Summary

This report gives an account of research carried out in order to compile an inventory of part of current investigation practices relating to the confiscation of certain items. This mainly concerns investigations carried out by investigating officers on electronic data carriers and computerised works after such confiscation. The report focuses on possible further standardisation of such research in connection with modernising the Code of Criminal Procedure. The main question posed in this research is: "What do we know about the confiscation of electronic data carriers and computerised works and the subsequent police investigations carried out on them?"

This general question gives rise to various quantitative and qualitative research questions which have been taken as a general guideline when clarifying confiscation practices.

Section 2 outlines the legal framework for the confiscation of items and the subsequent police investigation of electronic data carriers and computerised works. This makes it clear that the Code of Criminal Procedure contains very few specific regulations relating to the investigating of confiscated electronic data carriers or computerised works, as opposed to investigations carried out on data carriers and computerised works during an on-site search carried out in order to establish data: the law does contain specific provisions in respect of the latter. From the legal precedents discussed, it emerges that the lower courts differ in their opinions on whether the provisions governing the confiscation of items, including Article 94 of the Code of Criminal Procedure, still constitute a sufficiently foreseeable basis to enable investigating officers to compile information stored on a confiscated smart phone, partly in view of the provisions in Article 8 of the European Convention on Human Rights while also taking technological developments into account. The interpretation of these provisions, insofar as they relate to the confiscation of items for the purpose of carrying out additional investigations to gain access to the data they contain in the interests of establishing the truth, is not unanimous. There is still no specific legislation relating to this particular field to date.

With respect to the quantitative research questions, it has emerged that on the basis of existing figures for the confiscation and subsequent investigation of electronic data carriers and computerised works, investigating officers do confiscate a great many data carriers. These figures do not distinguish between the grounds for confiscation and the relevant authority by which or under whose responsibility the items are confiscated. Although such situations do occur, no specific figures exist in respect of the on-site inspection of computerised works by investigating officers in order to take cognisance of the data contained therein without formally confiscating the item in question. Moreover, no figures

relating to the deleting of files on electronic data carriers or computerised works are available either because these figures are not registered.

With respect to the qualitative research questions, the report concludes that in most cases, the decision whether data carriers are to be confiscated is made during preparations and particularly while in situ. In most cases the decision to confiscate these data carriers is made by the Public Prosecutor or the examining judge in view of the fact that items are generally confiscated while the premises are being searched. The outcome of this decision strongly depends on suspicion of the offence and the scope of the inquiry, and also on the authorities involved in such confiscation. The main principle here is that an assumption is made that all data present on the relevant items may be investigated, except for any data that comes under the professional right of non-disclosure.

All or part of the data is copied for further investigation unless such data is encrypted or access to it has been blocked. The copies are recorded in business systems, and policy relating to access to such business systems varies from region to region. Apparently there is no central management in existence with respect to the way in which data must be destroyed or made inaccessible, or when this should be done. Although the Police Data Act does contain regulations on statutory retention periods for such data and on its destruction, their content is not widely known in practice. The Code of Criminal Procedure does not contain any stipulations in this respect.

In practice, certain problems occur in respect of the confiscation of electronic data carriers and computerised works insofar as the relevant data comes within the scope of the professional right of non-disclosure. The existing legislation and regulations apparently do not provide sufficient clarity on these points in practice. The filtering of data that comes under the professional right of non-disclosure has not resulted in any practicable methods for criminal investigations to date.

With respect to the compiling of data that has been stored elsewhere (in the cloud), current legislation does not provide any specific powers, and no policy regulations are in existence either. Such data is only compiled sporadically. The relevant problems relate to issues concerning violations of other nations' sovereignty and the absence of sufficiently clear legal provisions on this point. Policy is based on the main principle that no data should be recorded in the event of doubts relating to violations of national sovereignty. It is advisable to ensure clarity with respect to the limits and options of cross-border investigations.

Investigating officers occasionally carry out investigations on (mainly) computerised works that have not been formally confiscated. Apparently these investigating officers do not have a clear idea of their legal powers and the circumstances under which data carriers may be investigated.

In the event that investigating officers find 'illegal content' on a data carrier, the general principle is that this data carrier is not restored to its owner. Policy in this respect varies from region to region. The possibility that security cameras register images of the relevant search in which investigating officers can clearly be identified is often cited as 'content to be deleted'. The investigation departments themselves are in some doubt regarding the extent to which such images may be deleted, and if so, who has the authority to delete them. The lack of any specific regulations in this connection is regarded as a problem by the criminal investigation departments, and this might be the reason why the deleting of all or part of files on electronic data carriers or computerised works is not registered.

While bearing the answering of the quantitative and qualitative research questions in mind, the report answers the main question relating to the research with the following general conclusions.

The overall picture that emerges from the research is that insufficient figures are available in a quantitative sense to enable any definite conclusions to be drawn, apart from the fact that large numbers of data carriers have been confiscated. The interviews show that no internal policy - or relatively little - has been formulated with respect to investigations into confiscated electronic data carriers and computerised works. In cases where such policy does exist, this is not always complied with to a sufficient extent, or it does not enjoy sufficient support.

It is up to the Dutch Supreme Court to provide a more definite answer to the question of whether the provisions relating to the confiscation of items (including Article 94 of the Code of Criminal Procedure partly in conjunction with the stipulations in Article 8 of the European Convention on Human Rights) constitute a sufficiently foreseeable basis for investigating officers to compile data stored on a confiscated smart phone. In such an event, the explanation of the scope of certain powers as stated in the law, which is not specified further in the relevant legislation, will be left to the judiciary. This might contribute to the weakening of a democratic legitimation of the explanation of the scope of powers relating to criminal procedure in view of technological developments. In cases where procedural facilities are deemed necessary, this will easily exceed the Supreme Court's law-formative duties. It seems desirable for the legislator to adopt an independent viewpoint on the scope of the relevant powers, and to initiate further statutory regulations if desired.

In practice, it is of great importance that a more unambiguous working method is prescribed for the points stated in the foregoing. The present legislation and regulations are insufficiently clear with respect to a number of points identified in the research, and it has emerged that they give rise to questions in practice. In cases where clarification of legislation and regulations is required, it is important that this clarification can be achieved in various ways. Amendments to the Code of Criminal Procedure will not be necessary

with respect to all the points. Moreover, maintaining a more unambiguous policy that can provide guidelines for everyday implementation in practice could be a significant factor here.