Summary

The Decryption Order and the Privilege Against Self-Incrimination
Do developments since 2000 suggest a need to force suspects to decrypt?

Background and research question

When a criminal encrypts his computer data or communications, it is difficult for criminal investigators to collect this information through computer search and interception. One of the possible solutions to this problem is to force the persons in question to decrypt their data. The Netherlands introduced a decryption obligation in the Computer Crime Act (1993). However, at present, suspects cannot be ordered to decrypt their data. To date the Dutch legislator has proceeded on the assumption that compelled decryption violates the privilege against self-incrimination (known in Dutch as the principle of *nemo tenetur*). According to established case-law of the European Court of Human Rights (ECtHR), the privilege against self-incrimination lies at the heart of the right to a fair trial in article 6 of the European Convention of Human Rights and Fundamental Freedoms (ECHR). The precise scope of the privilege has not yet been properly thought-out and there is acceptance of the necessary exceptions to the privilege in legislation and case-law.
A study carried out in 2000[294] concluded that it is a major breach of the privilege to compel suspects to decrypt their data and that this could not be justified in the interest of criminal investigation. However, since 2000 there have been new developments in the field of technology and case-law on the privilege against self-incrimination. Following the Amsterdam child-abuse case involving Robert M., the Dutch Second Chamber also raised the question whether a decryption order should be newly introduced for suspects. Against this background and in view of developments since 2000, the main question investigated in this report is: to what degree can a decryption order (an order enforcing co-operation to access protected data) be considered compatible with the privilege against self-incrimination? Answers to this question are based on desk research, analysis of legal developments in other countries, and five semi-structured interviews with experts in investigative practice.

The privilege against self-incrimination

The scope of the privilege against self-incrimination has, in the European Court's case-law, not significantly changed since 2000. The essence of the privilege still lies in the freedom to make statements or to remain silent. Sometimes a suspect may be put under a certain amount of pressure to obtain statements, but that pressure should not be excessive and must be controlled by procedural safeguards, such as access to a lawyer and inform-

294 Koops 2000. For an English summary, see Koops, B.J. (2000), 'Commanding Decryption and the Privilege against Self-incrimination. The Dutch perspective', in: C.M. Breur, M.M. Kommer, J.F. Nijboer & J.M. Reijntjes (eds.), *New Trends in Criminal Investigation and Evidence – Volume II*, Antwerpen etc.: Intersentia 2000, p. 431-445.

ing the accused of the consequences his attitude could have on the course of the proceedings. In other forms of compelled co-operation than making statements, the privilege implies that the more the suspect has to actively participate in the investigation, especially if he has to make an intellectual effort, the more likely this obligation to collaborate will be in conflict with the privilege against self-incrimination. A decryption order comes very close to making a statement, because the password resides in the head of the accused and it cannot be obtained without his (intellectual) effort. This is why, just like the 2000 study concluded, a decryption order for suspects infringes the privilege against self-incrimination.
This infringement may, however, be justified, because there are possible exceptions to the privilege. The European Court considers four factors, which together determine whether or not compelled co-operation is acceptable in light of the privilege against self-incrimination:
1 the nature and extent of coercion;
2 the weight of the public interest;
3 the presence of relevant safeguards in the procedure;
4 the way in which the compelled material is used.
As the amount of pressure to co-operate increases and compelled material plays a greater role as evidence, the public interest of compelled co-operation will have to be higher and more safeguards for legal protection will have to be present. In case of a lower level of coercion or a subordinate role of the compelled material as evidence, a decryption order will sooner stand the test of article 6 ECHR.
In Dutch law, the role of the privilege against self-incrimination has largely remained the same since 2000. A decryption order for suspects would still not fit well in the system of Dutch criminal law to the extent that a refusal to co-operate would be punishable. Case-law does indicate that it is possible to request decryption from suspects if they can excuse themselves, comparable to an interrogation when an accused may claim the right to remain silent. In this case, the suspect takes a certain procedural risk if he does not co-operate, because under certain circumstances, if the presence of protected files clearly raises questions, the judge might use his refusal to decrypt in the construction of evidence, in sentencing, or in other decisions to the detriment of the accused.

Developments abroad

In 2000, no country had introduced a decryption order for suspects, but things have changed substantially since then. The decryption order introduced in Belgium may not be issued to suspects, but France and the United Kingdom have introduced a decryption duty for suspects. The UK has extensive legislation with various legal safeguards as to when and how a decryption order may be given. In France, legislation is limited to criminalising the refusal to decrypt. In addition, Australia has introduced a statutory decryption order that specifically targets suspects, whereas in the United States, case-law is gradually shaping the conditions under which a decryption order for suspects is deemed consistent with the (American) privilege against self-incrimination (which has many similarities with the ECHR version of the privilege).

British and American case law suggest that co-operating with a decryption command is similar to making a statement, as it implicitly acknowledges the connection between the suspect and the encrypted material. This infringes the privilege against self-incrimination. However, according to US case-law, this can be justified either if the existence and location of the files and the suspect's ability to decrypt are a foregone conclusion, or if immunity is provided for the act of decryption and for the (incriminating) material that emerges after decryption. In the United Kingdom, the decryption order's infringement of the privilege against self-incrimination has been considered acceptable because of the many checks and balances in the British system and because of the court's discretionary power during trial to exclude compelled incriminating evidence. Although the case-law in these countries is still developing, it appears that a decryption order for suspects is considered acceptable under certain conditions, which can be shaped and further developed by the courts. British legislation thus provides points of reference for Dutch policy. The regulatory framework cannot be directly transferred, however; the United Kingdom has opted for a high degree of coercion (2 to 5 years' imprisonment for failure to co-operate), which can only be justified by extensive safeguards, including the possibility to exclude evidence, but also including some safeguards unknown to the Netherlands, such as an independent supervisory authority to oversee investigation powers.

Enforceability and developments in technology

The use of cryptography by suspects, particularly to encrypt stored data, has notably increased since 2000. For the time being, strong encryption seems to be used mainly in certain child pornography networks (which are often early adapters of advanced hiding technologies), but other groups of criminals could follow. An important development is the rise of 'anti-forensic' programs, i.e., crypto programs that do not only encrypt files but also make it possible to conceal the existence of encrypted files with 'plausible deniability'. These programs make it difficult for the judiciary to prove that there are any encrypted data on the hard disk.

On the other hand, the prosecution now appears to have greater opportunities than seemed the case in 2000 to argue that a suspect has possibly incriminating evidence (such as downloaded child pornography) on his computer and that he is able to decrypt, e.g., using indications from intercepted communications or traffic data. British and American case-law also show that

there are several possible cases in which the accused 'has something to explain' if he does not want to decrypt.
These two developments do not neutralise each other, but rather imply that much will depend on the circumstances whether a decryption order is enforceable. Therefore, unlike the 2000 study concluded, the difficulty of enforcement does not necessarily imply that a decryption order for suspects should be categorically rejected. Instead, it can be an option to have a statutory power that the judiciary may or may not apply depending on the circumstances. A decryption order will probably have little effect on serious and calculating criminals who do not co-operate with the police anyway, and is likely to affect rather the minor or less smart criminals. Experience in the United Kingdom indicates that a decryption order is imposed in only a limited number of cases, in which less than half of the addressees co-operate; in the past four years, only six refusers have been sentenced for not co-operating.

Conclusions and recommendations

The above findings show that a decryption order for suspects is not incompatible with the privilege against self-incrimination. It depends on how the law is structured (e.g. the type and degree of coercion used) and how it is applied in specific cases. Where the 2000 study concluded that the Netherlands should not adopt a decryption order for suspects because this would only be effective through a high level of coercion and this would yield an unacceptable infringement of the privilege against self-incrimination, the situation is somewhat different now. Developments abroad and in technology suggest that a decryption order for suspects could be compatible with the privilege against self-incrimination and – albeit in a limited number of cases – effective, provided the legislation and implementation are based on adequate safeguards.
Should the legislator, as in the UK, opt for a decryption order with a high level of coercion, then significant safeguards must be taken, such as a written order, access to a lawyer, a fair burden of proof, a discretionary power for the court to exclude self-incriminating evidence, and oversight of the practice by an independent supervising authority. It is also conceivable to choose less coercion, that is, not to criminalise the refusal to decrypt, but to allow the court to draw adverse inferences from a decryption refusal in constructing the evidence or in sentencing. Furthermore, the judiciary can, in some cases, also consider providing a suspect with immunity if he will decrypt. The decrypted material can then not be used against the suspect but it can be used against others or, for example, to identify (or exclude) victims, which in child pornography cases can be an important aspect.
Viewed together, there are three options for the Dutch legislator regarding the decryption order for suspects.

1 *Maintain the status quo.* An order to decrypt may not be issued to suspects, but the police and judiciary may request suspects to co-operate voluntarily. Under certain circumstances, current law allows the court to use the fact that a suspect has not decrypted in the construction of evidence or when sentencing.
2 *A decryption regulation in accordance with the regulation of interrogation.* Current practice to request decryption is formalised, in a statute or lower regulations, in order to regulate the decryption request in the same way as interrogation is regulated (art. 29 Dutch Code of Criminal Procedure). This will not make much difference in practice, but it fits better in the legal system because co-operating with decryption is more similar to making statements than to delivering physical evidence. Regulating decryption requests according to the rules for interrogation has the advantage that appropriate safeguards are present, such as access to a lawyer and informing the suspect beforehand of the right to remain silent. This could increase the possibilities of drawing adverse inferences from the suspect's decision not to co-operate.
3 *A decryption command to suspects with criminalization of non-co-operation.* Failure to co-operate with a decryption order is penalised under Article 184 of the Dutch Criminal Code (the general provision on not complying with a legal order, carrying up to three months' imprisonment) or under a separate provision that carries a higher maximum punishment. The ECHR requirements imply that a heavier penalty will be more acceptable if it is restricted to specific types of offences that demonstrably cause a major social problem. Criminalising the refusal to decrypt infringes the privilege against self-incrimination more seriously than the previous option; it must therefore have many safeguards and its need should be carefully substantiated. In order not to deprive the privilege against self-incrimination of its meaning, in any case, the court should always have the legal possibility to exclude compelled decrypted data from the evidence.

Analysis of the ECtHR case-law and the Dutch legal system shows that the second option is preferable to the first one. Unlike in 2000, the third option does not have to be rejected outrightly. There is some scope within the limits of the privilege against self-incrimination to issue, under threat of a criminal sanction, a decryption order to suspects. In view of the strong requirements, it will not be very effective in general, but it may be in specific cases. It is therefore ultimately a question of public policy whether penalising the refusal to decrypt – which can be done within the boundaries of the privilege against self-incrimination if sufficient safeguards apply – is preferable over regulating decryption requests in accordance with the regulation of interrogation.

In view of this conclusion, it is recommended that the legislator renews its consideration whether and under what conditions a decryption order could be issued to suspects. The legislator should in any case seriously consider the second option. The choice between the second and third option (i.e., between little or much coercion) rather boils down to a decision of criminal policy. This does not imply a zero-sum trade-off between legitimacy and effectiveness. It is especially important for a decryption order for suspects, that a well-considered combination is chosen of the coercion to be applied, the way in which compelled material is used, and procedural safeguards, as well as that the legislator carefully motivates on the basis of public interest why the chosen regulatory framework yields an acceptable infringement of the privilege against self-incrimination.

It is important for policy-makers not to expect miracles from a decryption order. It will only be effective in a limited number of cases where a defendant clearly 'has something to explain' and where already much evidence is available against the suspect. Moreover, the legislator should show reserve in the instrumental use of criminal law: the objective is to punish criminals for offences they have committed, and not to punish defendants for failure to cooperate in gathering evidence. Furthermore, in respect of the policy concerning the decryption order, it is recommended to look at the broader perspective of problems encountered in digital investigation (e.g. cloud computing) and to consider alternative ways of addressing the problem of encryption, such as police Trojans that can secretly intercept passwords or keys.