



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIFTH SECTION

DECISION

Application no. 23624/20
Lamin MINTEH
against France

The European Court of Human Rights (Fifth Section), sitting on 19 May 2026 as a Chamber composed of:

Kateřina řimáčková, *President*,

María Elósegui,

Mattias Guyomar,

Gilberto Felici,

Mykola Gnatovskyy,

Vahe Grigoryan,

Sébastien Biancheri, *judges*,

and Victor Soloveytchik, *Deputy Section Registrar*,

Having regard to:

the above application lodged on 10 June 2020;

the decision to give notice of the application to the French Government (“the Government”);

the observations submitted by the respondent Government and the observations in reply submitted by the applicant;

the written comments submitted by Fair Trials, a non-governmental organisation which was granted leave to intervene by the President of the Section;

Having deliberated, decides as follows:

INTRODUCTION

1. The case concerns the criminal conviction of the applicant on the ground that he had refused, while in police custody, to disclose the secret decryption key to unlock his mobile phones. The applicant relied on Articles 6 § 1 and 8 of the Convention.

THE FACTS

2. On 17 November 2017, the applicant was stopped by police while he was driving his vehicle without a seatbelt. An inspection found that he was transporting on his person a sum of 6,680 euros (EUR) in cash, with large traces of cocaine and cannabis on the notes, as well as a block of cannabis resin, which was lying on the floor in front of the passenger seat. A mobile phone was also found in the car and seized by the police.

3. An expedited police investigation was opened. A search of the applicant's home revealed three other mobile phones, a touch screen tablet, sports betting slips and EUR 3,780 in cash. The applicant was taken into police custody. During his interview, the police officer immediately informed him that his lawyer did not wish to assist him. He then invoked his right to remain silent and also refused to disclose the decryption keys to unlock his mobile phones.

4. The relevant extract of the interview record of 18 November 2017 is worded as follows:

“... Q: Your lawyer does not wish to attend your interviews; do you agree to be interviewed in his absence?

A: No.

Q: Do you agree to provide us with the passcodes to unlock your mobile phones?

A: I wish to remain silent.

Q: I am informing you that refusing to provide us with your mobile phone passcodes constitutes an additional offence; do you confirm your statement?

A: Yes.

Q: Do you have anything else to add?

A: No.

After reading this record, he has confirmed its content and signed it together with me; done at 12.30 p.m.”

5. The investigators abandoned their attempts to access the mobile phone data.

6. On 21 November 2017 the applicant was brought before the public prosecutor of the *tribunal de grande instance*, who charged him, firstly, with having transported, possessed, offered or supplied, and acquired drugs as a recidivist, and, secondly, of having refused to disclose to the judicial authorities, or to implement, a secret decryption key for access to a “cryptographic means” which was suspected of having been used to prepare, facilitate or commit an offence, while having knowledge thereof. This last offence was provided for by Article 434-15-2 of the Criminal Code (see paragraph 13 below). The lawyer chosen by the applicant was not present when he appeared before the prosecutor but indicated that he would attend

the Criminal Court hearing, at which the applicant was to stand trial under the fast-track procedure, on the same day at 1 p.m.

7. During that hearing the applicant's lawyer requested that a preliminary question of constitutionality (*question prioritaire de constitutionnalité* – QPC) be referred to the Constitutional Council concerning Article 434-15-2 of the Criminal Code on the constitutional principles of the right to a fair trial, the presumption of innocence and the right to respect for one's private life and correspondence. The trial was adjourned and the QPC was transmitted to the Constitutional Council.

8. By decision no. 2018-696 QPC of 30 March 2018, the Constitutional Council ruled that the provision was compliant with the Constitution. It found as follows:

“6. The first paragraph of Article 434-15-2 of the Criminal Code provides for a sentence of three years' imprisonment and a fine of EUR 270,000 in the case of 'anyone' who has knowledge of the secret decryption key for access to a 'cryptographic means' that may have been used to prepare, facilitate or commit an offence, and refuses to disclose that key to the judicial authorities, or to implement it when so directed by the authorities. It can be seen from the Court of Cassation's settled case-law, as indicated in the decision referring the preliminary question of constitutionality, that this obligation applies to everyone, including those suspected of having committed an offence using such a 'cryptographic means'.

7. Firstly, by requiring a person with knowledge of a secret decryption key to disclose it to the judicial authorities, or to implement it, only if the 'cryptographic means' is suspected of having been used to prepare, facilitate or commit a serious offence (*délit* or *crime*), and only if the instruction comes from a judicial authority, the legislature pursued objectives of constitutional value, namely those of preventing offences and identifying the perpetrators, both being necessary for the protection of rights and principles of constitutional value.

8. Secondly, under the first sentence of section 29 of the Law of 21 June 2004 ..., a 'cryptographic means' is defined as 'any hardware or software designed or modified to convert data, whether it be information or signals, using secret encryption keys, or to carry out decryption with or without a secret key'. The impugned provisions only requires a person suspected of committing a serious offence using a 'cryptographic means' to disclose or to implement the secret decryption key if it is established that they have knowledge of that key. Those provisions do not seek to obtain confessions from the suspect and do not entail any acknowledgment or presumption of guilt but merely enable access to be gained to encrypted data. In addition, the police or judicial investigation must have established the existence of data processed by the 'cryptographic means' that is suspected to have been used to prepare, facilitate or commit a serious offence. Lastly, such data, already being fixed on a medium, exist independently of the will of the suspect.

9. It follows that the impugned provisions do not contravene the privilege against self-incrimination, nor the right to privacy or the confidentiality of correspondence.

10. The first paragraph of Article 434-15-2 of the Criminal Code, which moreover does not disregard defence rights, the principle of proportionality of penalties, freedom of expression, or any other right or freedom guaranteed by the Constitution, must be held to be constitutional.”

9. By a judgment of 7 June 2018, the Criminal Court found the applicant guilty on all charges, as a recidivist, and sentenced him to six years in prison with immediate remand in custody and a two-thirds minimum term. It ruled:

“... Twice, at the police station, the accused exercised his right to remain silent, which he continued to do at the court hearing.

The purpose of the provision that affords this right to defendants aims to limit the psychological pressure that comes merely from being placed in police custody. This means that they should not incriminate themselves inadvertently as a result of such pressure (not to mention police coercion, which is commonly raised at trial). However, the court is entitled to establish the truth independently of any objective or subjective pressure.

The trial is the only time and place that is exempt from any pressure. Despite this fact, Mr Minteh preferred to leave the consistent incriminating evidence to stand. This was made up of serious indications from objective and scientific facts (contamination of bank notes, unexplained sources of income from undeclared work as an Uber driver etc.).

Consequently, it should be noted that the defendant, who impeded the establishment of the truth, for both the prosecution and the defence, ... chose a path of crime linked to trafficking in drugs, an offence heavily punished by law as it is seriously detrimental to public health as well as to general public order.

Accordingly, the Criminal Court considers all the circumstances relating to the extent of the harm to the protected interest, of the seriousness of the alleged offences and the significance of the *mens rea*.

It follows that the Criminal Court can base its decision on the penalty that is set out in the relevant criminal provision relied upon to classify the offences in question. The maximum sentence is 10 years in prison, together with a fine and ancillary penalties. However, having regard to the character of the defendant as described above, the following sentencing terms are appropriate.

A committal order must be issued against him to ensure the immediate enforcement of the sentence. In addition, it is appropriate to impose a minimum term of up to two-thirds of the sentence imposed, to convey to Mr Minteh that his strategy of remaining silent has given rise to concerns that he may reoffend on a larger scale in the field of drug trafficking.

...

FOR THESE REASONS

...

Sentences Lamin Minteh to SIX YEARS' imprisonment;

With a minimum term of FOUR YEARS;

Issues a committal order against Lamin Minteh;

...”

10. The applicant lodged an appeal against the judgment. By a judgment of 7 November 2018, the Paris Court of Appeal upheld his conviction for the drug-related offences and the refusal to disclose to judicial authorities a secret decryption key for access to a “cryptographic means”, without endorsing the

factor of recidivism in respect of this last offence. The court limited the sentence to four years in prison with immediate remand in custody, and by way of ancillary penalty banned him from entering the French *département* of Val-de-Marne for three years and ordered the confiscation of the seized items. The reasoning given was as followed:

“... With regard to the refusal to disclose or implement when requested by judicial authorities a secret decryption key for access to a ‘cryptographic means’ ... the court considers that the court below was correct to uphold this charge against Mr Minteh, given that the facts of his case arose from his refusal to disclose his mobile phone passcodes to the investigators, thereby making it impossible to examine those devices.

With regard to the alleged unconstitutionality of Article 434-15-2 of the Criminal Code, the court observes, in the light of the case-law of the European courts and that of the Court of Cassation, that a breach of the right to remain silent and the right against self-incrimination applies when the data in question cannot exist independently from the will of the suspect; that this is not the case here as the content on the mobile phones can be obtained by technical means.

With regard to the alleged absence of actual use of the phone which facilitated the offence, the court notes that the items found in the defendant’s possession at the time of his arrest, namely the block of cannabis resin and the very large sums of money, analysis of which revealed levels of cannabis and cocaine higher than those usually found on banknotes in circulation, suggested that the mobile phone had been used in connection with drug-related offences.

The court will therefore uphold the judgment of the court below regarding the conviction on this charge, but without endorsing the factor of recidivism.

With regard to the facts of the unlawful acquisition, transportation, possession, offering or supply of drugs as a recidivist, the court considers that the trial judges were legally justified in finding Lamin Minteh guilty on this charge, with the allegations against him having been established by the following matters:

- the items discovered in the defendant’s possession, namely the sum of EUR 6,680 in cash on Lamin Minteh’s person, the presence of a block of cannabis resin on the floor of the vehicle he was driving, as well as a mobile phone;
- analysis carried out on the bank notes found on the defendant’s person at the time of his arrest, which revealed higher levels of cannabis and cocaine than those usually found on bank notes in normal circulation.
- the discovery of EUR 1,650 and EUR 2,130 in cash, and three other mobile phones during the search of his home,
- the defendant’s failure to provide coherent explanations to justify the possession of these sums of money;
- the numerous convictions featuring on his criminal record for similar offences.

The court therefore upholds the judgment appealed against, declaring the defendant guilty on this charge.”

11. The applicant appealed against the judgment to the Court of Cassation. Firstly, he relied on Article 6 of the Convention to argue that the Court of Appeal had breached his right not to incriminate himself by ruling that the data on his mobile phone existed independently of his will and could be

accessed by technical means. Secondly, the appeal also cited Articles 6 and 8 of the Convention to criticise the reasoning given by the Court of Appeal on the grounds that it failed to consider whether access to the mobile phone may have led him to provide information that did not exist independently of his will.

12. On 10 December 2019, the Court of Cassation dismissed the appeal. It gave the following reasoning:

“In dismissing the plea alleging the unconstitutionality of Article 434-15-2 of the Criminal Code, the judgment states that a breach of the right to remain silent and the privilege against self-incrimination occurs when the data cannot exist independently of the suspect’s will, which is not the case with data contained in mobile phones as it can be obtained by technical means.

In so ruling, and since the privilege against self-incrimination does not extend to data that can be obtained from the person concerned by exercising coercive powers, but to data which exist independently of the person’s will, the Court of Appeal did not breach any of the statutory or constitutional provisions invoked in the ground of appeal.

Accordingly, the complaints cannot be upheld.

In finding guilty the defendant for refusing to disclose or implement a secret decryption key for access to a ‘cryptographic means’ when requested by judicial authorities, the judgment observes that Mr Minteh refused to provide investigators with the passcodes to his mobile phones, making it impossible to analyse them. The court adds that the items found in his possession at the time of his arrest, i.e. the block of cannabis resin and the large sums in cash, of which analysis revealed higher levels of cannabis and cocaine than usually found on notes in circulation, suggest that the mobile phone was used in connection with drugs offences.

In the light of that reasoning as it stands, which is sufficient, without contradiction, and based on its independent assessment of the adversarially debated facts, the Court of Appeal duly substantiated its decision.

In finding guilty the defendant of drug-related offences for which he was prosecuted, the judgment states *inter alia* that his guilt derived from the items found in his possession ... and the lack of coherent explanation to justify possession of these sums of money.

In the light of that reasoning as it stands, which is sufficient and derives from its independent assessment, the Court of Appeal duly substantiated its decision without reversing the burden of proof ...”

RELEVANT LEGAL FRAMEWORK AND PRACTICE

A. Relevant domestic law

13. Under Article 434-15-2 of the Criminal Code:

“An individual who has knowledge of the secret decryption key for access to a ‘cryptographic means’ that is suspected of having been used to prepare, facilitate or commit a serious offence (*crime* or *délit*), and who refuses to disclose that key to the judicial authorities, or to implement it, upon an instruction of the authorities, given in

accordance with Titles II and III of Book 1 of the Code of Criminal Procedure, shall be liable to a sentence of three years' imprisonment and a fine of EUR 270,000.

If this refusal is made under circumstances where the disclosure or implementation of the decryption key would have prevented a serious offence from being committed or would have limited its consequences, the sentence shall be increased to five years' imprisonment and a fine of EUR 450,000."

14. In a judgment of 13 October 2020 (Court of Cassation (Criminal Division), no. 20-80.150), delivered after the events in this case, the Criminal Division of the Court of Cassation clarified the notion of "instruction" (*réquisition*) contained in this Article. In particular, it held that a mere request made during an interview, without any warning that refusing to comply might constitute a criminal offence, did not amount to an instruction.

15. In another judgment delivered on the same day (Court of Cassation (Criminal Division), no. 19-85.984), the Court of Cassation clarified for the first time the scope of the offence set out in Article 434-15-2 of the Criminal Code and defined the concepts of "cryptographic means" and "secret decryption key", which it distinguished from a mobile phone passcode. In this judgment the court stated that a passcode would only constitute a decryption key if it allowed the decryption of the data contained on the phone.

16. In a judgment of 7 November 2022 (Court of Cassation (Criminal Division), no. 21-83.146), the Court of Cassation further clarified the scope of the offence set out in Article 434-15-2, stating that a mobile phone passcode could only constitute a secret decryption key if the device was equipped with internal data encryption technology. It found as follows:

"... a decryption key refers to any software or any other information that enables the decryption of data that has been converted by a 'cryptographic means', whether during the storage or transmission of data. This means that a mobile phone passcode may constitute a decryption key if that mobile phone is equipped with a 'cryptographic means'.

It is for the court to determine, therefore, whether the mobile phone in question is equipped with such a feature and whether its passcode allows the decryption of all or part of the encrypted data contained on it or to which it provides access.

In upholding the acquittal, the judgment states that the passcode used to unlock the home screen of a smartphone is not a secret decryption key, as it does not intervene in the sending of a message and is not aimed at rendering data intelligible or unintelligible, within the meaning of section 29 of the Law of 21 June 2004, but merely allows access to mobile phone data and applications which may or may not be encrypted."

B. European Union law

17. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data,

and repealing Council Framework Decision 2008/977/JHA, states that multiple rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for investigations and criminal proceedings. Article 4 in the version applicable since 6 May 2018, reads as follows:

“Member States shall provide for personal data to be:

- (a) processed lawfully and fairly;
- (b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are processed ...”

18. In a judgment of 4 October 2024 (*Bezirkshauptmannschaft Landeck* (Attempt to access personal data stored on a mobile telephone) C-548/21, EU:C:2024:830), the Grand Chamber of the Court of Justice of the European Union (CJEU), in response to a request for a preliminary ruling by the Austrian authorities, gave an opinion on the compatibility with EU law of the seizure by police of a mobile phone of an individual suspected of drug trafficking, and on the investigators’ unsuccessful attempts to unlock it. The Court considered that EU law must be interpreted as not precluding national legal rules which afforded the competent authorities the possibility of accessing data contained in a mobile telephone, for the purposes of preventing, investigating, detecting and prosecuting criminal offences in general – provided those rules defined with sufficient precision the nature or categories of offences concerned – ensured respect for the proportionality principle and made reliance on that possibility, except in duly justified cases of urgency, subject to prior review by a judge or an independent administrative body.

COMPLAINTS

19. The applicant complained under Article 6 § 1 of the Convention that his conviction and sentence for having refused to disclose a secret decryption key to unlock his mobile phones had breached his right to remain silent and not to incriminate himself.

20. Under Article 8, he claimed that this conviction and sentence had breached his right to respect for his private life in that Article 434-15-2 of the Criminal Code did not define precisely enough the concepts of “cryptographic means” and “secret key” and that it did not provide sufficient safeguards to protect people’s privacy.

THE LAW

A. The complaint under Article 6 § 1 of the Convention

21. The applicant complained that his conviction and sentence for having refused to disclose or implement secret decryption keys to unlock his mobile phones had breached his right to remain silent and not to incriminate himself. He relied on Article 6 § 1, the relevant part of which reads as follows:

“In the determination of ... any criminal charge against him, everyone is entitled to a fair ... hearing ... by [a] tribunal ...”

1. *The parties’ submissions*

22. The applicant did not challenge his conviction for the offence of drug trafficking on the basis of the evidence gathered by the investigators, an offence for which he had served a prison sentence. He emphasised, however, that throughout his custody he had exercised his right to remain silent when questioned, including when he was requested to disclose the secret decryption key to unlock his mobile phones and that his silence had entailed a separate conviction under Article 434-15-2 of the Criminal Code.

23. Relying on the criteria established by the Court, notably in *O’Halloran and Francis v. the United Kingdom* ([GC], nos. 15809/02 and 25624/02, § 55, ECHR 2007-III), he firstly argued that even though he had not ultimately disclosed the decryption key for his mobile phones, he had been pressured to do so while in custody. This pressure was due to the risk of criminal prosecution and the deterrent sentence under Article 434-15-2 of the Criminal Code, which potentially entailed actual deprivation of liberty since its maximum term precluded any possibility of adjustment. The investigator’s use of this provision during the interview, in the absence of a lawyer, had constituted a clear means of exerting pressure in his view.

24. The applicant added that mobile phone data could not be regarded as existing independently of his own will, contrary to the Government’s submission based on *Saunders v. the United Kingdom* (17 December 1996, *Reports of Judgments and Decisions* 1996-VI), since he was the only person able to decrypt and gain access to them. He submitted that it was only because a person chose to acquire a mobile phone, install applications on it and create content, such as photographs, that those data existed.

25. Secondly, the applicant complained of insufficient safeguards surrounding the application of Article 434-15-2 of the Criminal Code. He argued that a request for the disclosure of a decryption key had to be treated as a search, an investigative measure for which the presence of a lawyer was not mandatory, meaning that the latter could not serve as a safeguard against arbitrariness. He further argued that the public prosecutor, under whose authority the police custody took place, could not request the disclosure of a decryption key because he did not qualify as a “competent legal authority”

within the meaning of Article 434-15-2 of the Criminal Code and Article 6 (*sic*) of the Convention, as the prosecutor lacked independence and impartiality (he referred to *Medvedyev and Others v. France* [GC], no. 3394/03, ECHR 2010; *Moulin v. France*, no. 37104/06, 23 November 2010; and *Brusco v. France*, no. 1466/07, 14 October 2010). Lastly, he criticised the lack of safeguards relating to the scope of Article 434-15-2, which could apply to any criminal offence, including speeding.

26. Thirdly, as to the use of evidence obtained during the proceedings, the applicant stated that this conviction had been based exclusively on the exercise of his right to remain silent, during police custody when his lawyer was not present, and that this was separate from his conviction for drugs offences. He stated that investigators did not inform suspects of the consequences that the disclosure of secret decryption keys could have in the context of criminal proceedings.

27. The Government, also relying on the criteria set out in *O'Halloran and Francis* (cited above), took the view that no coercion had been used by the authorities against the applicant, other than recourse to police custody. The applicant had chosen to exercise his right to remain silent, and the domestic courts had consequently relied on other evidence obtained during the investigation to find him guilty.

28. Referring to *Saunders* (cited above), they argued that the data contained in a mobile phone existed independently of the suspect's will and that the authorities could access it using other means, such as through forensic computer analysis, if necessary with technical intervention on the mobile phone itself.

29. The Government also stated that the privilege against self-incrimination was not absolute, and that it had to be consistent with the imperatives of ensuring safety and establishing the truth. The Court should therefore be prepared to tolerate interference with this right provided that the overall fairness of the proceedings was preserved. Drawing particularly on the judgments in *John Murray v. the United Kingdom* (8 February 1996, *Reports of Judgments and Decisions* 1996-I) and *Simeonovi v. Bulgaria* (no. 21980/04, 12 May 2017), they emphasised that overall fairness must be assessed in relation to the nature and degree of coercion, the weight of the public interest in prosecuting the offence, the existence of appropriate safeguards in the proceedings and the use made of the evidence obtained.

30. They observed that the applicant had been able to exercise, and had indeed relied upon, all the rights accorded to individuals in police custody. They further referred to the safeguards established by the legislature and emphasised by the Constitutional Council in connection with such a procedure: a person could only be convicted if it was proven that he or she was aware of the secret key, the investigation must have established that the mobile phone had been used to commit the offence, and the request to

disclose or implement the decryption key must have been made by a judicial authority.

31. The Government further argued that the purpose of Article 434-15-2 was not to obtain a confession from the suspect and did not constitute a presumption of guilt but was exclusively aimed at the decryption of data on a mobile phone. The Government stated that the applicant had been informed of the consequences of his refusal to disclose the decryption key for his mobile phone.

32. Lastly, they emphasised the need to combat drug trafficking effectively, as it seriously undermined public health and public order in general.

2. The third party's comments

33. Drawing on a comparative-law study, the non-governmental organisation Fair Trials pointed out that Belgium and England and Wales had provisions similar to those in France and that the courts in these Contracting States considered that the obligation to disclose a decryption key did not infringe the privilege against self-incrimination. The Netherlands did not have specific legislation on this matter, but its case-law took the same approach as in those States. In contrast, the Swedish Ombudsperson had taken the view that the use of force to place a finger on a mobile phone to unlock it failed to comply with the domestic law on fingerprints, which did not allow for such use.

34. The third party observed that the main rationale for the privilege against self-incrimination was to protect the accused from improper compulsion by investigation authorities, thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6.

35. It also argued that an obligation to disclose a decryption key facilitated the investigation by allowing investigators to access, without resorting to uncertain technical processes, information that might incriminate the suspect. This amounted to placing the burden of establishing the truth on the suspect.

36. Lastly, they submitted that the obligation to disclose a passcode was not one of the exceptions to the privilege against self-incrimination, as set out in the *Saunders* judgment (cited above). In their view, as all the exceptions related to biometric data, they did not apply to a passcode, which did not exist independently of a person's will.

3. The Court's assessment

(a) General principles

37. The right not to incriminate oneself is primarily concerned with respecting the will of an accused person to remain silent and presupposes that the prosecution in a criminal case seek to prove their case against the accused

without resorting to evidence obtained through methods of coercion or oppression in defiance of that will (see *Saunders*, cited above, §§ 68–69; *Jalloh v. Germany* [GC], no. 54810/00, §§ 100 and 102, ECHR 2006 IX; and *Bykov v. Russia* [GC], no. 4378/02, § 92, 10 March 2009). The right to remain silent during police questioning and the privilege against self-incrimination are generally recognised international standards which lie at the heart of a fair procedure under Article 6. Their aim is to provide an accused person with protection against improper compulsion by the authorities and thus to avoid miscarriages of justice and secure the aims of Article 6 (see *John Murray*, cited above, § 45; *Jalloh*, cited above, § 100; *Bykov*, cited above, § 92; and *Ibrahim and Others v. the United Kingdom* [GC], nos. 50541/08 and 3 others, § 266, 13 September 2016).

38. It is important to recognise that the privilege against self-incrimination does not protect against the making of an incriminating statement *per se* but, as noted above, against the obtaining of evidence by coercion or oppression. It is the existence of compulsion that gives rise to concerns as to whether the privilege against self-incrimination has been respected (see *Ibrahim and Others*, cited above, § 267). For this reason, the Court must first consider the nature and degree of compulsion used to obtain the evidence (see *Heaney and McGuinness v. Ireland*, no. 34720/97, §§ 54–55, ECHR 2000-XII, *O’Halloran and Francis*, cited above, § 55, and *Bykov*, cited above, § 92). The Court, through its case-law, has identified at least three kinds of situations which give rise to concerns as to improper compulsion in breach of Article 6. The first is where a suspect is obliged to testify under threat of sanctions and either testifies in consequence (see *Saunders*, cited above, and *Brusco*, cited above), or is sanctioned for refusing to testify (see *Heaney and McGuinness*, cited above, and *Weh v. Austria*, no. 38544/97, 8 April 2004). The second is where physical or psychological pressure, often in the form of treatment which breaches Article 3 of the Convention, is applied to obtain real evidence or statements (see, for example, *Jalloh*, cited above, and *Gäfgen v. Germany* [GC], no. 22978/05, ECHR 2010). The third is where the authorities use subterfuge to elicit information that they were unable to obtain during questioning (see *Allan v. the United Kingdom*, no. 48539/99, ECHR 2002-IX).

39. Testimony obtained under compulsion which appears on its face to be of a non-incriminating nature, such as exculpatory remarks or mere information on questions of fact, may be deployed in criminal proceedings in support of the prosecution case, for example to contradict or cast doubt upon other statements of the accused or evidence given by him or her during the trial, or to otherwise undermine his or her credibility. The privilege against self-incrimination cannot therefore reasonably be confined to statements which are directly incriminating (see *Ibrahim and Others*, cited above, § 268). According to the Court’s case-law, for statements to be regarded as self-incriminating it is sufficient for them to have substantially affected the

accused's position (see *Beuze v. Belgium* [GC], no. 71409/10, § 178, 9 November 2018).

40. However, the right not to incriminate oneself is not absolute (see *Heaney and McGuinness*, cited above, § 47; *Weh*, cited above, § 46; and *O'Halloran and Francis*, cited above, § 53). The degree of compulsion applied will be incompatible with Article 6 where it destroys the very essence of the privilege against self-incrimination (see *John Murray*, cited above, § 49). But not all direct compulsion will destroy that very essence and thus lead to a violation of Article 6 (see *O'Halloran and Francis*, cited above, § 53). What is crucial in this context is the use to which evidence obtained under compulsion is put in the course of the criminal trial (see *Saunders*, cited above, § 71, and *Ibrahim and Others*, cited above, § 269).

41. More recently (see *De Legé v. the Netherlands*, no. 58342/15, § 74, 4 October 2022), the Court has held that, in order for an issue to arise from the perspective of the privilege against self-incrimination, there must first be some form of coercion or compulsion exerted on the person concerned. That person must also be facing existing or anticipated criminal proceedings – that is to say, a “criminal charge” within the autonomous meaning of Article 6 § 1.

42. Where these prerequisites are met, it is necessary to determine whether the use of evidence obtained by means of coercion or compulsion should nevertheless be considered as falling outside the scope of protection of the privilege against self-incrimination. The privilege does not extend to the use in criminal proceedings of material obtained from an accused through methods of coercion when this material has an existence independent of his or her will (*ibid.*, § 75, with reference to *Saunders*, cited above, § 69).

43. If the prerequisites for the applicability of the privilege against self-incrimination are met (see paragraph 41 above), and the use of evidence obtained through coercion or compulsion does fall within the scope of protection of that privilege (see paragraph 42 above), it is necessary to examine whether the procedure did not extinguish the “very essence” of the privilege, that is to say, to determine the manner in which the overall fairness of the proceedings was affected. For this purpose, it will be necessary to have regard, in turn, to the following factors: the nature and degree of compulsion used to obtain the evidence; the existence of any relevant safeguards in the procedure; and the use to which any material so obtained is put (see *De Legé*, cited above, § 78).

(b) Application of those principles to the present case

44. The applicant contended that his conviction and sentence had infringed his right to remain silent and not to incriminate himself in relation to the drugs offences with which he had been charged.

45. With regard to his right to remain silent, the Court considers that, as noted by the Constitutional Council (see paragraph 8 above), the provisions of Article 434-15-2 of the Criminal Code are not intended to obtain a

confession from the suspect and do not imply any presumption of guilt. They are only intended to obtain the decryption of data and thereby prevent criminal offences and to help identify perpetrators. The Court would add, as will be demonstrated below (see paragraph 58), that the data contained in a mobile phone exists independently of the will of its user.

46. It further notes that the application of Article 434-15-2 of the Criminal Code is surrounded by a number of safeguards, namely the involvement of a judicial authority, the informing of the suspect that their refusal may give rise to criminal proceedings, and the need to demonstrate that the device was used in committing the offence and that the suspect knew the decryption key.

47. In relation to these elements, the Court finds no indication in the present case that there has been a breach of the right to remain silent.

48. With regard to the privilege against self-incrimination, the Court notes that the parties disagreed as to whether the application of Article 434-15-2 of the Criminal Code in this case fell outside the scope of protection afforded by this right. It will examine this question in the light of the conditions for the application of this right set out in *De Legé* (cited above).

49. In this regard, it considers, firstly, that the Government cannot validly argue that the only coercive measure to which the applicant was subjected was his detention in police custody. While police custody was an initial coercive measure enabling investigations to be carried out in the presence of the applicant and to question him about the offences he may have committed, the Court notes that the applicant, as is apparent from the interview record of 18 November 2017 (see paragraph 4 above), was subjected to a further indirect coercive measure when the investigator requested him to disclose the keys to unlock his mobile phones, while informing him that a refusal to do so would lead to prosecution for a fresh criminal offence (see, *mutatis mutandis*, *John Murray*, cited above, § 50). The Court reiterates, in this regard, that the situation of a suspect who is punished for refusing to give evidence may be such as to raise concerns about the existence of improper compulsion in breach of Article 6 (see *Heaney and McGuinness* and *Weh*, both cited above). The applicant was therefore subjected to a coercive measure when he was asked to disclose the decryption keys for his mobile phones.

50. Secondly, the Court observes that the conviction and sentence based on the provisions of Article 434-15-2 of the Criminal Code were the outcome of criminal proceedings brought against the applicant for drug-related offences, proceedings which fell within the scope of Article 6.

51. Thirdly, having established that these prerequisites have been met, the Court has to determine whether the refusal to disclose the decryption key and the resulting sanction fall within the scope of protection afforded by the privilege against self-incrimination.

52. In doing so, the Court has to first decide what information the police officers were seeking to obtain by subjecting the applicant to the contested coercive measure (see paragraph 49 above). It observes, on this point, that the

third-party intervener considered that the privilege against self-incrimination applied to the passcode that enabled access to the mobile phone, whereas the parties and domestic courts considered that it concerned the data contained on the device.

53. The Court shares the latter view. Admittedly, the offence for which the applicant was convicted related only to his refusal to disclose a decryption key for a “cryptographic means”. However, the only purpose of requiring suspects to disclose this key was to allow the authorities to implement it to access the data on the mobile phone and to search for evidence relating to the offence in question. The Court therefore considers that the complaint relates to the data contained in the mobile phones and not to the decryption key itself.

54. It further notes that the domestic courts held unanimously that the data existed independently of the applicant’s will. To reach this conclusion, the Court of Appeal (see paragraph 10 above), in a judgment upheld by the Court of Cassation (see paragraph 12 above), held that the data contained in the mobile phones could be obtained by other technical means. The Constitutional Council ruled in the same way, having noted that mobile phone data was “already fixed on a medium” (see paragraph 8 above).

55. The Court sees no reason to disagree with this solution. Unlike in cases where it has found a violation of Article 6 of the Convention on the grounds that the authorities did not possess the necessary information, and had no choice but to obtain it from the persons concerned by resorting to coercive powers that went against their will not to disclose that information (see *J.B. v. Switzerland*, no. 31827/96, ECHR 2001-III; *Funke v. France*, 25 February 1993, Series A no. 256-A; *De Legé*, cited above; and *Heaney and McGuinness*, cited above), in the present case, when the police officers asked the applicant to disclose the secret decryption keys for his mobile phones, his devices had already been seized during the search of his vehicle and the house search, meaning they were therefore already in the possession of the police.

56. However, the Court further notes, like the domestic courts and the Government, that the applicant was no longer the only person able to access the mobile phone data, since the use of technical means, especially in the area of forensic analysis, could have allowed authorities to override his refusal and gain access to the data contained on the devices.

57. The fact that, in this particular case, the investigators chose not to use such technical means, given the evidence already gathered, does not detract from this conclusion. Nor is this conclusion affected by the fact that the applicant himself purchased the mobile phones and installed applications or used them to take photographs.

58. It follows from the foregoing that the Court considers the data stored on the applicant’s mobile phones to have existed independently of his will. As a result, the privilege against self-incrimination did not apply to these data and there is no need to examine whether the proceedings in question impaired the very essence of this right.

59. Consequently, the Court concludes that this complaint must be declared inadmissible for being manifestly ill-founded pursuant to Article 35 §§ 3 (a) and 4 of the Convention.

B. The complaint under Article 8 of the Convention

60. The applicant contended that his conviction and sentence had breached his right to respect for his private life, in that Article 434-15-2 of the Criminal Code did not define the concepts of “cryptographic means” and “secret decryption key” with sufficient precision and did not provide for adequate safeguards in order to protect information contained in mobile phones. He relied on Article 8, of which the relevant parts read as follows:

“1. Everyone has the right to respect for his private life ...

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

61. The Government objected that the applicant had not raised this complaint before the domestic courts. The applicant did not reply on this point.

62. The Court reiterates that the purpose of the rule on the exhaustion of domestic remedies is to afford a Contracting State the opportunity of addressing, and thereby preventing or putting right, the particular Convention violation alleged against it. It is true that under the Court’s case-law it is not always necessary for the Convention to be expressly invoked in domestic proceedings, provided that the complaint is raised at least in substance. It would be contrary to the subsidiary character of the Convention machinery if an applicant, ignoring a possible Convention argument, could rely on some other ground before the national authorities for challenging an impugned measure, but then lodge an application before the Court on the basis of the Convention argument (see *Hanan v. Germany* [GC], no. 4871/16, § 148, 16 February 2021, and *Humpert and Others v. Germany* [GC], nos. 59433/18 and 3 others, § 151, 14 December 2023).

63. The Court notes that the applicant relied on Article 8 of the Convention before the Court of Cassation in only two grounds of appeal. In the first he challenged the argument that the data could be obtained by technical means, and in the second contended that the Court of Appeal had failed to examine whether the disclosure of the decryption key would lead the applicant to reveal information that did not exist independently of his will (see paragraph 11 above).

64. The Court considers that to examine the complaint of insufficient precision surrounding the legal terms under Article 8 of the Convention and of a lack of safeguards to protect the information contained in mobile phones

would be contrary to the purpose of the rule on the exhaustion of domestic remedies, given that the domestic courts were not called upon to rule on these issues in the proceedings.

65. The court concludes that the objection raised by the Government must be upheld and that this complaint is to be rejected on the grounds that domestic remedies had not been exhausted in accordance with Article 35 §§ 1 and 4 of the Convention.

For these reasons, the Court, unanimously,

Declares the application inadmissible.

Done in French, and notified in writing on 11 June 2026.

Victor Soloveytschik
Registrar

Kateřina Šimáčková
President