**The Nemo Tenetur principle and the case law of the ECHR**

To date, the ECtHR has not yet ruled on the issue, which means that national courts and tribunals do not have clear supranational guidance in this matter. A thorough study of the case law of the European Court of Justice does teach us how the Court classically answers questions about the right to remain silent and the principle of non-incrimination. The jurisprudence can therefore give us an idea of how to deal with an obligation of decryption. However, the peculiarity of the decryption issue (only the key is obtained through coercion, but serves to make potentially a lot of information accessible/readable) makes a comparison with existing situations difficult and a prediction of the Court's approach difficult.

The judgments of the ECtHR on the non-incrimination principle generally follow the same pattern, at least the approach of the ECtHR can be deduced from a reading of the judgments in question. **[[1]](#footnote-1)**

1. **Will the nemo tenetur principle be compromised?**

First of all, the Court investigates whether there is an infringement of the *nemo tenetur* principle. This investigation divides into two sub-questions.

(1) Is coercion exercised by the government? The Court takes the threat of a criminal sanction into account as coercion. **[[2]](#footnote-2)**The same applies, for example, to a negative inference from a refusal to cooperate. **[[3]](#footnote-3)**

(2) Is the coercion exercised to obtain potentially direct or indirect self-incriminating evidence through the defendant?

However, not every exercise of coercion on the accused with a view to obtaining potentially self-incriminating evidence constitutes a violation of the *nemo tenetur* principle, for example, the taking of DNA material under coercion which the Court has accepted for a long time that there is no violation of the principle**[[4]](#footnote-4)**. A further analysis is therefore required on this point.

1. *Principle*

The ECtHR consistently points out in its case law that the principle of non-incrimination and the right to remain silent are aimed at protecting the accused against unlawful pressure from the government in order to prevent miscarriages of justice and to achieve the aim of Article 6 ECHR (the right to a fair trial).**[[5]](#footnote-5)** According to the Court, the right guarantees in particular the freedom of the accused to remain silent in the context of an interrogation and includes the prohibition to oblige someone to make a statement.**[[6]](#footnote-6)** The *nemo tenetur* principle therefore offers protection in the first place against enforced self-incriminating statements. The Court rightly shows itself to be sensitive to this. The exercise of coercion can indeed give rise to false statements. A confession under torture is the typical example of this. The content of the confession depends entirely on the will of the person making the statements. Coercion can influence the content and thus the "evidence". The risk of affecting the reliability of the evidence and the right to a fair trial is therefore high in this situation. An adequate protection against coerced statements is therefore important. However, this problem does not play a role in the enforcement of a key. Whether the key consists of a series of letters and numbers or of biometric data, there is no risk of making false, incriminating statements about the crime under investigation. **[[7]](#footnote-7)**

In assessing the question whether the *nemo tenetur* principle has been violated, the Court makes a distinction between material that *exists independent of the will of the defendant, to which* the *nemo tenetur* principle would not apply, and *material that exists depending on the will of the defendant.***[[8]](#footnote-8)** This distinction has to be seen, among other things, in the context of the freedom of explanation. The will dependence of the existence of the material must therefore be judged at the moment the coercion is exercised. The evidence still has to *come into* existence at that moment and the existence (and therefore also the content) depends on the will of the accuse**[[9]](#footnote-9)**, as a result *of* which the above mentioned risk of a distorted representation of reality arises *through* the exercise of coercion. Since the enforced key already exists at the moment that it is enforced by means of a decryption obligation, the existence of the key is, among other things, independent of will. The key exists - as mentioned above - independent of the will of the suspect, and the correctness of the communicated key can be checked immediately. There is no risk of distortion of the truth.

The Court itself quotes several examples of material that exists independent of the will of the defendant. It explicitly states that non-incrimination law does not apply to these types of evidence:

"*The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which has an existence independent of the will of the suspect such as, inter alia,* ***documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing****.* ” **[[10]](#footnote-10)**

In the United Kingdom's P.G. and J.H. case, the Court adds the voice print to this list. The Court simply states that the right not to incriminate oneself does not apply to such material. The way in which that voice print was obtained (*in this case* by means of secret recordings) is irrelevant in this respect:

"*In so far as the applicants complained of the underhand way in which the voice samples for comparison were obtained and that this infringed their privilege against self-incrimination, the Court considers that the voice samples, which did not include any incriminating statements, may be regarded as akin to blood, hair or other physical or objective specimens used in forensic analysis and to which privilege against self-incrimination does not apply*." **[[11]](#footnote-11)**

Based on this jurisprudence, it can be defended, among other things, that obtaining under duress biometric data that may be the key to potential evidence (e.g. an iris scan, facial scan, fingerprint or possibly the voice that allows decryption of an IT system or files) is not problematic in the light of the *nemo tenetur* principle.

We don't see why the analysis would be any different for obtaining a key consisting of, for example, a combination of numbers and letters. In that case the key may look like an explanation, but it cannot be equated with an explanation. It is a fixed fact. The risk of undermining the reliability of the evidence, which makes the protection of the freedom of explanation essential, does not play on the level of the enforced key.

Nor is a distinction between the two types of keys justified on the grounds that one does not necessarily depend on the cooperation of the person concerned to obtain biometric data, whereas one does for the combination of letters and numbers. First of all, in order to obtain an iris scan, for example, it seems to us that it is also necessary for the person concerned to cooperate physically (in order not to exercise coercion that is so serious that it quickly becomes humiliating and inhumane and thus constitutes a violation of art. 3 ECHR). The same applies to obtaining urine, exhaled air and voice prints. In Jalloh/Germany, the Court explicitly recognizes that the *nemo tenetur* principle is also not applicable in the case of limited active cooperation of the accused to obtain body material (*see below*).**[[12]](#footnote-12)** Consequently, this cannot justify a distinction between the different types of encryption either.

1. *Exception*

The right to remain silent and the *nemo tenetur* principle may not apply in principle to evidence that exists independently of the will of the accused, but there are exceptions. After all, there is case law available in which the Court decides that the enforcement of evidence that exists independent of the will of the person concerned constitutes an infringement of the *nemo tenetur* principle. This consistently concerns the duty of the accused to provide "material evidence" at the request of the government. **[[13]](#footnote-13)**However, the Court fails to provide clear criteria and above all a clear *reasoning as to* why the *nemo tenetur* principle applies.

More specifically, the Funke/France case involved an obligation for the defendant to hand over documents which the public authorities believed to exist, although they were not sure of their existence. Where they did not succeed in obtaining these documents themselves, they tried by force to persuade the accused to hand over the documents. According to the Court, this constitutes a violation of the right to remain silent and the principle of non-incrimination.**[[14]](#footnote-14)** Also in J.B./Switzerland, the Court is considering an order to hand over documents. Again, the Court seems to attach importance to the fact that the public authorities did not already seem to have knowledge of the existence of the information to be transmitted. In that case, too, the Court of Appeal decided to violate the principle of non-incrimination, without extensive review. Transposed to the decryption order, this could translate into the requirement that first of all it must be demonstrated in a serious manner that the encrypted data and key exist and that the knowledge of that key exists on the part of the defendant (*infra*).

In view of the fact that the Court in Funke/France and J.B./Switzerland explicitly refers to the fact that the existence of the requested documents is uncertain, we believe that the Court considers it important here that the burden of proof may not be reversed.**[[15]](#footnote-15)** In this context, reference is sometimes made to the criterion whether or not the evidence *was obtained* independently of the will of the accused.**[[16]](#footnote-16)** It is and remains in the first instance the task of investigative bodies to trace evidence of crimes and that task may not be shifted to the accused by means of a duty of cooperation. Indeed, the Court often links the right to remain silent to the presumption of innocence.**[[17]](#footnote-17)** By shifting the burden of proof, there is a risk that a person who wants to cooperate but is unable to cooperate (because he does not have the required information), would still be convicted for his lack of cooperation. The risk of undermining the presumption of innocence is therefore high in these situations.

When we apply the Funke and J.B. jurisprudence to the decryption obligation, we first establish that there is in any case no reversal of the burden of proof when the government forcibly performs an iris scan, takes a fingerprint or applies facial or voice recognition to the suspect to decrypt a computer system. The investigative authorities themselves look for every element in the chain of evidence, i.e. the computer system, the key, the encrypted material. The Funke and J.B. courts are therefore not opposed to the coercive extraction of biometric data.

The question then arises as to whether a distinction according to the type of key can justify a difference in protection. A distinction could indeed be justified in principle, for example, because in the case of encryption using biometric data, the veracity of the statement as to whether or not the data subject has the code can be verified immediately. In this context, there is no risk of the presumption of innocence being affected by a conviction based on the refusal to hand over the "key". There are only two reasons for this refusal. Either the suspect does not want to hand over the key (biometric data), in which case he could justifiably be sanctioned if reasons of public interest force him to decrypt it. Or the suspect is unable to hand over the key because his biometric data are not the key. In this case, the suspect can perfectly prove that the computer system or the encrypted data are not decrypted on the basis of his fingerprint, face, voice or eye. If the encryption consists of digits and letters, it is not possible to verify whether the statement that the person concerned does not know the code is correct. Thus, only in the latter case is there a risk that a person would be convicted for lack of cooperation when he may actually not know the code. In this context, the Belgian public prosecutor's office's duty to provide sufficient proof that the person concerned is aware of the key (*above*) is therefore of great importance. This duty removes the reason for different treatment according to the type of key. Moreover, this duty of principle of proof on the part of the public prosecutor ensures that the burden of proof with regard to the potentially criminal element of the "knowledge of the key" (*supra* concerning the possession of child pornography - the point with which one struggles in England) is not reversed either. Also on the basis of the Funke and J.B. jurisprudence, we therefore dare to conclude that the obligation to decrypt the key, whereby the Public Prosecutor's Office must sufficiently demonstrate that the suspect has knowledge of the key, does not violate the *nemo tenetur* principle.

Finally, there is the case of Jalloh/Germany, which concerned the physical coercion of a person (administering an emetic) to obtain drug doses that the person had swallowed. In this case, the Court tries to clarify the scope of the *nemo tenetur:*

*"[The court] notes that the privilege against self-incrimination is commonly understood in the Contracting States and elsewhere to be* ***primarily*** *concerned with respecting the will of the defendant to remain* ***silent*** *in the face of questioning and* ***not*** *to be* ***compelled*** *to provide a* ***statement****. However, the Court has on occasion given the principle of self-incrimination as protected under Article 6 § 1 a* ***broader meaning*** *so as to encompass cases in which* ***coercion to hand over real evidence*** *to the authorities was in issue* [met verwijzing naar Funke/Frankrijk en JB/Zwitserland]*. In Saunders, the Court considered that the principle against self-incrimination did* ***not cover*** *"material which may be obtained from the accused through the use of compulsory powers but which has an existence* ***independent of the will*** *of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing. In the Court's view, the evidence in issue in the present case, namely, drugs hidden in the applicant's body which were obtained by the forcible administration of emetics, could be considered to fall into the category of material having an existence independent of the will of the suspect, the use of which is generally not prohibited in criminal proceedings.* ” **[[18]](#footnote-18)**

The Court goes on to explain why, in this case, despite the fact that it concerns evidence that exists independently of the defendant's will, it considers that the principle of non-incrimination applies. Indeed, there are several reasons why, in the eyes of the Court, the case differs from the examples listed in Saunders:

1. As in *Funke* and *J.B.,* coercion was exercised on the person to obtain material evidence. The body material, listed in Saunders, on the other hand, is material obtained under duress for further forensic examination with a view to determining, for example, the presence of alcohol or drugs. At this point, the question arises as to whether we should understand the decryption duty as a duty to forcibly hand over a key, which in itself does not constitute material evidence, or whether, with the decryption duty, essentially all the underlying data are also provided by the suspect under duress, which obviously constitutes potentially hard evidence. In this second interpretation the obligation to decrypt the key results in a violation of the right to remain silent. That is so independent of the type of key. In this interpretation, by forcibly handing over a code of numbers and letters or by forcibly having a fingerprint or other biometric data taken, the suspect would always hand over all the underlying data as a result of the coercion. However, we do not support this interpretation. Blood, breath or urine is also obtained when blood is taken or in the context of a breath analysis or urine test by coercive exercise on the person of the suspect. With the blood, breath or urine, however, the detectives also obtain the alcohol or drug percentage under coercion, which can also be hard evidence of a crime. We therefore dare to argue that the stricter interpretation in this one is the right one. Through coercion, the key is obtained to potential evidence that the detectives detect themselves, but cannot read. Therefore, the investigators have already detected the computer system or the relevant data themselves, without coercion on the person. Neither the computer system nor the files and data are therefore obtained by coercion on the person. The discovery of evidence always precedes the decryption order and, if necessary, follows it further. It is only when a potentially interesting computer system or data have been identified, located and isolated that an order is issued to make the data found readable. This command relates directly to the detected but encrypted information. If the encrypted information is of a certain size, it will then again be the investigative authorities who, once decrypted, will continue to search the information. In the same way, an order to open a house as part of a search would be different from an order to say where you have hidden the evidence. The decryption order is no more or no less than the digital locksmith.
2. The degree of coercion exerted also differs manifestly from the coercion required to obtain the material listed in Saunders. After all, the latter only requires that the suspect passively undergoes limited interference in his physical integrity or actively cooperates in the supply of material resulting from the normal functioning of the body. For the latter the Court explicitly refers to breath, urine and voice prints. On the other hand, the degree of coercion used in the Jalloh case was such that it even constituted a violation of the prohibition of torture, inhuman and degrading treatment, as prescribed by art. 3 ECHR. In this sense, the Jalloh case is rather a maverick case, since the Court seems to be particularly sensitive to the way in which coercion was exercised. Classically, the nature and degree of coercion only plays a role at the level of a possible justification of an infringement of the right to remain silent (*infra*). What is special about the exercise of coercion in question is that it has eliminated the will and ability to refuse. If one takes DNA, blood or urine with coercion, this coercion relates to the direct taking of material evidence with respect for the freedom and will of the suspect to disagree. In the Jalloh/Germany case, a form of *ricochet coercion* was exercised which consisted of administering a (vomiting) drug and thus breaking the suspect's freedom of will by means of the coercion so that he could no longer prevent his body from spontaneously handing over the evidence (outbreaks). In other words, the body was forced to cooperate spontaneously and moreover in a non-natural way. It resembles the interrogation of a suspect under hypnosis to make him confess.
3. *Conclusion regarding the decryption obligation*

In view of the above, we are of the opinion that on the basis of the case law of the ECHR it is perfectly defensible that the penalized duty to communicate an IT key, in whatever form, does not affect the principle and therefore art. 6 ECHR. The same applies, among other things, to the penalized duty to provide the key itself, since this essentially amounts to the same thing. The duty of the accused to hand in the key himself is even preferable to the duty to communicate the key in view of the in that context more limited interference with the right to privacy and more limited risk of abuse. After all, the password can be the same for several files or systems. **[[19]](#footnote-19)**

Since discussion about the answer to this first question with respect to the obligation to deregulate remains possible in view of the peculiarities of the problem, we will, for the sake of completeness, elaborate on the further analysis of the obligation to deregulate in the light of the *nemo tenetur* principle below. However, the questions discussed below only need to be answered to the extent that the duty of decryption is taken into account as a violation of the *nemo tenetur principle*.

1. ***Is the principle in its essence affected?***

When the Court finds that the *nemo tenetur* principle has been violated, it examines whether the principle has been violated in its essence. Under no circumstances can a violation of its essence be justified (*infra*). Whether there is an impairment of the essence of the principle, the Court assesses on the basis of the following criteria**[[20]](#footnote-20)**: (1) the nature and degree of coercion and questioning, (2) the presence of relevant procedural guarantees, and (3) the extent to which the enforced material is used. We review the three criteria below and apply them immediately to the Belgian decryption obligation. Again, it will turn out that on the basis of current case law it is difficult to predict whether the ECtHR, should it consider that the obligation to decrypt the *nemo tenetur* principle is compromised, will consider it to be an impairment at its core.

1. Serious forms of coercion, such as the threat of severe prison sentences in this case, quickly lead to a violation of the principle at its core. The same applies to broad searches, which constitute a major restriction on the freedom of explanation[[21]](#footnote-21) or a broad order to hand over potential evidence[[22]](#footnote-22). On the other hand, limited searches are less likely to affect the essence of the right to remain silent.[[23]](#footnote-23) In the case of compulsory decryption, only very limited information is requested under duress, i.e. only the key (cf. code, password, login). On the other hand, this key can be used to decrypt a great deal of potential evidence.
2. The presence of relevant procedural safeguards, which mitigate the coercion, are also taken into account by the Court. This concerns, for example, the existence of an opportunity for the defendant to explain why he does not give or cannot give certain information [[24]](#footnote-24)and the hearing about it on the initiative of the authorities.[[25]](#footnote-25) The fact that, under Belgian law, the public prosecutor's office must provide proof of the knowledge of the key of the person concerned is, among other things, important in this respect. In this respect, the Public Prosecutor's Office must sufficiently demonstrate that the person concerned is familiar with the code, obviously taking into account the defence put forward by the accused regarding his knowledge of the key.
3. Finally, the Court takes into consideration the extent to which the enforced material is used. The question is whether the evidence obtained plays an important or limited role in the taking of evidence. If the obligation to provide information or cooperation is limited, and, for example, relates to only one element of the underlying crime, then the use is limited and the Court will rather conclude that the principle has not been affected in its essence. In the context of the decryption obligation, the question again arises as to what exactly should be put on the scales. In principle, the investigative authorities only enforce the acquisition of the key. The key itself does not play a role in the taking of evidence, especially since**[[26]](#footnote-26)** under Belgian law the authorities themselves must first prove that the suspect has the key and therefore has access to the information behind the key. The communication of the key therefore does not imply the potentially incriminating statement that (only) the suspect has access to the encrypted information. That statement in itself could indeed be incriminating. For example, as indicated above, sharing the key could implicitly imply the statement that the suspect has access to child pornography material. This "statement of access" provides evidence of an objective element of the offence of *possession of* child pornography. Once again, however, it can be considered that enforcing the key can make a large amount of information available and readable. The question is then whether this information should be considered as "enforced" as well. If that question is answered in the affirmative, the enforced material does potentially play a major role in the production of evidence. We have already argued why we believe that only the key is enforced, and not the underlying evidence (*supra* ).
4. ***Can the impairment be justified?***

Finally, whether or not there is an impairment at the core of the *nemo tenetur* principle is important for the answer to the third question in the ECHR test: can the impairment be justified by a public interest? After all, an impairment in the essence can never be justified, not even in the context of the fight against the most serious forms of crime. **[[27]](#footnote-27)**

Interesting in this context is the ruling in the O'hallaron and Francis case, which concerns a duty to identify in traffic offences. In order to justify the - limited - coercion exercised, the Court reasoned as follows: *"[a]ll who own or drive motor cars know that by doing so they subject themselves to a regulatory regime. This regime is imposed not because owning or driving cars is a privilege or indulgence granted by the State but because the possession and use of cars (like, for example, shotguns ...) are recognised to have the potential to cause grave injury". Those who choose to keep and drive motor cars can be taken to have accepted certain responsibilities and obligations as part of the regulatory regime relating to motor vehicles, and in the legal framework of the United Kingdom these responsibilities include the obligation, in the event of suspected commission of road-traffic offences, to inform the authorities of the identity of the driver on that occasion. "***[[28]](#footnote-28)**In the context of a decryption obligation, a similar justification may be considered. On the other hand, if we, as a society, put heavy forms of encryption as a general good, something that must be available to everyone in order to pursue maximum data security, users must assume certain responsibilities and obligations in relation to their computer use, including the obligation to hand over the encryption key when ordered in the event of concrete, serious suspicions of a crime.

1. ***Practical considerations***

Finally, the question can be asked about the effectiveness of a decryption order. If not, this practical question is even more difficult to answer than the legal question.

While biometric keys such as fingerprint, *vein recognition***[[29]](#footnote-29)***,* facial recognition, and iris scan typically provide an increased sense of secure encryption, this poses neither legal nor practical problems. If the suspect is caught, acceptable physical coercion can be exerted to see the biometric keys used. This can take the form of, for example, taking the fingerprint *manually militari* or holding the iPhone X in front of the suspect's face. Also, in certain circumstances, for example, prosthetics or duplicates can be made from recovered fingerprints. By the way, this is one of the reasons why the major smartphone developers are gradually switching to *vein recognition,* as this can hardly be reconstructed with a prosthesis.

However, it only becomes really difficult when intellectual keys are used. Thus, the encryption sector flourishes on the argument of *plausible deniability*. For example, Veracrypt reassures every user of its encryption software with the message: "*In case an adversary forces you to reveal your password, VeraCrypt provides and supports two kinds of plausible deniability*: (...)".**[[30]](#footnote-30)**The possibility is built into the software to create digital safes, the so-called *hidden volumes*. For example, if a person suspected of paedophilia is confronted with a decryption order, he simply gives 'a' code that only gives access to a volume containing photos of sunflowers and adult men. *Hidden operating systems are* also offered: "*It may happen that you are forced by somebody to decrypt the operating system. There are many situations where you cannot refuse to do so (for example, due to extortion). VeraCrypt allows you to create a hidden operating system whose existence should be impossible to prove (provided that certain guidelines are followed). Thus, you will not have to decrypt or reveal the password for the hidden operating system*"**[[31]](#footnote-31)** . In principle, such a hidden operating *system* will never even be discovered.

Another problem that seriously complicates investigative practice is that it might even be a bad idea to try the code given by the suspect. Certain apps, software and devices allow the programming of an alternative code - a so-called *kill code* - which, when keyed in, completely erases and blocks the data carrier. It therefore seems appropriate that in case of doubt, a decryption order is issued with a view to obtaining and trying the code and that no action is taken on the basis of a code provided voluntarily. To the extent that a *kill code* is then issued on the basis of the aforementioned order, action can at least still be taken on the basis of §3 of article 88quater of the Code of Criminal Procedure, which provides for the punishability of 'obstructing' the computer search. Trying out a code given voluntarily by the accused should nowadays only be an ultimum remedium.

This makes it clear that in many cases the effectiveness of an order for decryption may leave something to be desired in so far as it serves to establish the objective truth in the investigation in which the order for decryption was issued. On the other hand, it offers a counterbalance to the negative consequences of the freedom of encryption. The refusal to grant access to a data carrier when there is reason to do so is indeed punishable in today's society because it rightly harbours an inherent danger to public security and society. Autonomous criminality also creates the possibility to forfeit data carriers that would otherwise have to be returned, even if there are serious indications that a library of pedopornographic material, for example, is hidden behind the encryption.

1. ***Conclusion regarding the decryption obligation***

The judiciary faces the challenge of rethinking classical concepts in function of the specificity of the digital age. When the Code of Criminal Procedure of 17 November 1808 entered into force on 7 December 1808, it was perhaps not yet considered that there would ever exist places or (storage) spaces that a search warrant and a locksmith would not be able to cope with. Now we are faced with the challenge that free encryption software such as Veracrypt[[32]](#footnote-32) allows files to be put into a virtual safe that can only be opened with a 256-bit encryption key. This software is mainstream, legal and very easy to use. Article 48 of the Act of 13 June 2015 on electronic communications states unequivocally in paragraph 1: "*The use of encryption is free*". If one **[[33]](#footnote-33)**would attempt to crack a 256 bit code with the processing power of 1,000,000 computers each with a 3GHz processor with a processing power of 3 billion calculations per second, one would still be faced with the fact that breaking the code could take 1,223,914,354,360,000,000,000,000,000,000,000,000,000 years. It is an understatement to say that in many situations this is suspiciously like a *safe haven* for digital evidence. Most recently, on 19 July 2018, the Constitutional Court also recalled**[[34]](#footnote-34)** - in the context of the procedure for the annulment of data retention legislation - that human rights also create a positive duty for states under the rule of law to protect their citizens against serious human rights violations. It is not nonsensical, in the given circumstances, to balance the legally enshrined freedom of encryption with other fundamental rights, such as the right to life (Article 2 ECHR), the prohibition of torture (Article 3 ECHR), the right to freedom and security (Article 5 ECHR) and also the right to privacy (Article 8 ECHR). There is therefore a case for the "*O'hallaron reasoning*" that this freedom must necessarily be accompanied by certain responsibilities and obligations of the encryption user to enable law enforcement, including the obligation to decrypt when there are serious indications that the encryption freedom is being abused.

Moreover, Article 17 of the ECHR prohibits provisions of the ECHR from being interpreted as implying a right for a State, a group or a person to engage in any activity or perform any act with the aim of nullifying the rights or freedoms set forth in the ECHR.**[[35]](#footnote-35)** Admittedly, the right to remain silent as an additional hindrance to the breaking of potentially practically unencryptable codes does not yet imply the right to engage in any activity behind that solid encryption wall with the intent to destroy other people's rights or freedoms. Nevertheless, we dare - by way of a club in the henhouse - ask ourselves the question whether accepting the right to remain silent as a ground not to have to decrypt, when the public prosecutor shows that there are serious indications that (1) a data carrier contains evidence of crimes (which would allow victims or perpetrators to be identified and possibly even to stop a crime) and (2) the person concerned knows the decryption key, does not come awfully close to somewhat honouring an abuse of right, *in this case* the abuse of the right to remain silent and the prohibition of self-incrimination outside their respective authentic context and without serving the purpose which it is intended to serve, namely protection against miscarriages of justice and reversal of the burden of proof and the associated risk of conviction of innocents.

**Jan Kerkhofs, Federal Magistrate, Belgian Federal Prosecutor's Office**

**Dr. Charlotte Conings, lawyer, Stibbe Brussels**

1. See for a detailed analysis on the subject, which also serves as inspiration here: C. Conings, *Classical and digital search for criminal evidence,* Antwerp, Intersentia, 554-556. [↑](#footnote-ref-1)
2. ECHR 25 February 1993, No 10828/84, Funke/France; ECHR 17 December 1996, No 19187/91, Saunders/United Kingdom; ECHR 21 December 2000, No 34720/97, Heaney and McGuinness/Ireland; ECHR 21 December 2000, No 36887/97, Quinn/Ireland; ECHR 3 May 2001, No 31827/96, J.B./Switzerland; ECHR 8 April 2004, No 36887/97, Quinn/Ireland; ECHR 3 May 2001, No 31827/96, J.B./Switzerland; ECHR 8 April 2004, No 31827/96, J.B./Switzerland. 38544/97, Weh/ Austria; ECHR 4 October 2005, no. 6563/03, Shannon/United Kingdom; ECHR 29 June 2007, no. 15809/02 and 25624/02, O'Halloran and Francis/United Kingdom; ECHR 14 October 2010, no. 1466/07, Brusco/France; ECHR 5 April 2012, no. 11663/04, Chambaz/Switzerland. [↑](#footnote-ref-2)
3. ECHR February 8, 1996, no. 18731/91, John Murray/United Kingdom; ECHR March 18, 2010, no. 13201/05, Krumpholz/Austria. [↑](#footnote-ref-3)
4. ECHR 17 December 1996, no. 19187/91, Saunders/United Kingdom. [↑](#footnote-ref-4)
5. ECHR 25 February 1993, No 10828/84, Funke/France; ECHR 8 February 1996, No 18731/91, John Murray/United Kingdom; ECHR 17 December 1996, No 19187/91, Saunders/United Kingdom; ECHR 21 December 2000, No 34720/97, Heaney and McGuinness/Ireland; ECHR 21 December 2000, No 34720/97, Heaney and McGuinness/Ireland. 36887/97, Quinn/Ireland; ECHR 3 May 2001, No 31827/96, J.B./Switzerland; ECHR 10 September 2002, No 76574/01, Allen/United Kingdom; ECHR 5 November 2002, No 48539/99, Allan/United Kingdom; ECHR 8 April 2004, No 76574/01, Allan/United Kingdom. 42371/02, Pavlenko/Russia; ECHR 14 October 2010, n° 1466/07, Brusco/France; ECHR 5 April 2012, n° 11663/04, Chambaz/Switzerland; ECHR 31 October 2013, n° 17416/03, Tarasov/Ukraine; ECHR 31 January 2017, n° 40233/07, Kalnéniené/Belgium. [↑](#footnote-ref-5)
6. EHRM 11 juli 2006, nr. 54810/00, Jalloh/Duitsland: "*The privilege against self-incrimination is commonly understood in the Contracting States and elsewhere to be primarily concerned with respecting the will of the defendant to remain silent in the face of questioning and not to be compelled to provide a statement.* ” [↑](#footnote-ref-6)
7. See in this context: ECHR 17 December 1996, no. 19187/91, Saunders/United Kingdom; ECHR 21 December 2000, no. 34720/97, Heaney and McGuinness/Ireland; ECHR 21 December 2000, no. 34720/97, Heaney and McGuinness/Ireland. 36887/97, Quinn/Ireland; ECHR 29 June 2007, Nos 15809/02 and 25624/02, O'Halloran and Francis/United Kingdom; ECHR 18 March 2010, No 13201/05, Krumpholz/Austria; ECHR 31 October 2013, No 17416/03, Tarasov/Ukraine. [↑](#footnote-ref-7)
8. ECHR 17 December 1996, no. 19187/91, Saunders/United Kingdom, §92. The criterion was recently confirmed: ECHR 31 January 2017 , no. 40233/07, § 52: "*Finally, s'agissant du droit de garder le silence et de ne pas contributeren à sa propre incrimination, il n'apparaît pas que la requérante ait, à la différence de l'affaire Allan c. Royaume-Uni (précité, §§ 50-53), fait l'objet de contrainte ou de pression, ni même d'un subterfuge pour lui soutirer des aveux ou d'autres déclarations l'incriminant. On the contrary, the previsions made during the course of the litigious perquisition are material elements that exist independently of the will of the requerante*. The same criterion is also found in the EU Directive on the presumption of innocence (Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, *OJ. L.* 11 March 2016, no. 65), Article 7.3 of which states: "*The exercise of the right not to incriminate oneself shall not prevent the competent authorities from gathering evidence that is lawfully obtained by the use of legal coercion and that exists independently of the will of the suspects or accused persons*"). [↑](#footnote-ref-8)
9. This is confirmed by the fact that the Court itself refers to documents that can be seized by means of an investigation order as material that exists independently of the will of the accused. Although these documents may have been created by the will of the accused in the past, and therefore their existence may have depended on the will of the accused, at the time of the execution this constitutes material that exists independently of the will of the accused. The documents exist, and nothing can change that on the basis of the will of the suspect. [↑](#footnote-ref-9)
10. ECHR 17 December 1996, no. 19187/91, Saunders/United Kingdom, §92. [↑](#footnote-ref-10)
11. ECHR 25 September 2001, no. 44787/98, P.G. and J.H/U.K., § 80. [↑](#footnote-ref-11)
12. ECHR 11 July 2006, no. 54810/00, Jalloh/Germany. [↑](#footnote-ref-12)
13. See ECHR 25 February 1993, no. 10828/84, Funke/France; ECHR 3 May 2001, no. 31827/96, J.B./Switzerland; ECHR 11 July 2006, no. 54810/00, Jalloh/Germany. [↑](#footnote-ref-13)
14. EHRM 25 februari 1993, nr. 10828/84, Funke/Frankrijk: "*The Court notes that the customs secured Mr Funke's conviction in order to obtain certain documents which they believed must exist, although they were not certain of the fact. Being unable or unwilling to procure them by some other means, they attempted to compel the applicant himself to provide the evidence of offences he had allegedly committed. The special features of customs law (see paragraphs 30-31 above) cannot justify such an infringement of the right of anyone "charged with a criminal offence", within the autonomous meaning of this expression in Article 6 (art. 6), to remain silent and not to contribute to incriminating himself*." [↑](#footnote-ref-14)
15. The legislator therefore rightly states that the duty 'to search for certain data' from art. 88quater §2 Sv. is contrary to *the nemo tenetur principle* when it is imposed on the accused. [↑](#footnote-ref-15)
16. See e.g. Corr. Dendermonde November 17, 2014, *NJW* 2016, afl. 336, 132, note C. Conings; D. Dewandeleer, "Crimes and criminal investigations in the IT context" in R. Verstraeten and F. Verbruggen, Criminal and *Criminal Procedure Law,* Bruges, die Keure, 2009-10, (125) 159-160, footnote no. 126. [↑](#footnote-ref-16)
17. ECHR 25 February 1993, No 10828/84, Funke/France; ECHR 8 February 1996, No 18731/91, John Murray/United Kingdom; ECHR 17 December 1996, No 19187/91, Saunders/United Kingdom; ECHR 20 October 1997, No 20225/92, Serves/France; ECHR 21 December 2000, No 34720/97, Heaney and McGuinness/Ireland; ECHR 21 December 2000, No 34720/97, Heaney and McGuinness/Ireland. 36887/97, Quinn/Ireland; ECHR 3 May 2001, No 31827/96, J.B./Switzerland; ECHR 10 September 2002, No 76574/01, Allen/United Kingdom; ECHR 8 April 2004, No 38544/97, Weh/Ukraine; ECHR 19 February 2009, No 16404/03, Shabelnik/Ukraine; ECHR 31 October 2013, No 17416/03, Tarasov/Ukraine. [↑](#footnote-ref-17)
18. ECHR 11 July 2006, no. 54810/00, Jalloh/Germany, §110-113. [↑](#footnote-ref-18)
19. Explanatory report to the Cybercrime Convention of 23 November 2001, http://conventions.coe.int/Treaty/EN/Reports/html/185.htm, § 202; Report on behalf of the commission, *Parl.St.* Senate 1999-2000, no. 2-392/3, 69-70. [↑](#footnote-ref-19)
20. ECHR 5 November 2002, No 48539/99, Allan/United Kingdom; ECHR 11 July 2006, No 54810/00, Jalloh/Germany; ECHR 29 June 2007, No 15809/02 and No 25624/02, O'Halloran and Francis/United Kingdom; ECHR 10 January 2008, No 54810/00, Jalloh/Germany; ECHR 29 June 2007, No 15809/02 and No 25624/02, O'Halloran and Francis/United Kingdom; ECHR 10 January 2008, No 54810/00, Jalloh/Germany. 58452/00 and 61920/00, Lückhof and Spanner/Austria; ECHR 10 March 2009, no. 4378/02, Bykov/Russia; ECHR 1 April 2010, no. 42371/02, Pavlenko/Russia; J. Meese, "*Th e sound of silence.* The right to silence and the *nemo tenetur principle* in criminal cases. A historical and comparative overview" in J. Rozie, S. Rutten, A. Van Oevelen (eds.), *Zwijgrecht versus spreekplicht,* Antwerp, Intersentia, 2013, (37) 41. [↑](#footnote-ref-20)
21. ECHR 17 December 1996, No 19187/91, Saunders/United Kingdom; ECHR 21 December 2000, No 34720/97, Heaney and McGuinness/Ireland; ECHR 4 October 2005, No 6563/03, Shannon/United Kingdom. [↑](#footnote-ref-21)
22. Zie bijvoorbeeld EHRM 25 februari 1993, nr. 10828/84, Funke/Frankrijk*,* overweging nr. 30: "*production of papers and documents of any kind relating to operations of interest to their department*"; EHRM 3 mei 2001, nr. 31827/96, J.B./Zwitserland, overweging 39: "*documents etc. which might be relevant for the assessment of taxes*"; EHRM 5 april 2012, nr. 11663/04, Chambaz/Zwitserland: "*les livres, documents et pièces justifi catives se trouvant en sa possession et* [...] *attestations et états présentant de l'importance pour sa taxation.* ”. [↑](#footnote-ref-22)
23. ECHR 29 June 2007, nos. 15809/02 and 25624/02, O'Halloran and Francis/United Kingdom; ECHR 10 January 2008, nos. 58452/00 and 61920/00, Lückhof and Spanner/Austria. [↑](#footnote-ref-23)
24. ECHR 29 June 2007, nos. 15809/02 and 25624/02, O'Halloran and Francis/United Kingdom; ECHR 10 January 2008, nos. 58452/00 and 61920/00, Lückhof and Spanner/Austria. [↑](#footnote-ref-24)
25. ECHR 18 March 2010, no. 13201/05, Krumpholz/Austria. [↑](#footnote-ref-25)
26. EHRM 29 juni 2007, nrs. 15809/02 en 25624/02, O'Halloran en Francis/Verenigd Koninkrijk: i.v.m. een plicht tot identificatie van de persoon die het voertuig bestuurde op het ogenblik van een verkeersmisdrijf: "*the identity of the driver is only one element in the offence of speeding, and there is no question of a conviction arising in the underlying proceedings in respect solely of the information obtained as a result of section 172(2)(a)*". Zie in dezelfde zin: EHRM 10 maart 2009, nr. 4378/02, Bykov/Rusland, overweging 103: "*it played a limited role in a complex body of evidence assessed by the court*". [↑](#footnote-ref-26)
27. ECHR 17 December 1996, No 19187/91, Saunders/United Kingdom; ECHR 21 December 2000, No 34720/97, Heaney and McGuinness/Ireland; ECHR 21 December 2000, No 36887/97, Quinn/Ireland; ECHR 10 March 2009, No 4378/02, Bykov/Russia, recital 93: "*Th e general requirements of fairness contained in Article 6 apply to all criminal proceedings, irrespective of the type of offence at issue. Public interest concerns cannot justify measures which extinguish the very essence of an applicant's defence rights, including the privilege against self-incrimination guaranteed by Article 6 of the Convention.* ”. Although the Court of Appeal does not always clearly distinguish between the three different questions, the assessment of a possible justification can only follow after it has been established that there is no violation of the *nemo tenetur* principle at its core. Taking the public interest into consideration in step two would completely undermine the *nemo tenetur* principle because a large public interest could even justify serious forms of coercion. See also the *dissenting opinions* of Judge Pavlovschi and Judge Myjer at ECHR 29 June 2007, nos. 15809/02 and 25624/02, O'Halloran and Francis/United Kingdom; C. Conings, *Classical and digital search for criminal evidence,* Antwerp, Intersentia, 549-550. [↑](#footnote-ref-27)
28. ECHR 29 June 2007, nos. 15809/02 and 25624/02, O'Halloran and Francis/United Kingdom, §57. [↑](#footnote-ref-28)
29. Zie <https://www.bayometric.com/fingerprint-vs-finger-vein-biometric-authentication/> [↑](#footnote-ref-29)
30. <https://www.veracrypt.fr/en/Plausible%20Deniability.html> [↑](#footnote-ref-30)
31. <https://www.veracrypt.fr/en/Hidden%20Operating%20System.html> [↑](#footnote-ref-31)
32. [www.veracrypt.fr](http://www.veracrypt.fr)  [↑](#footnote-ref-32)
33. *Brute force* is often used to [crack](https://nl.wikipedia.org/wiki/Cracken) [passwords](https://nl.wikipedia.org/wiki/Wachtwoord) or retrieve lost or forgotten passwords that are encrypted with strong [encryption](https://nl.wikipedia.org/wiki/Encryptie). It tries all possible combinations of available characters. [(https://nl.wikipedia.org/wiki/Brute\_force\_(method)](https://nl.wikipedia.org/wiki/Brute_force_(methode))) [↑](#footnote-ref-33)
34. Constitutional Court, July 19, 2018, judgment no. 96/2018, recital B.22: "*The contested law also aims to enable an effective criminal investigation and punishment of sexual abuse of minors and to make it effectively possible to identify the perpetrator of such a crime, even when electronic means of communication are used. At the hearing, reference was made to the positive obligations that follow from Articles 3 and 8 of the European Convention on Human Rights regarding the protection of the physical and moral integrity of minors and other vulnerable persons, as interpreted by the European Court of Human Rights (ECHR, 2 December 2008, K.U. t. Finland, §§46-49). (…)*” [↑](#footnote-ref-34)
35. For example, very recently - on 24 May 2018 - in the case of *ROJ TV t/Denmark, the* ECtHR ruled unanimously that the complaint had to be rejected as inadmissible on the grounds of Article 10 ECHR (freedom of expression) of ROJ TV for abuse of rights within the meaning of Article 17 ECHR. Thus, the ECtHR cannot abuse the freedom of expression to support terrorist activities and carry out terrorist propaganda. The Court of Appeal considered the following (ECHR 24 May 2018, no. 24683/14, ROJ TV/Denmark):

    *"“47. Consequently, the Court finds that, taking firstly account of the nature of the impugned programmes, which included incitement to violence and support for terrorist activity, elements extensively examined by the national courts, secondly, the fact that the views expressed therein were disseminated to a wide audience through television broadcasting and, thirdly, that they related directly to an issue which is paramount in modern European society - the prevention of terrorism and terrorist-related expressions advocating the use of violence - the applicant company's complaint does not, by virtue of Article 17 of the Convention, attract the protection afforded by Article 10.*

    *48. Having regard thereto, the Court considers that the applicant company is attempting to deflect Article 10 of the Convention from its real purpose by employing this right for ends which are clearly contrary to the values of the Convention. Consequently, the Court finds that, by reason of Article 17 of the Convention, the applicant company may not benefit from the protection afforded by Article 10 of the Convention."* [↑](#footnote-ref-35)