT-IOD, and NVWA. Respondents indicated that they had expected the authorities to be deployed on a larger scale. Reasons cited for why this was not the case include unfamiliarity with the authorities, alternative means to obtain the relevant data, and the absence of a seized device in an investigation.

Methodology

When an automated device is seized, measures are taken to prevent data on the device from being erased. For instance, many devices are put into airplane mode before being seized. To facilitate the investigation of historical data stored on the device, a copy of the device, referred to as an *image*, is made. The investigation of the data then occurs based on this copy.

When Article 556 Sv is applied, it can be determined in various ways which data was stored on the device after the seizure. Typically, at the end of the period specified in the order, a second *image* is made after restoring the network connection. The two *images* are then compared to identify which data was added after the seizure. In cases where there is an urgent need to access certain data, such as when co-suspects of a robbery – with whom an arrested suspect is in contact via a chat group – are on the run, the data may sometimes be viewed directly on the seized device itself.

A network search based on Article 557 Sv sometimes follows a network search based on Article 125j Sv, which is conducted at the location where a device is currently situated. It may be desirable, partly due to the impact on the privacy of the individuals involved, to continue the network search at the office of the respective investigative service. To do this, it is necessary to seize the device. However, practically speaking, the availability of the

device is not always required to perform a network search under Article 557 Sv, as access to a network application can sometimes be obtained using login credentials. For carrying out the actual network search, the seized device is generally not used. Instead, a forensic device equipped with specialized software is used to record data.

To gain access to a network application, certain actions may need to be performed, and it was unclear at the start of the pilot whether these actions were permissible. First, logging in sometimes requires changing the password, which has generally been deemed permissible. Second, many applications are secured with two-factor authentication, which sometimes generates a code sent to a smartphone. During the pilot, it was assumed that this code could only be accessed if an order had been issued under Article 556 Sv.

Results, effects, and appreciation

The study reveals that it is sufficiently clear which authority applies in which situation. It is possible to determine whether data is on the seized device or on a server elsewhere, and it is also possible to establish whether data has been stored on a device after the seizure. One point of attention is the consultation of data on a seized device. Data that is visible is not always stored on the device itself. For example, the text of chat messages is often on the device itself, but photos accompanying chats are increasingly stored in the cloud. When a smartphone is examined shortly after the seizure, both the data on the device and the data in the cloud are often viewed, some of which may have been stored after the moment of seizure.

Because three different authorities are involved here – Articles 556 and 557 Sv, as well as the authority to conduct an investigation into data on the device – three different orders are required, with two orders only being issued after authorization by the examining judge (RC). This is not efficient. The decision-making process generally appears to work efficiently. Compared to the situation outside the pilot, where the public prosecutor (OvJ) makes a request to the RC under Article 181 Sv, the pilot procedure is significantly more efficient. Because the authorities are legally standardised, it is clear how the application should be structured and assessed.

According to the police's Plan of Action, only trained investigative officers should submit applications to use the authorities, and the application should be reviewed by a TDO-er (digital specialist). It was found that untrained investigative officers also submitted applications. In some units, applications were not processed by the Interception Desk if advice from a TDO-er was not provided, but in other units, the lack of advice did not pose an obstacle. The application is assessed by a public prosecutor (OvJ), who requests authorization from the examining judge (RC). Several TDO-ers indicated that OvJs and RCs do not always have sufficient knowledge of the authorities to make correct decisions. There was one instance where an RC initially did not grant authorization but did so after further explanation. According to these respondents, RCs do not always have sufficient understanding of the impact of using the authorities. The RC we spoke to did not recognize this depiction. This RC mentioned that in cases of uncertainty, he would ask the OvJ further questions or contact a specialized cyber RC.

The authorities under Articles 556 and 557 Sv fulfill a need and in about 40% of the cases that we have reviewed, they produce data relevant to the investigation. Sometimes the authorities cannot be used despite the desire to do so. Reasons for this include the inability to seize a device, the absence of the sought-after data on the device (or the device being completely wiped remotely), or technical obstacles to recording the data.

According to respondents from investigative services, the 3-day period from the moment of seizure is rarely sufficient to exercise one of the pilot authorities. They attribute this to the decision-making process often taking a minimum of 3 days. However, the registration records show that orders often are not extended after 3 days. In theory, a stricter criterion applies to orders issued after the initial 3-day period, which must be urgently necessary for the investigation. However, it is unclear how to distinguish a regular investigative interest from an urgent investigative interest. The period can be extended up to a maximum of 6 months, and in most cases, this period is sufficient. However, there have been instances where device security could only be breached after 8 months. In that case, data from the last 2 months could not be recorded. This is seen as problematic because those data could also be relevant to the investigation. Technically, it is not possible to record only data from a specific period.

The application of the pilot authorities generally places a high value on subsidiarity and proportionality. When relevant data can be obtained in a less intrusive manner, such as by requisitioning data, that option is sometimes chosen. The public prosecutor's order is delineated by specifying the particular applications that may be investigated, such as certain email boxes, chat programs, and social media accounts. However, in cases of verbal orders and verbal authorizations, there is sometimes scarcely any delineation, which is seen as a point of contention.

Compared to network searches under Article 125j Sv, network searches under Article 557 Sv typically infringe less on privacy rights and business interests because investigators do not need to remain in a home or business for an extended period. Under Article 557 Sv, only data that is reasonably necessary to uncover the truth may be recorded. However, technically, it is not possible to select only the relevant data. Therefore, a large amount of data that is not relevant to the investigation is recorded. The relevant data is then selected from the recorded data, often with the help of software, and the remaining data is documented in a residual investigative report.

The application of the pilot authorities necessarily takes some time, as an application must be prepared and reviewed by at least the prosecutor and an examining judge. However, this does not appear to affect the overall duration of the investigation. In urgent cases, verbal orders and verbal authorizations can be issued.

Since investigative officers, the prosecutor, and the examining judge are involved in the application of the authorities, their workload increases, which is accompanied by labor costs. The necessary training and desired intervision also incur costs. Additionally, material costs can be expected due to the need to purchase hardware, storage capacity, and software licenses. The financial implementation consequences of introducing the pilot authorities cannot be specified, as they depend on many variables, including differences among the investigative services in available resources and the choices made regarding, among other things, software packages.

Improvement in Criminal Procedure?

The introduction of the pilot authorities results in an improvement in criminal procedure. The legal regulation of investigative authorities in the current Code of Criminal Procedure lags behind the digital world in which crimes are committed. The proposed legal regulation meets such a significant need that it is necessary to continue applying the pilot authorities even after the pilot ends. Since the Criminal Procedure Innovation Act (Innovatiewet

Strafvordering) expires on October 1, 2025, a legal provision will need to be established to enable their application beyond that time.

Recommendations for adjusting and supplementing the draft legislation

- With respect to the investigation of data on seized devices, the Explanatory Memorandum (in Dutch: Memorie van Toelichting, or MvT) for the draft legislation makes a threefold distinction in investigations: investigations that make a limited infringement on privacy rights, systematic investigations, and major systematic investigations. Every systematic investigation requires an order from the public prosecutor (OvJ), while a major systematic investigation also requires authorization from the examining judge (RC). The mere fact that data is stored on a device after its seizure does not significantly increase the infringement on privacy. Therefore, we recommend not creating a separate authority for investigating data stored on the device after seizure. When the authority to investigate data on a device exists, it should encompass the investigation of newly stored data. Should this recommendation not be adopted, two recommendations are made to improve the proposed Article 2.7.39: removing the condition of seizure for the applicability of the authority and modifying the description of the data to which the authority applies, clarifying that it does not concern data generated by the device itself. Furthermore, we deem it desirable that devices can be seized solely for the purpose of accessing newly received communication data, provided that appropriate limitations are observed.
- Regarding network searches, it is recommended to distinguish between active and passive searches. In a passive network search, only data visible on an opened automated device is accessed without the need for active intervention by the investigator, such as logging into an application or actively causing the device to synchronize. This includes, for example, viewing a photo in the cloud on a device. In all other cases, it is an active network search. The standard network search using a forensic laptop to record data is an active network search.
- It is advisable for the investigation of data (often requiring an prosecutor order) to cover the passive network search. It is somewhat coincidental whether data is on the device being investigated or on a server elsewhere. If the user had used a different application, the location of the data might have been different. The infringement on privacy is not greater when the data in question is actually stored in the cloud.
- For active network searches, the proposed Article 2.7.40 distinguishes between two forms: the network search conducted during the physical search of a location and the network search following the seizure of a device. It is recommended to formulate the provision so that all forms of non-covert network searches are included, even cases where no device is seized but a search can still be conducted. The draft of the first Supplementary Act includes provisions for conducting covert network searches using obtained login credentials. There are also conceivable cases where, without seizing a device, logging in is possible without the process being covert.
- According to Article 2.7.40, no authorisation from the examining judge (RC) is generally required to conduct a network search during the first 3 days after the seizure. This also applies to active network searches. It is recommended that authorisation from the RC should always be required for active network searches due to their potential scope, the infringements on third-party rights, and issues of sovereignty.
- Based on Article 2.7.40, a network search can be conducted for up to 3 months following the seizure. This period may be too short in specific cases. It is advisable

not to set a maximum duration but to allow extensions whenever there is still a sufficient investigative interest, similar to the regulation of telephone tapping.
- The draft legislation includes the authority to render data on a network inaccessible (Article 2.7.56). The purpose of this, according to the provision, should only be to stop a crime or prevent new crimes. It is recommended to also allow inaccessibility for another purpose: enabling a network search without data disappearing (data freezing).
- We recommend introducing a provision permitting all measures reasonably necessary to implement orders under Articles 2.7.38-2.7.40. This might include changing a password when prompted to log in.
- It may be necessary to remove inaccessible data from an automated system, for example, because its possession is illegal. A provision for this is included in the draft legislation for establishing books 1-6 of the new code. In the draft proposal of the first supplementary law, this provision is amended. This amendment appears to limit destruction to cases where criminal prosecution has been initiated. It is desirable to allow for destruction outside of that context as well.

Supplementary policy

- During the decision-making process regarding network searches, the location of data is often a pertinent issue. If data is actually stored on a server in another country, the sovereignty of that country may impede an investigation by the Dutch authorities. It is frequently unknown where the data is located. There are varying views on how to handle this situation. It is important to develop policy on this matter.

Legal transitional provision

- It is desirable for the authorities granted by Articles 556 and 557 Sv to remain applicable after the expiration of the Criminal Procedure Innovation Act until the new code comes into effect. We recommend that a draft bill for this purpose be submitted to the House of Representatives (Tweede Kamer).

2.2 Article 558 Sv

Content of the pilot

Article 558 Sv allows for measures to be taken to disable biometric security on an automated device. This authority has only been marginally involved in the pilot, as a supporting authority for the application of Articles 556 and 557 Sv, because this authority could already be applied based on the jurisprudence of the Supreme Court (Hoge Raad) even before the pilot began.

Results, effects and appreciation

Article 558 Sv is regularly applied, with subsidiarity and proportionality always being observed. The authority is only used when other methods to unlock a device, such as requesting the cooperation of the suspect, have proven ineffective. In such cases, minimal physical constraints are applied, such as restraining the suspect. No cases have been reported where physical force was used to perform a facial scan or iris scan. The application of this authority has not always been successful. For instance, when a suspect resists or when too many attempts to unlock the device have been made, access to the device is sometimes not achieved. Although Article 558 Sv does not limit whose biometric features can be used for

security purposes, the authority has, as far as is known, only been used to gain access to a device being used by a suspect.

Recommendation

The authority should only be applied when security features such as facial recognition, fingerprints, and iris recognition are in use. Article 2.7.43 section 2 proposes to limit the authority to 'biometric features designated by a general administrative order' (in Dutch: algemene maatregel van bestuur, or amvb). It is recommended not to include an exhaustive list of biometric features in the law or in an amvb, as this would make the law less technology-neutral and future-proof. Although the cases reviewed in the study did not involve other types of biometric features for security, in principle, security with various types of features is possible, and tech companies are working on developing these.

3 Pilot Audiovisual Recording (AVR)

3.1 Subpilot AVR Video Footage

Content of the pilot

In this sub-pilot, conducted at the police units and public prosecutor's offices in North Holland and East Netherlands, and the courts in North Holland and Overijssel, an approach was tested where video footage is succinctly summarised in police reports. The abbreviated police report and the described footage are included in the case files.

Number of cases

A selection of cases was made for treatment as pilot cases by the police. Initially, these were only robberies of premises involving adult suspects. As the number of pilot cases was lower than expected, the selection criteria were broadened during the pilot. The target of 60 cases with a first-instance verdict was not achieved. As of 1 July 2024, a total of 29 cases had been processed as pilot cases by the police, and 17 pilot case verdicts had been issued. No cases had yet been handled in appeal. The small number of cases necessitates caution regarding drawing conclusions.

Methodology

When video footage is secured, a selection of the relevant parts is made. If there are multiple long recordings that follow each other in time or if an event is recorded from multiple camera angles, a compilation is generally made according to the agreements. In the compilation, unrelated bystanders are not blurred. The selected video footage should be included in the case files in MP4 format, along with a police report describing its content. In the pilot methodology, a shortened police report can suffice, in which time indications should be included according to agreements with the Judiciary.

Practically, time indications were not always included in the shortened police reports. Additionally, there were instances where the footage was not provided in MP4 format or the codecs were incorrect, causing the footage to be unplayable by the Public Prosecution Service (OM) and the Judiciary, necessitating re-transmission. There are significant differences in the actual methodology between the two involved police units. In the East Netherlands unit, few compilations were made, and the shortened police reports were scarcely shorter than regular reports. In the North Holland unit, compilations were made when beneficial, and the shortened police reports were indeed shorter, though still quite detailed.

The footage was sent by the police to the OM and then from the OM to the examining judge's office. SecureTransfer was initially used for this. There were frequent problems with the exchange of documents, which led to the search for alternative ways to exchange files. According to the pilot's principles, the integrity of the received footage was to be verified by comparing the hash value of the received file with that of the sent file. This did not actually occur. There are no indications that the integrity of the received files was compromised.

When footage is included in the case files, it is reviewed by the interviewed public prosecutors (OvJs) and trial judges in preparation for hearings. Examining judges (RCs) do not always have time to review the footage in preparation for preliminary examinations. At the North Holland court, the footage is generally shown at the beginning of the trial. Judges at the Overijssel court appear to have done this less frequently or not at all.

Results, effects and appreciation

Public prosecutors (OvJs), judges, and lawyers appreciate that video footage is, unlike in regular practice, standardly included in the case files. This also adds value when a detailed police report is available. The reason for this is that the footage provides a more comprehensive view of events than the written report. When the shortened police reports are indeed shorter than regular reports, no relevant information is missed. It is appreciated that irrelevant details are omitted. The observations of the reporting officers are considered relevant because investigators sometimes have better screens, enabling them to view the footage better, and because they can provide context based on their knowledge and experience.

When there is a lot of footage or multiple long recordings, it is valuable to create a compilation. This offers a better overview of what happened while reducing the workload for the OM and the Judiciary. Playing the footage does not present any issues when the footage is provided in the agreed format. However, exchanging the files is considered a significant bottleneck because it sometimes does not work directly and requires considerable effort. The ability to play the footage on their own computers after receiving it is especially appreciated by OvJs. In regular practice, footage is usually delivered on a USB stick or DVD, which cannot be played on the hardware used by the OvJs.

The processing time does not seem to be significantly affected by the pilot methodology. During preliminary hearings, compilations are sometimes not yet available, but the non-compiled footage usually is. For the police, it saves a lot of time when they can produce less detailed reports. However, creating compilations takes more time. On balance, there is no increase in workload for the police. Reviewing the footage typically takes judges and OvJs around 15 minutes. Given the significant added value compared to reading the police report, they believe the extra time investment is worth it. The limited additional workload is associated with additional labour costs. The police need to invest in personnel training, hardware, and software to create compilations if footage is to be included in case files on a large scale.

Improvement in Criminal Procedure?

The pilot methodology results in an improvement in criminal procedure. It is important for the parties involved in the process to be able to view relevant video footage. The police report on this footage is essential, but it can be more concise than in regular practice. The additional workload and costs of the pilot methodology are limited. The pilot methodology can be extended to other types of footage, such as bodycam footage and videos made by citizens.

Recommendations for adjusting and supplementing the draft legislation

While working with slightly less extensive police reports than in regular practice is recommended, it is not advisable to legislate that summarised reports can be made. The reason for this is that the law does not specify the content of a full police report, nor does it define what the content of a summarised report should be. The summarised police reports made in the context of the pilot comply with the general reporting obligation.

The pilot methodology affects the determination of which documents should be considered as case files. According to current law, source material upon which a police report is based does not need to be included in the case files. Although the proposed definition in Article 1.8.1 can be maintained, its interpretation deserves reconsideration, as source material underlying a police report should, in principle, be regarded as a document to be included in the case files. It is desirable to establish clear criteria for determining whether source material should be included in the case files.

Supplementary policy

It is desirable for working agreements to be made and adhered to between the police, the Public Prosecution Service (OM), and the Judiciary regarding the creation of compilations, the reporting of video footage, and the file formats in which video footage is delivered.

3.2 Subpilot AVR Suspect Interrogations

Content of the pilot

In this sub-pilot, an approach was tested in which suspect interrogations are audiovisually recorded and summarised in a police report. Both the summarised police report and the recording of the interrogation are included in the case files. This methodology was mostly applied in the same cases where the sub-pilot involving video footage was conducted.

Methodology

When a suspect in a pilot case is interrogated, the interrogation is audiovisually recorded. Existing equipment in the interrogation rooms was used for this purpose. In East Netherlands, the recording was made with one camera. In North Holland, three cameras were used, with the footage combined into a single view.

After the interrogation, a shortened police report is created. Practically, this is not possible during the interrogation, as this would require the investigator to prepare on-the-spot summaries of the key statements. Because the report is made afterward, it is not signed by the suspect. The shortened police report is significantly shorter than a full report. It contains summaries of the essence of the suspect's statements, generally including time indications. An experiment was conducted where the recording of the interrogation was listened to for creating the shortened report. However, this proved too time-consuming. Therefore, notes were taken during the interrogation, which were later elaborated. The recording and the shortened police report were added to the case files. In the recording, the faces of the investigators and the screens were blurred.

Judges and public prosecutors (OvJs) have on occasion listened to the entire recording. More frequently, only parts of the recording were played back, where the time indications in the shortened report were crucial. Parts of interrogations, such as small talk at the beginning, are not relevant for the adjudication. It has also happened that a judge did not listen to the recording, considering it irrelevant and too time-consuming. When recordings were listened to, it was done because the shortened police report provided too little information, and by some judges also because they believe they should review all case files.

The recordings were not played during the hearing and were not used as evidence. When the suspect's statement was relevant, other methods were found to use it, such as confronting the confession during the hearing and having it repeated. The lawyers we spoke to did not listen to the recordings because they were present during the interrogations themselves.

Results, effects and appreciation

Reviewing the recording has the advantage of providing access to the exact questions and answers, and observing the suspect's body language. In cases where the reporting is contested, it can be verified against the recording without requiring the recording to be

subsequently added to the case files. However, the added value of this is considered limited, as judges and public prosecutors (OvJs) in regular practice assume that the officer accurately records all relevant information.

The workload significantly increases when the pilot methodology is applied and the recordings are actually reviewed. This affects not only the OM and the Judiciary but also the police. In regular practice, the police report is prepared during the interrogation. Preparing the report after the interrogation takes more time, partly because it involves deciding which parts of the interrogation are relevant and how to succinctly summarise them. Without a full police report, subsequent interrogators will also have to review the recording.

There is a risk that relevant information in an investigation may be lost because the recordings are not reviewed. The police intelligence service also experiences negative effects from this methodology, as only written text can be processed. During interrogations, it is difficult for the investigator to refer back to previous statements of the suspect if they were not noted down. One advantage of this methodology is the potential increase in the quality of the interrogation. The conversation with the suspect does not need to be interrupted for note-taking.

Improvement in Criminal Procedure?

The pilot methodology, where suspect interrogations are recorded and included in the case files along with summarised police reports, does not result in an improvement in criminal procedure. Since the summarised report provides insufficient information about the interrogation, it is necessary to listen to the recording. This requires a substantial amount of time from the involved parties within the police, the Public Prosecution Service (OM), and the Judiciary, while generally not providing additional information compared to a full report. A frequently heard question during interviews was: what problem are we actually solving?

Due to the significant impact on partners within the criminal justice chain, it was decided during the pilot to cease creating summarised police reports of suspect interrogations in pilot cases. The interrogations were still recorded, and the recordings were included in the case files.

Recommendations

We recommend investigating whether it is desirable to record suspect interrogations more frequently than currently indicated in the Instruction on the Auditory and Audiovisual Recording of Interrogations of Complainants, Victims, Witnesses, and Suspects. When a suspect interrogation is recorded, it is possible to review the course of the interrogation if necessary, it can encourage interrogators to conduct the interrogation carefully, and it allows for not having to take notes during the interrogation, which can improve the quality of the interrogation. Recording suspect interrogations more frequently would also align with the non-binding but highly authoritative United Nations' Principles on Effective Interviewing for Investigations and Information Gathering (Mendez Principles).

When suspect interrogations are recorded, it could be efficient to convert them into written text using speech-to-text software. Currently, the Generic Service for Automatic Speech Processing (GDAS) is being developed within the police. It is expected to be ready for testing in an operational environment in the near future. We recommend, within the context of the AVR pilot, investigating in a limited number of cases whether GDAS can be helpful in producing usable and reliable police reports.

There are divergent opinions among respondents on whether recordings of suspect interrogations should be routinely included in the case files. Including them is an advantage from the perspective of transparency and verifiability of how the interrogation was conducted and reported. At the same time, it is generally not considered necessary to listen to the recordings. Some judges fear that if the recordings are included in the case files, they will need to be reviewed, and their availability could lead to more instances where lawyers contest the reporting.

In the context of the AVR Video Footage sub-pilot, it was recommended that source files on which police reports are based should be considered case files. In line with this, it is recommended that recordings of suspect interrogations should also be routinely included in the case files. This does not imply that judges should routinely listen to the recordings. This should only occur when it is deemed relevant.

Furthermore, it is advisable to investigate whether it is desirable to record suspect interrogations conducted by examining judges (RCs) and other investigative services apart from the police, and include these recordings in the case files.

Supplementary policy

It is desirable for agreements to be made and adhered to between the investigative services, the Public Prosecution Service (OM), and the Judiciary regarding the reporting of (suspect) interrogations.

3.3 Subpilot AVR In-Court Sessions

Content of the pilot

This sub-pilot was carried out at the Limburg district court and the Den Bosch court of appeal, along with the corresponding public prosecutor's offices. Court sessions were audio recorded, after which the recordings and summarised police reports were included in the case files.

Number of cases

At the Limburg district court, 82 substantive sessions were recorded, including 11 pro forma sessions. Appeals were filed against the court's rulings 23 times, of which 4 appeals were withdrawn. In 2 of the 19 appeal cases that had to be heard, a full police report of the session was immediately prepared. The court requested the elaboration of a summarised police report 13 times. In only 4 appeal cases was the hearing held based on the summarised police report of the session. As of 10 July 2024, 10 appeal hearings had taken place at the Den Bosch court of appeal. The sessions in cases recorded by the Limburg district court were also recorded in appeal in principle. In addition, the court of appeal recorded 31 other appeal sessions.

Methodology

Based on selection criteria, a preselection of cases to be recorded was made. It was then up to the judges to decide whether the session would actually be recorded. In dozens of cases, this did not happen, for instance, because the case was deemed too complex for the pilot or due to security risks.

Several courtrooms were equipped with special microphones, allowing each speaker to be recorded separately. The microphones were connected to a laptop with software intended

not only to make the recording but also to create a verbatim transcript of the recording for internal use by the Judiciary. The recording of the session was included in the case files, along with a usually summarised police report.

It was decided that the summarised report would only include the data required by law. Practically, this means that the defences and requests made by the defence and the court's decisions on them were recorded, but the reasoning behind the decisions was not. If a defendant made a confession, this was noted without including the verbatim content of the confession.

Listening to the recording is necessary to obtain sufficient information about the first instance hearing when only a summarised police report of the session is available. However, this is very time-consuming. Therefore, most of the involved parties did not listen to the recordings. In preparing for the appeal hearing, the clerk and the presiding judge of the session combination listened to the recording, but the other judges probably did not.

Results, effects and appreciation

The quality of the audio recordings is excellent. However, the quality of the transcript, which was intended to aid in reviewing the recording, is inadequate. This is partly due to misattributed text, missing text, and incorrect interpretation of words. The audio recording generally contains more information than a regular court session report. However, non-verbal communication, which is described in a regular report when relevant, cannot be observed on the recording. It is also not always clear who is speaking when listening to the recording. The recording includes all communication during the session, usually in spoken language (with incomplete sentences) and sometimes in difficult-to-understand dialects.

A regular court session report only describes the relevant parts of the session, predominantly formulated in formal language. Written text can be more efficiently processed than an audio recording. When reading a professionally written report on relevant session aspects, the reader retains the information better than when listening to a recording. Text can also be skimmed, while listening to a recording requires every word to be heard. Reviewing a recording takes at least as long as the session itself and additional time to replay unclear segments and take notes. This greatly increases the time required to prepare for a session. In a session with a panel of three judges, this applies to the clerk, all three judges, the attorney general, and the defendant's lawyer. Compared to the regular process, this represents a significant increase in workload, while the work pressure is already high. For the clerk who summarised the session, the workload initially decreases, but this time-saving is negated if a detailed report must still be prepared on request of the court of appeal.

The pilot methodology not only involves high personnel costs but also substantial material costs, as courtrooms need to be equipped with recording devices and the recordings must be stored.

Improvement in Criminal Procedure?

The pilot methodology does not result in an improvement in criminal procedure. Listening to the recording of the session is a very time-consuming activity that adds no value compared to reading a full report of the session. However, recording the session for internal use within the Judiciary does have value in some cases.

3.4 New evidence for audio and/or video recordings

Article 576 Sv stipulates that audio and/or video recordings constitute an independent means of evidence. In regular practice, such recordings are used as evidence through the means of the judge's personal observation (Article 340 Sv). During the AVR pilot, this evidence was used on a limited scale. Different choices were made regarding the presentation of this evidence in the judgment or ruling. The North Holland court, in the evidentiary annex, only mentioned the evidence without including the substantive content. This content, however, was mentioned in a reasoning segment. The Limburg district court and the Den Bosch court of appeal included both the evidence and the substantive facts and circumstances in the evidentiary annex. Both approaches are legally sustainable.

It cannot be concluded that there is an improvement compared to the methodology outside the pilot because the law already allowed the use of audio and/or video recordings as evidence, and the methodology does not fundamentally differ from using the judge's personal observation. Among respondents, there is no need for the introduction of a new form of evidence for AVR. However, there are no negative experiences with the new evidence that would lead to a recommendation to remove the new form of evidence from the draft legislation.

Although the use of audio and/or video recordings through the judge's personal observation is possible, we cautiously conclude that introducing the new form of evidence is desirable. The decisive argument for this is that the 'judge's personal observation' as means of evidence pertains to observations made during the hearing. The caution arises from the fact that the new form of evidence is likely to be seldom used, as the report describing the content of the recording will generally suffice as evidence. If the new form of evidence is retained in the draft legislation, it is advisable to adjust its formulation.

3.5 Cross-pilot recommendations

Creating, storing, and making available audio and/or video recordings infringes on the privacy rights of those involved. It is desirable to investigate under what conditions recordings of interrogations or court sessions may be made, stored, and made available.

A necessary condition for including recordings in the case files on a large scale is the provision of a methodology that eliminates the need for exchanging files between partners in the criminal justice chain.

4 Pilot Assistant Public Prosecutor (hOvJ)

4.1 General

Content of the pilot

In this pilot, experience was gained with the exercise of certain special investigative authorities by assistant public prosecutors (hOvJs). These authorities include the requisition of certain types of data (mainly Articles 126nd and 126ne Sv, and often bank data) and the use of the IMSI-catcher (Article 126nb Sv), which can gather the IMSI number of a phone, enabling that phone to, for example, be tapped subsequently. Additionally, authorities related to the return of seized items not voluntarily surrendered by the possessor (Article 116 paragraphs 3-4 Sv) were exercised by assistant public prosecutors. Outside of the pilot, these authorities are reserved exclusively for the public prosecutor (OvJ). Only designated assistant public prosecutors who completed the specially developed training exercised the pilot authorities. In total, there were 94 hOvJs involved.

Involved Criminal Justice Chain Partners

The pilot was conducted within three police units – across all types of teams: Basic Team (in Dutch: Basis Team, or BT), District Investigation Service (in Dutch: Districtsrecherche, or DR), and Regional Investigation Service (in Dutch: Dienst Regionale Recherche, or DRR) – and within the special investigative services FIOD, ILT-IOD, NLA-IOD, and NVWA. Public prosecutors (OvJs) from the respective prosecutor's offices were involved.

4.2 Special Investigative Authorities

Number of applications

The exact number of times the pilot special investigative authorities (BOB-bevoegdheden) were used by the police is unknown, as these applications were not specifically recorded. It appears that the authorities were used quite frequently by the police, but rarely by the Basic Teams (Basis teams). However, the special investigative services (BODs) did record the applications. The records show that assistant public prosecutors (hOvJ's) issued 2,144 requisitions based on Article 126nd Sv and 24 based on Article 126ne Sv. Over three-quarters of all requisitions by the BODs were made by the FIOD.

Methodology

There are significant differences among the investigative services involved regarding the position of the assistant public prosecutor (hOvJ) within the organisation and their working methods. When a public prosecutor (OvJ) is involved in a case, regular consultations take place between the investigative team and the case team (OvJ and prosecution secretary). During these consultations, discussions include which requisitions will be made. In regular practice, a request is then submitted to the Public Prosecution Service (OM), usually reviewed by the prosecution secretary, after which an administrative employee drafts the requisition, and an OvJ signs it.

In the pilot methodology, the investigative officer generally consults the relevant hOvJ about the desirability of issuing a requisition. This includes discussing the scope of the requisition. If the hOvJ agrees, the investigative officer drafts a police report of the request, referencing the suspicion report, and sends it to the hOvJ. The hOvJ evaluates the request primarily based on legal criteria and practicality. If the suspicion report has not been previously established, the hOvJ must do so. If the hOvJ finds the request unsatisfactory, it is revised by the requester and resubmitted. Once the request is approved, the requisition is drafted.

hOvJ's can be more or less involved in the investigation for which the requisition is requested. Requesters have approached both hOvJ's who were already involved in the investigation, such as the coordinator of an investigative team, and hOvJ's who were unfamiliar with the case. This choice was determined by practical factors, like the hOvJ's availability, rather than the expected quality of decision-making.

It has frequently happened that the OvJ decided on a requisition that fell within the hOvJ's authority. This was sometimes due to the unavailability of a pilot-hOvJ. Especially in Basic Teams, it was also common for requisitions discussed during a meeting with the OvJ to be issued by the OvJ for practicality. In complex or sensitive cases, OvJs sometimes indicated a desire to issue the requisition themselves.

hOvJ's have rarely used the authority to decide on the use of the IMSI-catcher. This authority is closely associated with the OvJ's wiretapping authority and requires a consideration of resource allocation. Therefore, it is usually the OvJ who has made this decision.

Results, effects and appreciation

To get an understanding of the quality of hOvJ's decisions, requisitions issued by hOvJ's were reviewed by OvJ's in two rounds. Initially, the review was conducted by a single OvJ. If this OvJ concluded, even after feedback from the relevant hOvJ, that the requisition should not reasonably have been issued, a committee of three OvJ's reviewed the requisition. In total, 245 requisitions were reviewed, roughly equally divided between the police and the special investigative services (BODs).

In the first round, 16% of the requisitions were negatively assessed by the committee, and in the second round, 13%. A breakdown by investigative services shows that in both rounds, the police received significantly fewer negative assessments (11% and 4% negative, respectively) than the BODs collectively (22% and 23% negative). All requisitions issued within the Regional Investigation Service (Dienst Regionale Recherche) of the police were positively assessed. There were significant differences within the BODs, particularly with the Dutch Labour Authority's Intelligence and Investigation Service (NLA-IOD), whose requisitions were often negatively assessed. No explanation was found for this. An analysis of the types of errors found revealed that in cases of a negative assessment, at least one error was made that would have prevented the requisition from being issued even with better justification.

Interpreting the results is challenging because no OM requisitions were included in the review, making it impossible to compare the rejection rate of hOvJ requisitions to that of OM requisitions. It is also not possible to determine an acceptable error rate. To get an impression of the quality of OM-issued requisitions, this was queried in interviews. Respondents, both from investigative services and the OM, indicated that OM-issued requisitions also frequently contain errors, including errors that render a requisition unfeasible. It is relevant that requisitions often include sections copied from the request, typically by an administrative employee. This also happens when an hOvJ drafts a requisition, meaning the quality of the request significantly affects the quality of the requisition. Overall, it cannot be concluded

that hOvJ's requisitions generally contain more errors than OM's requisitions. However, certain BODs seem to make relatively more errors than other investigative services. Errors in requisitions typically do not have severe consequences, partly because a new requisition can be issued.

The review of requests requires a magistrate's perspective. An hOvJ involved in the investigation might be inclined to issue a requisition too easily to aid the investigation. The data from the review rounds do not indicate that requisitions were more frequently rejected when the hOvJ had a closer connection to the investigation. Interviews with hOvJs and requesters reveal that hOvJs assess requests with equal care whether they are involved in the investigation or not.

When a request is submitted to an hOvJ, a requisition is issued more quickly than when the request is submitted to the OM. The difference in processing speed is particularly pronounced for requests made by the police and reviewed by the district prosecutor's office. It can take up to two weeks for a requisition to be issued, while an hOvJ generally issues the requisition on the day of the request. This shorter timeframe can impact the resolution of criminal offences. Requesters have indicated that quick turnaround is beneficial when the hOvJ handles the requisition, allowing them to walk in for consultations. If a request is deemed unsatisfactory, quick discussions can lead to a swift resubmission.

The time hOvJs require to review a request ranges from 30 to roughly 90 minutes. More preparation time is needed if the hOvJ is unfamiliar with the investigation. Interviewed OvJs indicated that they can review requests in a shorter time, sometimes in just five minutes. When hOvJs issue requisitions, the workload at the OM decreases while it increases at the investigative services. Overall, an increase in workload is possible.

Authorising hOvJs results in a shift of workload from the OM to the investigative services, with financial implications. Additionally, the training of hOvJs incurs costs.

Improvement in Criminal Procedure?

A significant advantage of having requisitions for data issued by hOvJ’s is that they are processed faster – often significantly faster – which can impact the ability to solve criminal offences in concrete cases. Another benefit is that the person issuing the requisition works within the same organisation, making it easier to consult. A possible downside is that hOvJ’s appear to need more time to assess requests than some employees at the OM. On balance, allowing hOvJ's to exercise the authorities under Articles 126nd and 126ne Sv represents an improvement in criminal procedure.

It is advisable to authorise only designated hOvJ's for these requisitions. Interviews have shown that not every hOvJ is equally suited to exercise the pilot authorities. Some hOvJ's primarily work in the preliminary stages of investigations (arrest, detention for investigation), while others have more affinity with investigative work. Limiting the number of authorised hOvJ's could enhance their expertise, as they would gain more experience with the authorities than if every hOvJ were authorised.

It is not an improvement in criminal procedure for hOvJ’s to requisition data in cases of organised crime or terrorist offences, as these involve complex and/or sensitive matters that should be decided by OvJ's. Similarly, the use of the IMSI-catcher is best assigned to the OvJ, as the OvJ will also have to decide on subsequent authorities, such as wiretapping, and because deploying the IMSI-catcher involves policy considerations due to the high costs and limited availability of IMSI-catchers.

Supplementary policy

Under the new code, the OvJ remains authorised to issue requisitions. Policies could be established to specify the types of cases in which requests based on Articles 126nd and 126ne Sv must be submitted directly to the OvJ. Factors such as the complexity of the case and the requisition could be relevant. It is also conceivable that the first requisition in a case should always be issued by the OvJ.

A recurring theme during the interviews was the lack of uniformity. It must be clear which forms should be used to submit requests and issue requisitions, and how these forms should be filled out. It should also be clear how and to what extent a request needs to be substantiated, and whether attachments should be included with the request report. Moreover, it is desirable to investigate whether the process for requesting data requisitions can be made more efficient. This could be achieved, for example, by making the entire process of requesting and issuing requisitions completely digital (with digital signatures) and by using a single document throughout the entire process of request and decision-making.

4.3 Powers in relation to seized items

Methodology

When an item is seized, a decision regarding the seizure must eventually be made. If the possessor of the item has not relinquished their claim to it, the public prosecutor (OvJ) is authorised to decide on its return based on Articles 116 paragraphs 3-4 Sv. The Criminal Procedure Innovation Act (Innovatiewet Strafvordering) has also allowed the assistant public prosecutor (hOvJ) to make this decision.

For instance, if a stolen vehicle is discovered and seized, the hOvJ can place the vehicle in the custody of the rightful owner. A custody contract is then drawn up for this purpose. Before the vehicle can be formally returned, the possessor must receive a letter indicating the intention to return the vehicle to the rightful owner. The possessor then has 2 weeks to file a complaint with the court regarding the intended return. If no complaint is made within this period, the vehicle can be formally returned.

Number of cases

The pilot authorities are only relevant to the police. They were not used by the special investigative services (BODs). The exact number of times the pilot authorities were used is unknown. It appears they were used less frequently than possible. This can be partly explained by the lack of familiarity with the authorities among investigative officers.

Results, effects and appreciation

The quality of decision-making in specific cases has not been investigated. OvJ's, hOvJ's, and requesters have the impression that hOvJ's are capable of making decisions and handling the associated formalities.

A significant advantage of having hOvJ's exercise these authorities is that seized items can be returned to their rightful owners more quickly than if the OM had to decide. OvJ's are often busy, which can result in a long wait before they make a decision on a request to apply Article 116 paragraphs 3 or 4 Sv. When the hOvJ decides, the seized items do not need to be transported to the Seizure House (Beslaghuis), which is common practice. The shorter

processing time for the seizure is often of great importance to rightful owners. This is why hOvJ's find the additional workload, estimated at 1 to 1.5 hours, acceptable. At the OM, the workload decreases. Overall, the workload is reduced, thereby lowering the costs associated with exercising these authorities.

Improvement in Criminal Procedure?

Granting the authorities of Article 116 paragraphs 3-4 Sv to every hOvJ results in an improvement in criminal procedure. A compelling argument is that rightful owners can retrieve their property significantly faster. These authorities are not particularly difficult to apply and cause relatively little infringement on the rights of the possessors and third parties. Unlike the situation with Articles 126nd and 126ne Sv, it is recommended to grant the authorities of Article 116 paragraphs 3-4 Sv to every hOvJ.

Recommendations for adjusting and supplementing the draft legislation

Article 2.7.27 paragraph 2 stipulates that the (assistant) public prosecutor ((h)OvJ) can make a decision leading to the destruction of a seized item. This is only permitted when it involves a small quantity of drugs. It is recommended to extend this authority to other items that are evidently required to be removed from circulation. Furthermore, it is advisable to specify in the law that a letter informing the possessor of the intention to return a seized item only needs to be sent when it is reasonably possible.

4.4 Legal transitional provision

It is desirable for the authorities under Articles 126nd, 126ne, and 116 paragraphs 3-4 Sv to remain applicable after the expiration of the Criminal Procedure Innovation Act until the new code comes into effect. We recommend that a draft bill be submitted to the House of Representatives (Tweede Kamer) for this purpose.

Dialogic innovatie & interactie
Hooghiemstraplein 33
3514 AX Utrecht
030-215 05 80
www.dialogic.nl