Compelled Decryption of a Mobile Phone

The Right Against Self-Incrimination in *Minteh v. France*

Javier Escobar Veas

30.06.2026 doi: 10.59704/c3a237eaf8049fd3

In *Minteh v. France*, decided in May 2026, the European Court of Human Rights held that compelling a suspect to reveal the password to a mobile phone does not violate the right against self-incrimination. The judgment addresses one of the defining and most contentious legal questions of the digital age, one that courts are currently grappling with (see, for example, German Federal Court and Dutch Supreme Court). And while courts across jurisdictions have adopted different frameworks, the ECtHR unanimously found no violation.

Minteh v. France is significant, but it is also unconvincing in its treatment of the challenges posed by new technology. In my view, rather than analyzing whether evidence exists independently of the suspect's will, courts should explore whether the defendant is compelled to actively participate in constructing the evidentiary case against themselves. This approach would be better able to tackle difficult legal questions like why compelling defendants to reveal their passwords is different from taking their fingerprints.

The Case

The defendant was stopped by French police for driving without a seatbelt. During the stop, officers discovered €6,680 in cash bearing traces of cocaine and cannabis, a block of cannabis resin, and a mobile phone inside the vehicle. A subsequent search of his home uncovered three additional phones, a tablet, and approximately €3,780. The defendant was taken into custody on suspicion of drug trafficking.

While in custody, the police asked the defendant to provide decryption keys for the seized phones. He invoked his right against self-incrimination and refused. Officers warned him that refusal constituted a separate criminal offense under Article 434-15-2 of the French Criminal Code, which criminalizes the refusal to disclose or implement a decryption key for a cryptographic device that may have been used in connection with a crime. He persisted in his refusal, and the police ultimately never accessed the phones' contents, having concluded that the other evidence was sufficient for a conviction.

Next to drug related offences, the trial court convicted the defendant for refusing to disclose the decryption method, an offense under the aforementioned legal provision. The Court of Appeals upheld the conviction, holding that there was no violation of the right against self-incrimination because the phone data existed independently of the defendant's will and that the authorities could theoretically have obtained it through technical means. In December 2019, the Court of Cassation dismissed his further appeal.

The ECtHR's Reasoning

The defendant challenged his conviction before the ECtHR under Article 6 (right to a fair trial) and Article 8 (right to privacy). The Article 8 complaint – that French legislation lacked sufficient precision and adequate safeguards for the highly personal information stored on smartphones – was declared inadmissible for failure to exhaust domestic remedies (§§ 60–65). The Court confined its substantive analysis to Article 6.

Under Article 6, the defendant contended that by threatening him with criminal prosecution if he refused to reveal his decryption keys, the French authorities had coerced him into assisting in his own prosecution. The ECtHR analyzed the right to remain silent and the right not to incriminate oneself separately.

On the former, the Court held that Article 434-15-2 does not intend to elicit a confession or presume guilt. Rather, its aim is to enable decryption of data to prevent offenses and identify perpetrators. The Court also found that the application of the legal provision is subject to several safeguards: judicial involvement, notification of the consequences of refusal, a requirement that the device be linked to the offense, and proof that the suspect holds the relevant key. Thus, the Court found no violation of the right to remain silent (§ 45-47).

Regarding the right not to incriminate oneself, the ECtHR found that, even though the defendant had been subjected to coercion, the evidence sought by the police was not covered by the right because of the so-called Saunders exception (§ 49-50). As established in *Saunders v. the United Kingdom*, the right against self-incrimination does not extend to evidence "which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect," such as blood samples and fingerprints.

In this case, the ECtHR held that the evidence sought by the police was not the decryption key itself, but the data contained in the phones. In the Court's opinion, this data existed independently of the defendant's will because the phones had already been seized and were in police possession. The ECtHR argued that this distinguishes the present case from others, such as *J.B. v. Switzerland* and *Funke v. France*, in which the authorities lacked the information entirely and could only obtain it through coercion. Furthermore, the ECtHR ruled that the defendant was no longer the sole individual with access to the information, as the police could access it via technical means. The investigators' decision not to pursue these methods, as they deemed the existing evidence to be sufficient, did not alter the analysis (§55-57). Accordingly, the Court found no violation of the right against self-incrimination.

The Evidential Value of the Decryption Key

Minteh v. France is the first ECtHR judgment to address compelled decryption and the right against self-incrimination directly, and its importance should not be underestimated. Yet, in my opinion, the decision leaves important questions unanswered and raises several problems.

Since the police ultimately wanted to access the data on the phones they had already seized, the ECtHR concluded that the existence of the evidence was independent of the defendant's will. Therefore, the right against self-incrimination did not apply to this evidence, also known as the Saunders exception.

However, this analysis mixes up the police's ultimate objective, i.e., the data contained in the phones, with their immediate objective, i.e., the decryption key that existed only in the defendant's mind. The Court overlooked the evidential value of the decryption key. Demonstrating that an individual possesses the decryption key for a digital device constitutes incriminating evidence, or, putting it more elegantly, it "furnishes a link in the chain of evidence" (*Hoffman v. United States*). This information establishes knowledge of the key and can be used to prove possession or control of the device's contents. This has been recognized, for example, by the U.S. Supreme Court in *Fisher v. United States*, where it held that complying with a subpoena tacitly acknowledges the existence and possession of the requested documents, as well as the individual's belief that the documents match the subpoena's description.

In conclusion, the police forced the defendant to provide incriminating information that existed only in his mind. By focusing solely on the data and ignoring the evidential value of the password, the Court bypassed the fundamental question rather than answering it.

The Saunders Exception and the Passwords

The distinction made in Saunders between evidence that exists independently of the defendant's will – such as blood samples, fingerprints, and DNA – and evidence that does not has long been criticized for being difficult to apply consistently (Escobar Veas 2025-2; Lamberigts; Redmayne). However, even accepting the Saunders distinction on its own terms, passwords sit firmly on the wrong side of it.

The ECtHR could reach this conclusion only by overlooking the independent evidential significance of the password itself. Forced disclosure of passwords naturally falls into the category of evidence that does not exist independently of the defendant's will. Unlike a fingerprint, a password must be remembered and communicated after being retrieved from memory. In the most direct sense, it is a product of the mind. Requiring its disclosure resembles compelled testimony more closely than taking a blood sample.

After all, what is the difference between forcing defendants to reveal a numerical password to their laptop, which contains incriminating messages and pictures, and forcing them to say where they hid the murder weapon? If the latter clearly engages the right against self-incrimination, it is difficult to see why the former does not.

Forensic Capabilities Influence the Scope of Rights

A central pillar of the judgment is the observation that the police could have accessed the phones through technical means. This reasoning raises two fundamental problems.

First, the ECtHR bases its conclusion on a hypothetical rather than an established fact. Modern smartphones use sophisticated encryption that even dedicated forensic tools cannot always bypass. (EUROPOL; BBC; Escobar Veas 2025-1). Whether independent technical access was actually feasible in the specific circumstances of this case, due to the models and software versions of the phones, as well as the encryption standards in use, was not proved.

But there is a deeper problem still. Under the Court's logic, the scope of the right against self-incrimination would be inversely proportional to the state's forensic capabilities: the more effectively authorities can bypass encryption, the weaker the protection afforded by the right. Conversely, if technology cannot circumvent a device's encryption, the right would apply. Fundamental protections, however, should not fluctuate with the commercial offerings of forensic technology companies. The point becomes even clearer if we think ahead to emerging brain-reading technologies: few would accept that the right against self-incrimination should evaporate the moment the state acquires the technical means to read a suspect's thoughts.

Final Reflection

The case of *Minteh v. France* reveals a deeper problem: The distinction outlined in *Saunders* is inadequate for the challenges posed by the digital age. The Court avoided confronting this inadequacy head-on by characterizing the disclosure of a password as merely a means of accessing pre-existing evidence.

The incoherence runs deeper than *Minteh* alone. When the Court distinguishes the present case from *J.B. v. Switzerland* and Funke v. *France* on the ground that the phones were already in police possession, it attempts to present its case law as internally consistent. However, as I have argued, the picture is not that simple. In both *Allen v. the United Kingdom* and *Van Weerelt v. the Netherlands*, the Court found no violation of the right against self-incrimination even though the tax authorities compelled the defendant to submit documents they did not already possess. In *Van Weerelt*, the ECtHR explicitly acknowledged that the Tax Authority had compelled the defendant "to give information that could not be obtained from any other source than the applicant himself for the purpose of levying taxes and interest in accordance with the applicable tax legislation." The possession of the evidence by the authorities, it turns out, is not the stable dividing line the Court implies it to be in *Minteh*.

Ultimately, *Minteh v. France* exposes the limits of a doctrine developed before new technologies became part of everyday life and justifies the need for a reinterpretation of the right. The question should no longer be whether evidence exists independently of the suspect's will, but whether the defendant is compelled to actively participate in building the case against themselves. This approach better explains why compelling defendants to reveal their passwords is different from taking their fingerprints or seizing their phones. Most importantly, it would explain why the answer to these questions should not depend on available forensic software.

I would like to acknowledge the Alexander von Humboldt Foundation for supporting the completion of this work with a Humboldt Research Fellowship.

ABOUT THE AUTHOR

Javier Escobar Veas

Javier Escobar Veas is an Alexander von Humboldt Research Fellow at the Max Planck Institute for the Study of Crime, Security and Law in Freiburg.Javier Escobar Veas is an Alexander von Humboldt Research Fellow at the Max Planck Institute for the Study of Crime, Security and Law in Freiburg.

SUGGESTED CITATION

Veas, Javier Escobar: Compelled Decryption of a Mobile Phone: The Right Against Self-Incrimination in *Minteh v. France*, Verfassungsblog, 30.06.2026, doi: 10.59704/c3a237eaf8049fd3.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260630-190617-0.