PRIVILEGE AGAINST SELF- INCRIMINATION IN RELATION TO JURISPRUDENCE WITH SPECIAL REFERENCE TO EUROPEAN COURT OF HUMAN RIGHTS IN DIGITAL ERA

Abstract

In this Article, the privilege against self-incrimination is analyzed, with the data encryption in digital gadgets and the complexity involved, the author attempts to base his in-depth analysis on the jurisprudence of the European Court of Human Rights case laws regarding self-Incrimination. Taken into consideration the reasoning drawn from the various cases brought before the European Court of Human Rights, the author tried to analyse cases such as forcing a person to produce a decryption key or self-decrypting information and subsequently submits the content in a readable format. The conclusion was that the privilege against self incrimination also applies to the context of encryption / decryption of computer data. The author also attempted to settle the question of the scope of the privilege in the sense that it precludes coercion to active cooperation.

Keywords: self-incrimination, encryption, decryption, encryption, European Court of Human Rights.

Author

Jyothi Abraham
Department of Law
School of Indian Legal Thought
Mahatma Gandhi University
Kerala, India.
jyothiphd2016@gmail.com

I. INTRODUCTION

In this chapter we will look at some aspects related to the encryption and decryption of computer data and the relationship between these activities and the privilege against self-incrimination.[1] In this regard that the doctrine has completely ignored this technical-legal problem, which is why we see as a doctrinal foray into this area is necessary and opportune. As far as we are concerned, ignoring this subject by the literature is a big minus, in the context in which the encryption of computer data is used more frequently. Since the legal issue already exists, it is possible at any time that the practice domestic judiciary to confront it. However, the absence of serious and relevant legal debate may result in the shaping of a judicial practice domestic judiciary that was not unitary or even contrary to the privilege against self-incrimination. As a personal note, the relationship between the privilege under analysis and the encryption of computer data. It has been subject of personal reflection for years. Thus, beyond the existing relationship between the privilege against self-incrimination and cryptography, after a thorough study we were able to become aware of true, the gray area in which this privilege lies. Consequently, what we set out to do was to try to we put as much order as possible in an area where contradictions and logical bits are the rule and by no means the exception.[2] It remains to be seen whether this chapter will open the door to legal debates in the doctrine of autochthonous. As regards the structure of this chapter, beyond an analysis of the privilege against self-incrimination, including by reference to the case- law of the European Court of Human Rights (hereinafter ECtHR or Court) in the matter, I will focus on five different hypotheses of encryption/ decryption, namely:

1. When the encryption/decryption key is represented by a password that is not found on a material support (this exists only in the memory of a person);
2. When the encryption/decryption key is represented by a password that is printed on a material support (eg. Handwritten writing);

[1] Sometimes, in the case-law of the European Court of Human Rights or in the specialized literature, there is a dissociation between the remain silent and the privilege against self-incrimination. Even if a differentiation could be made, it is rather one of nuance, and we see no partical relevance in referring to these notions as two different concepts, although in essence they cover aspects similar. For a similar opinion one can see; R. Chirita, *The right to silence and the privilege against self-incrimination*, 4 Notebooks of Criminal Law, 57 (2006). The opposite view is that the privilege against self-incrimination places an obligation negative task for the State, namely not to compel a person to provide evidence that could lead to the incrimination of whereas the right to remain silent refers to the possibility for judicial bodies to draw conclusions from the silence of the person in to its detriment see in this regard M. Udroiu, O. Predescu, *European Protection of human rights and the Romanian Criminal Process Treatise*, 664 Ed. C.H Beck, Bucharest (2008). Even from this perspective, we do not see why the right to remain silent should not represent a component of the privilege against self-incrimination. Whether the right to remain silent would concern only the refusal to make a statement and the conclusions reached unfavourable because we are not in the presence of a refusal to make statements. As far as we are concerned, in so far as the two notions are intertwined or an intrinsic link is revealed between them, these absurd consequences are removed, or at least. For a discussion regarding these two notions, we can also see: V. Puscasu, THE PRESUMPTION OF INNOCENCE, 192-193 (Ed. Universal Juridic, Bucharest 2010).

[2] For a new monograph on the issue of the right to silence and privilege against self-incrimination, see; V. Puscasu, *the right to silence and non-self-incrimination*, Universal Juridic, Bucharest, (2015). Although the work requires to be praised in terms of documentation and analysis, it is noted that it insists on issues already considered as traditional in this area. Thus, although we do not deny the need for such occurrences in order to clarify some basic aspects we feel that what is missing is the detachment at some point from the traditional and the anchoring of analysis in matters which will certainly become highly controversial in the future. We consider in this aspect that it is more efficient to prevent certain controversies or a non-unitary practice at the level of judicial bodies than trying to solve them post-factum.

3. When the decryption key is stored on a computer data storage medium USB, stick, SD Card, CD or DVD etc;
4. Where decryption is carried out by means of biometric elements (e.g; papillary of the user of the computer system or his/her voice);
5. When the direct decryption of computer data is requested and their transmission in an accessible/ readable format.

II. THE IMPORTANCE OF ENCRYPTION AND DECRYPTION

We do not want to dwell on technical aspects related to encryption or decryption of computer data, our analysis looks only at the legal aspects related to the applicability of the privilege against self-incrimination in this matter. When we refer to certain technical aspects, we will do it to highlight certain elements that may be relevant from the perspective of legal analysis. However, we still consider it appropriate to delve into the topic of encryption and decryption the little from the perspective of the consequences it generates in a criminal investigation. First, contrary to the established opinion in judicial practice, the use of cryptography is not a element intended per se to suggest criminal conduct. When we talk about encrypting some data the focus should be on data protection and not on concealing criminal behaviour. This is because IT data protection can also be successfully achieved through the process encryption. This does not mean that this process is always aimed at concealing illegal content of that data, content that could suggest criminal conduct, but rather that it is desired protecting content from unauthorized persons. The fact that some people end up using this process to hide behaviours. Crime is only the exception such exceptions should not lead to a rebuttal of the presumption of innocence by establishing a rebuttable or absolute presumption that what is encrypted is and incriminating. I consider that such a presumption is totally unreasonable, which should be attract a sanction from the perspective of the right to a fair trial.

Encryption is therefore an appropriate means for storing computer data in a secure environment many people may even use encryption without knowing it for example, by using https protocol (https;//www.google.com) instead of HTTP when accessing some web pages. Anyone who comes to question this conclusion must realize that in this in the age of technology, each individual's private life is not stored only in the memory of each individual or those close to him but also in a saddle of computer systems or means of storing computer data. Also it requires acceptance that only aspects of private life images are not notorious that a careful analysis of the means of storage of computer data such as access codes to different platforms or online services e-mail, virtual stores, internet banking, etc thus generating the risk of shaping significant property damage, identity theft, economic espionage etc.[3]

Last but not least, not only computer data related to private life are stored in virtual environment it is common for certain persons to store computer data related to their professional activity, including on computer systems held in my name or personal interest. It is also possible that computer data stored is of national interest for example, in the case of a receiver or liquidator. For protecting this data encryption is a solution that cannot be ignored otherwise theft of a computer system or of a storage medium involves not only a loss of

[3]Vezi S.M Oltmann, *Encryption and Incrimination: The Evolving Status of Encrypted Drives*,40(2) Bulletin of the Association for Information Science and Technology 22 (2014).

assets but also a loss of control over data important IT from a personal, professional or even national security perspective.

From this point of view, encryption of computer data is beneficial to any individual or legal entity. By way of example, in Law no. 11/1991 on combating unfair competition the trade secret is defined in Article 1 (b) as;

"information which, in whole or in the exact connection of its elements,it is not generally known or easily accessible to people in the environment that normally deals with thistype of information and which acquires commercial value by being secret and the holder has taken actionreasonable, having regard to the circumstances, to keep it secret; Protection of trade secretoperate as long as the conditions set out above are fulfilled'.

To the extent that the information under analysis does not meet the definition of trade secret, the offences referred to in Art. 5 of Law nr. No 11/1991 cannot be applied. The definition of trade secret becomes the central element, therefore, as regards the scope of the incriminating texts relating to unfair competition envisaged by this law. As can be seen, a positive condition for the qualification of information as a trade secret is that its holder takes reasonable steps, having regard to the circumstances, in order to keep it secret. The same problem can be identified in the context of the transmission of trade secrets through a wireless network, whether secure or unsecured. Given the possibility of interception. The question arises to what extent the trade secret holder has or does not have a positive obligation transmit computer data in an encrypted format.

Beyond that, at the level of clarity and predictability, this positive condition imposed by the legislator. It leaves something to be desired, the question may arise to what extent, under certain circumstances, the holder of the information would not have the duty to use encryption in order to keep the content of computer data secret. We can imagine an example where trade secrets were stored on computer systems that they are to be replaced by more efficient ones. To the extent that these systems fall outside the control of the trade secret holder is questioned to what extent encryption was required before formatting existing partitions on the storage means related to the computer system. As far as only calling is made in case of logical deletion or formatting, it is possible to recover computer data by means and procedures specific technical. The question therefore arises of what reasonable measures had to be taken in context in order to preserve secret trade secret regime.

I have referred to these examples to reinforce that encryption is first and foremost a means of protection. We even note that, in the context of Law no. 11/1991, if we were to accept the fact that in Under certain circumstances encryption is a reasonable measure of protection becoming a legal obligation. However, we accept that beyond these positive aspects, encryption is also an effective anti-forensic mechanism,[4] likely to hinder a criminal investigation or even hinder it everything. Considering the fact that the encryption process is within anyone's reach, no knowledge required advanced technical, some people may use this process to hide their own conduct Criminal.

[4] The concept of anti-forensic, as the name suggests, encompasses those techniques or procedures that make it difficult or difficult impossible research, identification and obtaining of traces or digital evidence.

This is also the premise that supports the need for a serious debate on the possibility of forcing / coercing a person to decrypt computer data in order for them to be accessible to judicial bodies. Although there are technical means by which this mechanism of protection (the use of brute force or dictionary attacks), these are generally not feasible in the extent to which the encryption / decryption key is strong and the encryption was full disk encryption.[5]To the extent that the encryption process concerned only certain files (file encryption), recovery.The content is made possible by identifying fragments of those files in an unencrypted form (for example, it is possible to create temporary files that are not subject to encryption).[6]

III. PRIVILEGE AGAINST SELF-INCRIMINATION IN RELATION TO JURISPRUDENCE EUROPEAN COURT OF HUMAN RIGHTS

The privilege against self-incrimination is appreciated in the literature as lacking clarity.[7] In essence, it places certain restrictions on criminal investigation in that an individual has the possibility not to provide judicial bodies with the information requested and which could be used against him.[8] However, a careful analysis of this privilege including in relation to ECtHR case-law on the matter shows that at the level of Content and implicitly at the level of scope, things are not entirely clear. The fact that respect for this privilege has become an implicit requirement for respect for the right to a fair trial (Article 6 of the Convention) in the light of ECtHR case-law is free of any controversy; see, to that effect, Funke v. France, Saunders v. the United Kingdom, etc. Such a conclusion is immaterial if the actual applicability of the privilege encounters problems.

1. **The Rationale For Privilege Against Self-Incrimination:** For my part, the analysis of the scope of the privilege should be premised on identifying precisely why the privilege in question is an important component of the right to a fair trial.[9] However, we note that even on this point, the Court has failed to resolve the issue and opinions in the literature are as divergent as possible.[10] For example, although the ECtHR introduced the privilege against self-incrimination into the content of the right to a fair trial in Funke v. France,[11] no clarification has been made as to the extent of the privilege, its origin or reason.[12] This lack of argumentation is all the more objectionable since the Funke case found a violation of Art. 6 of the Convention, although the coercion to cooperate concerned the surrender of bank documents, a hypothesis which required, in my view, a broader analysis from which the reasoning on which that solution was reached would clearly emerge. If the privilege against self-incrimination is strictly aimed at the proper administration of

[5]S. Lowman, *The Effect of File and Disk Encryption on Computer Forensics*, 7 (2010), http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf (last accessed on 22nd June 2023).
[6] See an analysis to this effect in E. Casey et al., *The growing impact of full disk encryption on digital forensics,8*Digital Investigation, 129 (2011).
[7]M. Redmayne, *Rethinking the Priviledge Against Self-Incrimination*, 27 (2) Oxford Journals of Legal Studies 209 (2007).
[8] Ibid.
[9] V. Pușcașu, *supra note* 2 at 195.
[10] For a brief analysis of this issue in the literature, see R. Chirița, s*upra note*2 at 58.
[11]State of play: customs authorities asked Funke to hand over documents relating to his bank accounts in the last three years. For his refusal to cooperate, he was sentenced to fines.
[12]Vezi şi A. Ashworth, *Self-Incrimination in European Human Rights Law – A Pregnant Pragmatism*? 30 Cardozo Law Review,753 (2008-2009).

justice and finding out the truth by preventing miscarriages of justice (the miscarriage of justice being, for example, mentioned in John Murray v. United Kingdom – para. 49), at first sight, it could be argued that forcing a person to provide the key to decrypting computer data to the authorities or to carry out the decryption act himself does not prejudice this privilege. Thus, while in the matter of statements made in violation of this privilege their reliability can be called into question as a result of the exercise of coercion, in the matter of decryption of computer data the situation differs considerably. This is because, unlike statements made before judicial bodies, the content of computer data is pre-existing at the time of coercion. In this respect, the obligation to submit documents resembles the obligation to decrypt or provide the key to decrypt computer data. Thus, it could be argued that there is an objective element capable of proving beyond any doubt that finding out the truth and, implicitly, the proper administration of justice is not affected. As far as I am concerned, although the privilege against self-incrimination is also meant to protect the credibility of the evidence obtained, which is aimed at preventing miscarriages of justice, the rationale for privilege under consideration.

It is not be just this obtaining a statement, through the use of coercive means, resulting in self-incrimination of the person on whom coercion is exercised should be considered by plan to be incompatible with the right to a fair trial. Thus, in Saunders v. United Kingdom,[13] the Court held as a matter of principle that the privilege against self-incrimination is closely linked to the presumption of innocence,[14] which is why it is necessary for the prosecution to construct its criminal charge without using evidence obtained as a result of coercive or oppressive means. Exactly the same conclusion is found in Marttinen v. Finland. Therefore, we consider it irrelevant whether the statement offered is one in accordance with objective reality or a false one, inappropriate to the truth. In my view, only the means by which this declaration was obtained is relevant – if this means involves some form of coercion on cooperation on the part of a person, the privilege must find its applicability.

However, given that the privilege against self-incrimination has acquired the fame it enjoys today, including due to the fact that it aims to protect the proper delivery of justice by hindering the possibility of judicial bodies to distort the truth, I consider it necessary to point out on a certain aspect, including in relation to this issue. Thus, although computer data possibly incriminating do not undergo changes as a result of self-incrimination by transmitting the key for decryption or decrypting them directly, this does not mean that finding out the truth cannot suffer. Suppose a person is investigated for committing the crime of child pornography, and there are indications that child pornography material is stored on his computer system. To the extent that the information system is encrypted and the authorities do not have access to computer data, in the absence of other elements to prove beyond reasonable doubt the existence of the constituent elements of the crime and the guilt of the suspect, criminal liability will be

[13] Saunders was required to participate in a series of interviews before inspectors appointed by the Department of trade and industry under sections 434 and 436 of the companies Act 1985, in case of refusal there is a rick of liability for contempt of court. Sauders cooperated with inspectors and his statements were used in criminal proceedings against him resulting in a conviction for several crimes.

[14] The same opinion in P. Mahoney, *Right to a Fair Trial in Criminal Matters Under Article 6 E.C.H.R.*,4(1) Judicial Studies Institute Journal, 121, (2004).

unlikely. In this context, it is obvious that potentially incriminating computer data can constitute evidence in the prosecution only to the extent that they are to be decrypted.

Let us suppose, however, that although there is such pornographic material on the suspect's computer system, he is not guilty of committing the crime of child pornography because; A third party has "planted" such computer data on his system or they have been copied by fault by the agent. To the extent that the suspect is asked for the key to decrypt computer data, and he, although he knows that he is innocent, is aware of the risk that such pornographic materials may exist on his system, the question arises to what extent there is or is not the concrete possibility that finding out the truth will suffer as a result of the decryption of computer data.

Finally, making a statement by means of coercive means to the effect that the suspect was at the scene of the act may affect the principle of finding out the truth even if that circumstance corresponds to reality, in so far as the establishment of that fact gives rise to a presumption even a relative one that it was that person who committed the offence. If the accused person is put in the situation of having to rebut a presumption formed as a result of coercion to collaborate, an imbalance is created that we see as totally problematic from the perspective of the right to a fair trial. In this situation, although coercion has not resulted in a statement that does not correspond to the truth, the way it is used/interpreted violates this principle.

In conclusion, domestic law presents some additional guarantees in relation to the Convention, which is why any conclusion to the detriment of the suspect or defendant, starting from his silence is strictly prohibited. Saunders was required to participate in a series of interviews before inspectors appointed by the Department of Trade and Industry under sections 434 and 436 of the Companies Act 1985, in case of refusal there is a risk of liability for the contempt of court. Saunders cooperated with inspectors and his statements were used in criminal proceedings against him that resulted in a conviction for several crimes.

Art. 6 of the Convention they can provide an appropriate scope of applicability to the privilege. In this respect, we are not necessarily talking about a restriction of the privilege against self-incrimination in domestic law, by reference to the provisions of the Code of Criminal Procedure, but rather it is necessary to interpret them appropriately. As far as witnesses are concerned, the conclusion is different. Thus, unlike suspects or defendants, witnesses do not enjoy the privilege of self-incrimination. They are obliged to cooperate with judicial bodies under penalty of liability for the crime of perjury or obstruction of justice. Their benefit is that the declaration and only this one cannot be used directly in the event of changes in standing. From this point of view, domestic law may be invalidated by the direct application of Art. 6 of the Convention. A reform of witness guarantees would be necessary and a starting point could even be art. 116 of the draft of the new Code of Criminal Procedure. The witness must either enjoy derived immunity or have the option of invoking the privilege against self-incrimination under identical conditions as the suspect or defendant. Furthermore, where the risk of self-incrimination appears obvious, judicial authorities should be obliged to inform the witness of the options for which he has at his disposal.

2. **Procedures In Which The Privilege Against Self-Incrimination Is Applicable:** It is beyond doubt that in criminal proceedings the privilege against self-incrimination can find its application, the question being only what its content and scope are. In Saunders, the coercion took place in a procedure considered to be administrative in nature,[15] which is why the Court held that the applicant was obliged to cooperate with the authorities.[16] However, the subsequent use of information obtained as a result of coercion in criminal proceedings calls into question respect for the privilege against self-incrimination. Thus, had there been a refusal in Saunders to cooperate with the authorities, the applicant's conviction for that refusal (in this case, contempt of court) would not have resulted in a violation of the privilege against self-incrimination because the product in question was assessed as purely administrative.[17]

It therefore follows that the applicant should have enjoyed immunity with regard to information obtained in the administrative proceedings, which cannot be used against him in criminal proceedings. Their use in such a trial led to the activation of the privilege against self-incrimination, the Court finding that the administration in criminal proceedings of statements obtained as a result of coercive means contravenes art. 6 of the Convention.

This view was made much clearer in IJL, GMR and AKP v. United Kingdom (see paras. 100-101), the plaintiffs being the other defendants in Mr Saunders' trial. The Court held that obtaining information as a result of coercion does not entail a violation of art. 6 of the Convention, but their subsequent use in criminal proceedings. The essential element is therefore to identify the nature of the procedure by reference to the time when the provisions of article 6 of the Convention shall become applicable. Where coercion is the subject of a criminal rather than administrative investigation, the violation of the privilege against self-incrimination occurs from the moment the statement of coercion is obtained, even if it occurs in the early stages of the proceedings (Heaney and McGuiness v. Ireland).[18]

As far as we are concerned, including in the prosecution in rem, the "perpetrator" can invoke the privilege against self-incrimination although he does not formally have the status of suspect or defendant. In this respect, I consider the reform brought about by Code of Criminal Procedure to be deeply objectionable. Thus, by giving up the preliminary documents, it was desired to avoid slippages through which evidence was obtained outside the criminal trial. However, at present, the prosecution has the possibility to administer evidence during criminal prosecution in rem attempting to deprive of any

[15] See also Abas v. Netherlands, Allen v. United Kingdom and King v. United Kingdom. In all these cases it was found that Art. Article 6 of the Convention has not been violated. However, in King's case it can be argued that the applicant was not convicted of refusing to cooperate but of failing to fulfil his tax obligations in relation to the declaration of income. We appreciate that this nuance is extremely important.

[16] It is important to note, however, that in a concurring opinion, Judge Morenilla held that Art. Article 6 of the Convention was violated from the outset, regardless of how statements taken as a result of coercion were subsequently used.

[17] See also Kansal v. United Kingdom, which concerned bankruptcy proceedings in which Kansal was ordered to declare certain matters which had been used against him in subsequent criminal proceedings.

[18] State of affairs: the applicants were suspected of committing terrorist offences and were therefore arrested and questioned about their whereabouts at the time of the offences. For refusing to cooperate with judicial bodies, they were sentenced to 6 months in prison.

procedural guarantees the person who is subsequently to acquire the status of suspect in question. Such an approach can only be a superficial reform that makes it even more difficult much the possibility of invoking in the preliminary chamber the violation of the right to a fair trial.

Identification of the nature of the investigation in which some form of coercion has been exercised it is also a sensitive subject. For example, in Shannon v. United Kingdom, the Court found violation of the privilege against self-incrimination in the context in which the applicant refused to participate in an interview with tax inspectors on the grounds that he did not receive a guarantee that the information provided did not will be used against him in criminal proceedings.[19] In order not to conflict with what was stated in the IJL case, GMR and AKP v. United Kingdom, the Court held that in Shannon the essential element was that the applicant was to be interviewed on matters already subject to proceedings criminal offences in which he was accused of committing several economic crimes.

In other words, it follows that, although the nature of the interview could be regarded as administrative, having regard to the existence of criminal proceedings concerning the matters to be interviewed, the privilege against self-incrimination becomes applicable.[20] As far as we are concerned, such a distinction between Shannon and IJL, GMR and AKP v. United Kingdom are rather based on the risk that the information obtained as as a result of coercion to be used subsequently in criminal proceedings. Risk what was also highlighted in Marttinen v. Finland (para. 73). Such reasoning, however, puts in discussion of the Opinion in Saunders and IJL, GMR and AKP v. United Kingdom, since It is difficult to accept that this risk was not quite obvious in these cases.[21]

These examples, which suggest a lack of coherence in ECtHR jurisprudence, are only the first from a long series of worrying examples in terms of the fact that instead of responding to certain questions are generated other question marks. However, I consider that it has been accepted by the Court that it is not absolutely necessary that at coercion to have a criminal charge against a person, the privilege of which may be applicable even in those situations where such an accusation can be anticipated. That conclusion is apparent inter alia Weh v. Austria (para. 53) and Reig v. Austria (para. 30). Thus, in these cases the Court relied on the fact that there were no pending criminal proceedings at the time of coercion or anticipated against plaintiffs. Including in the Funke case, although a violation of Art. 6 of Convention, there was no criminal proceeding pending against the

[19] Marttinen v. Finland para 70.
[20] A. Ashworth,*Self-Incrimination in European Human Rights Law - A Pregnant Pragmatism*?30 CARDOZO L. REV. 751 (2008-2009).
[21] M. Berger, *Self-incrimination and the European Court of Human Rights: Procedural Issues in the Enforcement of the Right to Silence,* 4 European Human Rights Law Review, 520-525, (2007). This discussion is particularly relevant in relation to domestic law, since it follows from judicial practice that that reports of tax evasion come almost unanimously as a result of the work carried out by inspectors Anti-fraud. According to art. 4 of Law nr. 241/2005 "constitutes an offence and is punishable by imprisonment from one year to 6 years refusal unjustified of a person to submit to the competent authorities legal documents and patrimony assets, in order to prevent financial, fiscal or customs checks, not later than 15 days after the notice".

applicant.[22] And in this case, the fact that such the procedure that could have been anticipated was sufficient to establish the applicability of Art. 6 of the Convention, reported to the privilege against self-incrimination.

3. **Extent Of The Privilege In Relation To The Object Of The Coercion:** As we mentioned at the beginning of this chapter, there are several hypotheses in which a person can coerced into cooperation in order to decrypt computer data. Therefore, it is necessary to analyze how which ECtHR case-law can be related to these assumptions.

- **Regarding the handing over of documents:** The fact that the obligation to provide certain documents to the authorities also falls within the scope of application of the privilege against self-incrimination in relation to art. 6 of the Convention is evident from the case-law of Court. If the obligation to provide certain documents would be beyond the scope of the privilege subject. The Funke case would not have found a violation of the right to a fair trial.[23]

  In my view, it is not the object of coercion that is central to the applicability analysis privilege against self-incrimination, but the manner in which coercion is carried out.[24] Therefore, throughout this chapter, we have repeatedly referred to the phrase "coercion to cooperate". We support this view because, in Saunders, there is an apparently problematic point which appears to exclude documents from the scope of the privilege. The Court has thus held that the essence of the privilege against self-incrimination is to respect the will of the accused to remain silent. Accordingly, the Court concluded that material which can be obtained by coercive means but which has an independent existence by the will of the accused (e.g. documents obtained by means of a warrant or biological evidence) are covered by this privilege. Such a conclusion would reveal a conflict between the conclusion in Funke and those held in Saunders, on the ground that the documents requested may have an existence independent of the will of the accused.

  Some might argue that, in Saunders, the Court drew a distinction between 'real' evidence (documents, biological samples, etc.) and those obtained as a result of a declaration or by providing oral information (testimonial evidence).[25] In doing so, it could be judged that the "real" evidence obtained as a result of coercion does not provide applicability to the privilege against self-incrimination, unlike coercion to provide an oral statement or information that does not have an existence independent of the will of the person who was coerced.[26] I do not wish to dwell on all this 'real' evidence to which the Court seems to refer.[27] I would merely like to point out that, as far as I am concerned, such a conclusion is erroneous. It is objectionable in firstly, because it seems absolutely excessive to give the state the possibility of forcing a

[22] M. Berger, *Europeanizing Self-incrimination: The Right to Remain Silent in the European Court of HumanRights*, 12 Columbia Journal of European Law, 350 (2006).
[23] A. Ashworth, *supra* note 21 at 753.
[24] M. Redmayne, *supra* note 8 at 214 to 215.
[25] A. Ashworth, *supra* note 21 at 758.
[26] We see this distinction as superficial, since even a person's thoughts can acquire autonomy if transposed to paper prior to the moment of constraint.
[27] R. Chiriță, *supra* note 2 at 68.

person to surrender authorities murder weapon. Clearly, the murder weapon is "real" evidence that has an existence independent of the will of the accused person. However, we see absolutely no reason in allowing the accused not to declare nothing, but nevertheless compel him to submit material evidence on the grounds that this evidence is not one testimonial. In other words, the accused has the opportunity to refuse to say where the gun is but is obliged to he was teaching it. Clearly, a distinction such as the one above cannot be accepted.

Also, as mentioned above, plan exclude obtaining documents from the scope of applicability of the privilege against self-incrimination would create a collision between those held in Funke and those in Saunders. However, it is not expressly apparent from the recitals in Saunders that in the presence of a jurisprudential reversal. The Court does not contradict what was held in Funke, it does not return on the conclusion of this case, but only develops the analysis of privilege against self-incrimination. Analysis which, moreover, Funke is completely absent.

Furthermore, a careful analysis of the Court's considerations in Saunders shows that it seems to have made at least as far as documents are concerned a distinction between the ways in which it is carried out coercion and not between 'real' evidence or 'testimonials'. Consequently, the existing wording in Saunders needs to be carefully analyzed, and it can be noted that obtaining any document is not excluded within the scope of the privilege against self-incrimination, but only those documents obtained as following a search warrant.[28] This conclusion reinforces the argument that the key is whether or not that constraint involves collaboration on the part of the accused. In the case of domiciliary search warrants, the prosecuting authorities. They may forcibly obtain the documents contained in the warrant, without the need for the cooperation of the accused person.[29] However, in so far as the cooperation of the accused person is required, the privilege against self-incrimination becomes applicable because such forced collaboration is contrary to his will[30] which is why such collaboration is, moreover, excluded by reference to the offence of obstruction of justice. This view has also been supported in the literature,[31] where it has also been held that biological evidence exceeds the scope of the privilege against self-incrimination on the grounds that it can also be obtained without the cooperation of the person concerned.[32]

For example, a DNA sample could be taken by a justified intrusion into the individual's privacy without violating Article 8 of the Convention and at the same time, without requiring conduct contrary to Article 3 of the Convention. In this context, the collection of biological samples such as blood or saliva, without the consent of the data subject, was not considered to be in conflict with the provisions of art. 3 and 8 of the Convention in X. v. Netherlands and Schmitd v. Germany.[33] It is

[28] M. Berger *supra* note 22 at 526.
[29]A. CHOO, THE PRIVILEGE AGAINST SELF-INCRIMINATION AND CRIMINAL JUSTICE,73 (Hart Publishing, Oxford, 2013).
[30] A. Ashworth, *supra* note 21 at 760.
[31] M. Redmayne, *supra* note 8 at 214.
[32] Sometimes there is talk of active v. passive cooperation. See also; V. Puşcaşu, *Supra* note 2 at 206).
[33] Jalloh v. Germany.

true that, in Jalloh v. Germany, the Court found that the privilege against self-incrimination had been violated, even though the authorities had obtained material evidence from the applicant's body without his cooperation. However, the conclusion in Jalloh only emphasises once again that what is essential is not the object of coercion but the way in which it is achieved. As far as we are concerned, it follows from Jalloh that, exceptionally, the privilege also applies when we are talking about obtaining pre-existing material evidence without the cooperation of the data subject, namely when it is done in violation of Article 3 of the Convention.[34] Thus, the rule is that the privilege against self-incrimination prohibits coercion to cooperate, whereas the exception concerns a situation where, in the absence of cooperation, intervention is made in order to obtain evidence in violation of art. 3 of the Convention.

In relation to the rule, although from a material point of view pre-existing documents may have an existence independent of the will of the accused person**,** their occurrence affects this will, which is why it is the coercion to cooperate that activates the privilege against self-incrimination and not the means evidence subject to coercion.[35] The fact that this is so, and the obtaining of documents as a result of coercion to cooperate entails the applicability of the privilege against self-incrimination, it follows with evidence including Heaney and McGuiness v. Ireland, a case subsequent to Saunders and in which the Court adopted the conclusion in the Funke case.

This chronological analysis of the Court's case-law shows that in Saunders it did not have there is a reversal of case-law, since it did not contradict what was held in Funke, and in Heaney and McGuiness agreed to the Funke judgment without contradicting Saunders.[36] Moreover, in JB v. Switzerland, the Court held that the privilege against self-incrimination had been violated although the subject matter. The coercion concerned the handing over of financial documents to the tax authorities.[37] In order to establish a violation of Art. 6 of the Convention, the Court held that those documents differed from the biological samples produced reference in Saunders, stating that only the latter are obtained without breach of willperson (para. 68). If in Saunders, the Court referred to any documents, by whatever means by which they are obtained, why in JB v. Switzerland coercion to the submission of documents led to the violation of art. 6 of the Convention?. Thus, in the case of biological samples, we are talking about passive collaboration in the sense that the data subject has the obligation not to oppose the collection of the biological sample, whereas active cooperation cannot be compulsed. With such a distinction we could and we agree, it is essential

[34] It could also be argued that, in Jalloh, the decisive factor was the fact that the applicant had regurgitated a quantity of cocaine was, without question, incriminating. Thus, a distinction could be drawn between biological samples taken in order to carry out an expert opinion and those pre-existing pieces of evidence which are per se incriminating. See, to that effect, para. 113 of thief. Jalloh v. Germany and A. Choo, op. cit., pp. 74–75. However, I consider such a conclusion to be contrary to what was stated in Saunders, where The Court relied on the idea that it was irrelevant whether or not evidence obtained as a result of coercion was per se incriminating – including The quoted author observing this. Also, to mark this element as defining in terms of applicability The privilege against self-incrimination would make the handing over of documents as a result of coercion no longer raise problems in this matter as long as their content can prove criminal conduct.
[35] A. Ashworth, s*upra* note 21 at 760.
[36] M. Redmayne, s*upra* note 8 at 213.
[37] R. Chiriță*supra note*2 at 65.

that the privilege against self-incrimination becomes applicable when coercion involves cooperation in the sense of active cooperation.

In conclusion, I consider that only an inadequate interpretation of the recitals in Saunders can create confusion in the scope of the privilege against self-incrimination in relation to handing over documents as an object of coercion to cooperation.[38] Any reasonable interpretation of the Court's case-law indicates that the surrender of documents as an effect of coercion to cooperate is contrary to the privilege against self-incrimination. Only documents obtained by means of a domiciliary search warrant and without the forced cooperation of the accused person causes Art. 6 of the Convention is not applicable (para. 102 in Jalloh v. Germany).

- **On providing a voice sample:** In P.G. and J.H. v. United Kingdom, the Court held that obtaining voice samples by means of non-consensual recordings do not entail a violation of the privilege against self-incrimination. From this perspective, the Court basically concluded that, as long as the voice samples did not contain incriminating statements, they could be regarded as blood, hairs or other such specimens used in forensic analysis and which, according to Saunders, it is not covered by the privilege. Although we do not criticise the solution reached by the Court from the perspective of respect for the privilege of self-incrimination, we cannot help but wonder how a coercion carried out in compliance with the provisions of art. 6 of the Convention if the person concerned refuses to cooperate and the authorities do not have possibility to use ambient recordings or telephone conversations to obtain voice samples "offered" involuntarily. Insofar as the only possibility of obtaining such samples is through 'participation active" of a person, the question arises to what extent his coercion to cooperate is consistent with the privilege under consideration.

The discussion in this context becomes somewhat problematic due to the fact that cooperation can be achieved either by means of a physical/moral constraint or by means of a legal norm establishing a sanction in case of refusal to cooperate. Physical/moral coercion becomes problematic because it puts in discussion of compliance with Art. 3 and 8 of the Convention, with the risk that disproportionate intervention will entail precisely the consequences of Jalloh v. Germany. The only solution would therefore remain the establishment of a legal obligation to cooperate on pain of sanctions in case of refusal, similar to the provisions regarding the collection of biological samples for participants to road traffic.[39]

Beyond these aspects, in relation to the issue of decryption of computer data, it is essential to see to what extent such compulsion becomes or does not become an exception to the rule. Without insisting at this time. In connection with this matter, mention that, as far as we are concerned, the decryption of computer data by means of a voice command requires distinct treatment. That's because the key are decryption of

[38] However, I cannot fail to note that the Court's case-law on privilege against self-incrimination raises problems of interpretation, in particular because of cases in which the United Kingdom was the defendant.
[39] In connection with those provisions, the Constitutional Court has held on several occasions that the legal obligation to cooperate for the purpose of biological sampling is in accordance with the privilege against self-incrimination. See in this regard V. Puşcaşu, Supra note 2 at 206-207.

computer data consisting of the voice of the holder of the computer system does not only involve: the need to identify characteristics of the voice, and content is also essential. In other words, for the decryption of computer data, it is not only the identification of the voice of the holder of the computer system that matters, it is also necessary for the holder to utter a word or phrase, which denotes a component testimonial covered by the privilege against self-incrimination.

- **Possibility to restrict the applicability of the privilege against self-incrimination or to cancel it:** In Funke, the Court implicitly recognised that privilege cannot be weighed against interest public in order to determine a violation of the right to a fair trial. It follows from the fact that that the decision favourable to the complainant was given contrary to the opinion of the Commission in the same case, which held that that coercive means was necessary to protect "the vital economic interests of the State".[40] That it is so including Heaney and McGuiness v. Ireland and Quinn v. Ireland, where the charge one of terrorism.It was undoubtedly of particular relevance from the perspective of the public interest, but nevertheless it was found violation of Article 6 of the Convention by failing to respect the privilege against self-incrimination.[41]

In Saunders, the Court also rejected the Government's argument that public could justify a restriction of privilege against self-incrimination,[42]and in Jalloh v. Germany, the Court held quite clearly that the requirements the general law relating to the fairness of criminal proceedings shall remain applicable irrespective of the type of offenceor the public interest invoked.[43]An extremely important cause in this regard may turn out to be Ibrahim et al. v. United Kingdom, where the accusation of terrorism has, in my view, led to an erroneous solution by the Court, which held that it did not the privilege against self-incrimination has been violated, even with regard to the statement of a witness who did not he was made aware of the right not to incriminate himself when this risk was as high as possible obviously. However, these issues are to be reassessed by the Grand Chamber, which is why we do not want to insist on a ruling that could be reversed.[44]

In John Murray v. United Kingdom, however, the Court held that the privilege against self-incrimination is not an absolute[45] in that, in particular situations, the silence of the accused can produce consequences unfavourable to him (para. 49 of the judgment). Also relevant in this regard are Averill v.United Kingdom and Telfner v. Austria, cases in which the Court has also emphasised the idea that, in certain circumstances, the silence of the accused can be turned within certain limits against him. It should be noted, however, that in all these cases the focus has been on the circumstances in which this passivity of the accused takes place and not on the nature

[40] A. Ashworth, *supra* note 21 at 753.
[41] M. Berger, *Self-Incrimination and the European Court of Human Rights: Procedural Issues in the Enforcement of the Right to Silence*, 2 European Human Rights Law Review, 358- 359 (2007).
[42] Marttinen v. Finland (paras. 74-75).
[43] Public interest which is put into an entirely different perspective in para. 107.
[44] M. Seet, *Suspected Terrorists and the Privilege Againsts Self-Incrimination*, 74 (2) Cambridge Law Journal, 208 (2015).
[45]A. Ashworth, *supra* note 21 at 754.

or gravity of the offence which is the subject of the accusation. These circumstances concern, for example, the degree to which the accusation was proved independently of what was stated by the accused person. Thus, to the extent that the evidence in the indictment is important (incriminating traces on body or clothes of the accused Averillv. United Kingdom) and an explanation is deemed necessary on the part of the accused (John Murray v. United Kingdom), the right to remain silent may be subject to certain restrictions. The ECtHR considered it reasonable to conclude in those circumstances that silence can only indicate an implicit admission of guilt. It should be noted, however, that this conclusion was also due to Section 35 of the the Criminal Justice and Public Order Act 1994, which basically established the internal regulatory framework for restricting Privilege. The ECtHR therefore reached the above conclusion only by reference to the domestic law subject to analysis. Strictly under in this aspect, the level of protection under domestic law is higher than that conferred by Article 6 of the Convention.

In O'Halloran and Francis v. United Kingdom, the Court found that self-incrimination was not infringed, although the coercion was as direct as possible in the sense that the applicants received a notice asking them to inform the police who drove the vehicle that was detected by radar as exceeding the legal speed limit. It is obvious that, by this judgment, the Grand Chamber of the ECtHR decided that the privilege of Self-incrimination is not absolute, but can be limited by reference to certain factors. What is objectionable, however, is the fact that no clear criteria were provided to be applied in other cases. For my part, this case is not representative of the assessment of its scope of the privilege against self-incrimination, seeming rather that the solution given was due to the context in which the coercion has taken place, namely with a view to preventing road accidents. In other words, the O'Halloran case and Francis v. United Kingdom seems to establish an exception to the rule rather than clarify whatneeded to be clarified. In support of the solution to this case, it could be argued that there is a consensus at Union level in the sense that the privilege against self-incrimination does not apply with respect to the identification of the person who has driven the vehicle.[46] Thus, in some Member States, in so far as the owner of the vehicle refuses to indicate the person who drove the vehicle is possible to use a presumption to the effect that the owner of the car was and its leader.[47]

It could also be concluded that the privilege against self-incrimination can be limited on the basis of the risk assumed by road users.Including Judge Borrego, in the opinion competitor, insisted on the idea that those who decide to own a vehicle and participate with it in Road traffic assumes certain obligations in order to preserve traffic safety, and the renunciation of the privilege Against self-incrimination may be one of these. This reasoning, although persuasive, is an extremely dangerous one because there is a risk of being extended to other spheres of activity, practically depriving the privilege against self-incrimination. Finally, in trace, even terrorists take certain risks in their work, which cannot result in abolition,

[46]Id at 753 and 771.
[47] Ibid.

For their part, the guarantees conferred by Art. 6 of the Convention. As in the case of road traffic, commercial activities, customs, etc. are strictly regulated, and it can also be argued that those persons who consent to take part in such activities accept the risks arising therefrom including the risk of be obliged to cooperate with certain control authorities/bodies. Such an approach would deprive Content rights conferred by art. 6 of the Convention, which have become practically illusory.

- **Possible criteria for justifying coercion:** From all the ECtHR case-law in this field, it seems to emerge the conclusion objectionable or notthat the privilege against self-incrimination may suffer certain limitations, not being an absolute one. Or, in other words, it is possible that in certain circumstances, although there is a coercion to cooperate, it may not or incompatible with the essence of the right to a fair trial. Even if we were to accept such a view, I consider it necessary to identify clear and reasonable criteria, qualities that do not seem to be met compared to sporadic criteria in the case-law of the Court.

  - **Public Interest:** With regard to this criterion, we have seen theapparent direction of the ECtHR in the matter of privilege against self-incrimination. Although this is not entirely clear and sometimes comes into an impermissible conflict with our own case-law, we may soon witness the legitimation by the ECtHR of a treatment preferential offered to persons accused of terrorism offences. Without neglecting the importance of the fight against terrorism, this repositioning of the ECtHR that calls into question the "right of the enemy" in which a person accused of terrorism. Loses the status of beneficiary of basic yet fundamental rights wouldn't it be fairer and more honest in referring to these people as combatants and giving up considering that sanctioning. Do they belong to the judiciary? The biggest problem is that the terrorism problem can degenerate into a problem at the level of respect for human rights, including in other areas where the public interest will be easy to highlight as a criterion for limiting or abolishing the privilege against self-incrimination for example, in drug trafficking, corruption offences, cybercrime, etc. Such an approach would effectively limit the right to a fair trial according to the degree of the public interest identified in the case under consideration. Although such a proportionality examination can find justification with regard to Articles 8-10 of the Convention raise serious questions about regarding respect for the right to a fair trial.[48]

    It is impossible for us to accept that a person who has committed a serious crime must benefit from to a lesser extent of due process than another person who had the "inspiration" to choose to commit an offence that does not denote a "significant" public interest. The situation can become all the more dramatic how much the seriousness of an offence or the public interest may differ significantly from one Member State to another. However, we have serious reservations that crimes such as abuse of office or conflict of interest justify a limitation of the right to a fair trial.

[48] D. Ionescu, *Gäfgen v. Germany: a moment of reflection and many questions*, 4 Notebooks of Law criminal, 25-26 (2012).

If such an approach is justified for them, all that remains is to offer similar treatment and in the case of crimes against the person (murder, deprivation of liberty, rape, etc.), because including these is particularly serious and should reveal a 'significant' public interest. That's how we end up we report to organized crimes (trafficking in human beings or drugs, cybercrime etc.) or economic (money laundering, tax evasion, etc.), because not taking them into account would no longer have a "real justification". In context, we can only ask rhetorically what would then be left of Art. 6 of Convention? A combination of rules apparently strict but applicable only in the case of a crime of theft or cheating? Because with regard to traffic offences, the Court has already clarified.

- **Impossibility / difficulty to obtain evidence by other means:** In the Funke case, there was a violation of Article 6 of the Convention, although the Court took into account the fact that: The customs authorities "could notor would not obtain the documents by other means." Specify is important in the context in which the inapplicability of the privilege could be invoked in view of the difficulty or, sometimes, the impossibility of decrypting computer data in the absence of cooperation of the suspect, defendant or to the witness by providing the key for decryption or by directly offering the content in a readable format (unencrypted).

  It is hard to believe that the privilege against self-incrimination would become unenforceable every time Judicial bodies would have difficulty establishing guilt. Incidentally, the privilege in question, by reporting To the presumption of innocence, it is based precisely on this relationship between the State and the accused, in which the conviction must be obtained without the latter's support[49] (see also para. 100 in Jalloh v. Germany).

  However, it is clear that the possibility of proving beyond a reasonable doubt that a person is guilty of the commission of an offence no longer justifies a genuine need to restrict the scope of the privilege against self-incrimination. This need is evident in precisely those situations where the prosecution is vulnerable to evidentiary perspective. I therefore consider that it is precisely those situations that must give rise to additional guarantees in favor of the accused person, because from the vulnerability of the evidence in the prosecution comes the temptation to transform the accused person in a prosecution witness – which is exactly what the Court pointed out in Saunders.

  On the other hand, to use such a criterion to restrict the applicability of the privilege may generate absurd consequences in which it becomes inapplicable even in the case of taking a statement by coercion. To the extent that the issues to be considered by the accused person are extremely relevant from the point of view evidentiary evidence and the only reasonable possibility of obtaining the desired information is by hearing the accused person, would create exactly the framework envisaged above. Again, the accused would turn into a prosecution witness then

[49] R. Chiriţa, *supra note*2 at 60-61; M. Udroiu, *Fundamental principles contained in the draft of the new Code of criminal procedure – towards a new model of criminal process*, 2 Notebooks of criminal law, 71 (2009).

when the prosecution cannot prove its own case. It is precisely that approach that conflicts with the presumption of innocence.

- **Nature and gravity of the penalty in case of refusal:** One possible criterion would be to refer to a minimum threshold of the adverse consequences that would the person who refuses to collaborate suffers.[50] In Saunders, the penalty for refusal to cooperate (contempt of court) was 2 years in prison, while in Allen – where the Court held that the privilege of self-incrimination - the risk was punishable by a fine. O'Halloran and Francis v. United Kingdom, the Court held it important that the penalty for refusal was one "moderate" and not a custodial one. If this privilege is an essential component of the right to a fair trial, such an approach It turns out to be nothing but incoherent and absurd. On the other hand, although in Funke the applicant was sanctioned for refusing to submit to the authorities certain bank documents requested by them by applying fines, however, the Court found a violation of the privilege against self-incrimination.

- **Nature and degree of constraint:** The Court made express reference to this criterion both in Jalloh v. Germany and O'Halloran and Francis v. United Kingdom. In Jalloh v. Germany, regurgitation forced drugs by restraining the suspect and administering chemicals through a tube inserted through the nose into the stomach was considered incompatible with the provisions of Art. 3 of the Convention and with the privilege against self-incrimination. In Allan v. United Kingdom, in its ruling, the Court held, in practice, that Coercion does not necessarily have to involve violence.[51] Thus, including the use of subterfuge in order to Obtaining an involuntary statement is likely to give rise to the privilege against self-incrimination.

- **Existence of procedural guarantees:** Also in Jalloh v. Germany, the Court referred to this criterion in its analysis concerning the destruction of the essence of the right to a fair trial by disrespecting the privilege of self-incrimination. Again, the analysis of a criterion used in an exceptional case such as Jalloh raises certain difficulties. We agree, however, that the existence of procedural guarantees could make the privilege of self-incrimination acquires a narrower applicability. In Jalloh v. Germany, however, it was held in sight of the improper means by which the applicant's body was interfered with. The only example where the subject of computer data decryption could be reported to the Jalloh case would be where the person concerned swallows the material entity on which the key for decrypting computer data is stored. As regards procedural guarantees to avoid abuses and arbitrary interventions, we consider that domestic law is far from setting an example to follow. Also, strictly in relation to the issue of decryption of computer data, it needs to be observed the fact that the domestic laws does not provide sufficient guarantees.

In conclusion, we are in a situation where every person must be of maximum good faith and cooperate with judicial bodies by providing the key to

[50] M. Berger, *supra* note 23 at 518.
[51] A. Ashworth, *supra*note 21 at 761 and 765.

decrypt computer data or content in a readable format, hoping that they, in turn, will not abuse the highly permissive framework established by Code of Criminal Procedure. And when we say that we also mean the constant practice of organs criminal prosecution to carry out computer searches by means of technical-scientific findings, in to circumvent all guarantees even as deficient as they are provided by code of criminal procedure. Perhaps it is time for the legislator to realize that such an intrusive means as Computer searches need to be based on appropriate safeguards. We think it's a far cry from culturelet us establish such safeguards where the law does not provide for them, which is why these legislative loopholes**. T**hey are extremely dangerous, the prosecution bodies often having the temptation to do everything what the law does not prohibit. In this context, this 'everything which the law does not prohibit' implies an intrusion into private life of a person in the absence of an effective control mechanism.

- **The information provided is not per se incriminating:** In Weh v. Austria, the applicant refused to indicate who had driven the vehicle, but did not was, from the Court's perspective, under the privilege against self-incrimination. Although the essential argument of the Court was that, at the time of the applicant's refusal, criminal proceedings could not even be in the recitals of the judgment, it was also concluded that the identification of the name of the person who driving the vehicle when committing a traffic offence is not per se criminal.

  As far as I am concerned, both conclusions are highly objectionable. Thus, it is at least bizarre to maintains that the identification of the person who drove the vehicle is not per se incriminating given that which is the central element of any traffic offence. If what was meant to be highlighted is the fact that that the identification of the name of the driver of the vehicle is not criminal, since conduct must also be proved; criminally, we would end up in a situation where most statements taken under duress would be devoid of this characteristic for the simple reason that not all the constituent elements of Offence. Many pieces of evidence need to be corroborated with others in order to obtain probative force, but this. It does not mean that, taken individually, they are not themselves incriminating.

  On the other hand, since information is required on the person who drove the vehicle in the context of suspicion or certainty that this vehicle has been used to commit a traffic offence is difficult It was to be believed that at the time of the complainant's refusal to provide the requested information, initiation could not have been envisaged criminal proceedings against him. However, in view of the possibility of using this criterion in the future, we are forced to analyse its applicability in relation to the key used to decrypt computer data.This is so much more so far as is possible that, in Jalloh v. Germany, including the fact that the evidence obtained (cocaine) was per se incrimination/n contributed to the Court's conclusion that the privilege against self-incrimination has been violated. However, in the Saunders case, the Court found a breach of privilege although the information provided were not per se incriminating. Thus, some might argue that a key used to encrypt/decrypt is not incriminating per se, only encrypted computer

data having this feature**.** In other words, it would may plead that such a key is neutral from an evidentiary perspective, unless Its content is incriminating.

As far as we are concerned, such a view is erroneous and shows confusion at the level of the function that such a key has.Whether we are talking about a password, a physical device or a trace Papillary, the key to encryption/decryption is always based on binary information that becomes part of the encrypted computer data.For example, if computer data is encrypted / decrypted via a papillary trace, the process consists of scanning it and retrieving a relevant binary code that offers uniqueness papillary traces. In other words, even if we are talking about a biometric key, at the core we are talking. Also about a binary code consisting of a string of "1" and "0". If one insists on the idea that this key is not incriminating per se, but only encrypted computer data If it has this feature, then we do not see why judicial bodies do not use against the accused person Encrypted content. Any analogy with a key or vault code is erroneous,[52] since a key used for decryption is not only the means by which the readable content of computer data is accessed as a result of their decryption.

Technically, the encrypted/decrypt key is a variable in a function, alongside encrypted/unencrypted computer data. An absolutely elementary encryption can take place by replacing a letter from the alphabet to the following – A becomes B, B becomes C, Z becomes A, etc. The number used for this exchange represents a variable (n) that is actually the key to encrypting / decrypting information. Thus, if n=1 then A becomes B (A + n) at the moment of encryption, and B becomes A at the moment of decryption (A - n). If n=2 then A becomes C at the time of encryption, and C becomes A at the moment of decryption. It is therefore noted that identifying the contents of variable n involves identifying the encryption/decryption key. Clearly, in the case of modern encryption algorithms, modification of computer data by reference to the variable containing the encryption key denotes great complexity. However, the conclusion that the key affects the content is maintained. This key is not identical in terms of its role to the password (passcode) used For authentication within an operating system, the CI also has the role of modifying the content of the data informatics,[53] becoming an integral part of the encryption / decryption function. That is why it is wrong to assimilate This key with the code of a vault.[54]

As for the vault, the access code only allows opening it without producing changes to the level of information contained therein. Exactly the same function has the password for logging into the an operating system. If the agent does not know the password for login, they will not be able to log in (login) within the operating system (Windows, Linux, etc.). This does not mean, however, that

[52] P. Reitinger, *Compelled Production of Plaintext and Keys*, 173-175 The University of Chicago Legal Forum, (1996); M. Smith apud J. Larkin, *Compelled Production of Ecrypted Data,* 14 Vanderbilt Journal of Entertainment and Technology Law, 256 (2012).
[53] N. McGregor, *The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege*, 12 Vanderbilt Journal of Entertainment and Technology Law, 602 (2010).
[54] B. Folkinshteyn, *A Witness Againsts Himself: A case for Stonger Legal Protection of Encryption*, 30 Santa Clara High Technology Law Journal,400- 402 (2014).

computer data cannot become accessible by direct connection to their means of storage. That is precisely why when performing a Computer search is irrelevant whether or not the user has set a password for authentication within the operating system, because the specialist will not – as a rule – try such authentication, but will interact directly with computer data by mounting the storage medium (e.g. a hard drive) to your own system computer through a blocker. Only to the extent that this password also has an encryption function, not just authentication within the system, it becomes a real key to decrypting computer data. As far as we are concerned, forcing a person to provide the key to decrypting computer data or submitting them in a readable/accessible format is similar to forcing a person to translate a document[55] in a language known to the judicial body.In all cases, what is desired is conversion content illegible into readable / accessible through coercion.

In conclusion,an encryption/decryption key has two intertwining functions: it allows access to computer data (1)in machine-readable format following the decryption process or vice versa (2). Precisely by that requires acceptance that even the encryption/decryption key is incriminating. If this issue were understood and accepted by some, we are convinced that it would not be reaches hasty conclusions based on an erroneous premise that the key is absolutely neutral from evidentiary perspective. Beyond the fact that knowing the key used to decrypt computer data generates a presumption reasonable[56]that the person holding the key also possesses computer data encrypted via,[57] as stated above, it is not neutral(it does not allow only access) but becomes part of encrypted content (has a direct role in modifying computer data). As far as we are concerned, we see such a key as representing pieces of a puzzle against which the rest of the pieces could not be put in order to form a complete and intelligible image.

IV. CONCLUSION

Technology is the resource of all people able to understand and use it. Criminal prosecution shall make use of any technological development in order to combat or prevent crime, while potential suspects encrypt their communications and computer data to make it harder to do business criminal prosecution bodies. In other words, technology is an asset that turns into an obstacle, depending on the entity to which we relate. For our part, the possibility of using new technology to raise Evidence requires a rethinking of how we relate to the right

[55] U.S. v. Ragauskas

[56] According to ECtHR case-law (e.g. Salabiaku v. France), a presumption of law or fact is compatible with Art. 6 of the Convention as long as it is reasonable. Thus, the presumption under French law (Customs Code) to whom the person in possession of the prohibited goods is guilty of committing the crime of smuggling has not been assessed as incompatible with the presumption of innocence – see also P. Mahoney, Supra note at 123. The clarification is important because It is hard to believe that the identification of child pornography material on the computer system belonging to the accused person of committing the offence of child pornography will not give rise to a presumption – extremely difficult to rebut – to the effect that it possessed or stored such pornographic material. The presumption is all the more reasonable given that the data concerned computers containing child pornography were encrypted, and the accused knew the key to decryption Their. Given this context, we cannot fail to take seriously the need to apply the privilege against self-incrimination in hypotheses of this kind.

[57] Smith, *Is the Right Against Self-Incrimination Properly Protected in Europe?* 27 International Legal Practitioner,117 (2002).

to privacy. This is because the prosecution means are increasingly intrusive and often not used as a last resort rather, it is the rule in a criminal investigation.

In this context, I consider there to be an imbalance in the equality of arms when argues that technology used to the detriment of the prosecution is a problem that can be solved only by restricting citizens' rights. If in terms of the right to privacy. Such a restriction may be justified within certain limits, I am of the opinion that the reduction of the duty not to participate in one's own incrimination (privilege against self-incrimination) to the status of illusory law in the context of computer data encryption represents a real regression in terms of respect for human rights. Beyond the pros and cons, we remain of the opinion that the privilege against self-incrimination remains an extremely important guarantee in terms of the right to a fair trial, and the risk of suspect, defendant or witness subsequently became a suspect or defendant in an agent of the State by the establishment of an obligatory relationship between him and the criminal investigation bodies deprives of content an elementary rule of criminal proceedings, namely that the prosecution bodies and only they have the obligation to prove the conduct Criminal. Depriving any person of the protection afforded by Art. 6 of the Convention when the problem arises encrypted computer data is a "slippery slope" that will have serious repercussions in that era when Digital completely absorbs the traditional in matters of probation.

