

Logical Foundations of Decryption Privacy

A Semantic Tableau Analysis of *Minteh v. France*

In accordance with the Semantic Tableau Consistency and Validity Testing Method

Contents

1	Introduction	2
2	The Semantic Tableau Method for Lawyers	2
2.1	Consistency Testing (Steps I–III)	2
2.2	Validity Testing (Steps I–III)	3
3	Formalization of the Legal Arguments	3
3.1	The Court’s Argument	3
3.2	The Applicant’s (Minteh’s) Argument	4
4	Semantic Tableau Validity Analysis	5
4.1	Validity Test of the Court’s Argument	5
4.1.1	Tree Explanation:	5
4.2	Validity Test of the Applicant’s Argument	6
4.2.1	Tree Explanation:	6
5	Logico-Legal Synthesis: Validity vs. Soundness	7
5.1	Why the ECHR Ruled the Court’s Premise is True	7
6	Broader Implications and Procedural Safeguards	7
6.1	The Article 8 Procedural Gate	7
6.2	The European Union Legal Context	8
7	Conclusion	8

1 Introduction

This report provides a formal logical analysis of the landmark European Court of Human Rights (ECHR) decision in *Lamin Minteh v. France* (Application no. 23624/20), sitting as a Chamber on 19 May 2026. The case centers on the criminal conviction of the applicant, Lamin Minteh, under Article 434-15-2 of the French Criminal Code for refusing to disclose the decryption keys (passcodes) of his mobile phones during police custody in November 2017.

During his initial arrest for driving without a seatbelt, police discovered cash contaminated with drugs and cannabis resin, leading to an expedited drug-trafficking investigation. A subsequent home search uncovered three additional mobile phones and further cash. While in custody, Minteh exercised his right to remain silent and refused to provide his passcodes. He was subsequently convicted of drug-trafficking offences and a separate offence for refusing to disclose the decryption keys.

Minteh appealed to the ECHR, arguing that his conviction and sentence for refusing to disclose the decryption key breached his right to remain silent and his privilege against self-incrimination under Article 6 § 1 of the Convention. He also raised a privacy claim under Article 8, asserting that the terms “cryptographic means” and “secret decryption key” lacked precision and that the law provided insufficient safeguards.

The Court declared the application inadmissible: the Article 6 § 1 complaint was rejected as manifestly ill-founded, and the Article 8 complaint was rejected for failure to exhaust domestic remedies. To rigorously evaluate the coherence of the legal arguments put forward by both the ECHR and the applicant, this report applies the formal **Semantic Tableau Method** as detailed in Appendix III of *Tableau.pdf* (Logic for Lawyers). This stepwise testing allows us to evaluate the consistency and validity of each argument and isolate the exact point of logico-legal divergence.

2 The Semantic Tableau Method for Lawyers

As outlined in Appendix III of *Tableau.pdf*, the semantic tableau method is a powerful tool for testing the consistency and validity of arguments. It proceeds by translating natural language statements into formal logic formulas, staying as close to the natural text as possible to provide the clearest representation of what has been said.

2.1 Consistency Testing (Steps I–III)

1. **Step I: Instantiate the formulas to closed sentences.** First-order logic formulas are instantiated using individual constants to eliminate quantifiers.
2. **Step II: Test the consistency of the closed sentences.** A tree (tableau) is constructed using inference rules.
 - Existential quantifiers are instantiated with a new individual constant (e.g., $x = a$).
 - Universal quantifiers are instantiated with all existing constants already in use (e.g., $x = a, x = b$).
 - If a branch contains a formula and its negation (e.g., $P(a)$ and $\neg P(a)$), that branch is *closed* (marked with $\times$).
3. **Step III: Draw a conclusion about the original set.** If at least one branch remains open, the set of sentences is *consistent*. If all branches are closed (no open branches are left), the set is *inconsistent*.

2.2 Validity Testing (Steps I–III)

To prove that an argument is logically valid (i.e., the conclusion must follow if the premises are true):

1. **Step I: Negate the conclusion.** Construct the negation of the conclusion and simplify using conversion formulas (e.g., $\neg\neg\Phi \equiv \Phi$).
2. **Step II: Test the consistency of this set.** Create a tableau containing the premises and the negated conclusion.
3. **Step III: Draw a conclusion.** If the tableau is closed, the set of closed sentences is inconsistent, meaning there is no situation in which the premises and the negation of the conclusion can be simultaneously true. Thus, the argumentation is **valid**. If the tableau remains open, the argumentation is **invalid**.

3 Formalization of the Legal Arguments

To analyze *Minteh v. France*, we establish the following domain of discourse: evidence and data. Let:

- $D(x)$ be the predicate: x is data stored on a mobile phone.
- $W(x)$ be the predicate: x exists independently of the suspect's will.
- $P(x)$ be the predicate: the privilege against self-incrimination applies to x .
- m be the constant representing the specific data on Lamin Minteh's mobile phones.

3.1 The Court's Argument

The ECHR's decision relies on three core premises to conclude that the privilege against self-incrimination does not protect the data on Minteh's phone.

Premise 1 (Pr_1): The privilege against self-incrimination 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 (relying on *Saunders v. UK* and *De Legé v. Netherlands*).

Formula: $\forall x(W(x) \rightarrow \neg P(x))$

Premise 2 (Pr_2): The data stored on a mobile phone exists independently of the suspect's will (relying on the fact that the data is already fixed on a medium and can be obtained by other technical/forensic means).

Formula: $\forall x(D(x) \rightarrow W(x))$

Premise 3 (Pr_3): The evidence requested from Lamin Minteh (m) is data stored on a mobile phone.

Formula: $D(m)$

Conclusion (C_{Court}): The privilege against self-incrimination does not apply to Lamin Minteh's mobile phone data.

Formula: $\neg P(m)$

3.2 The Applicant's (Minteh's) Argument

Minteh's defence and subsequent appeal relied on an alternative conception of the nature of digital data.

Premise 1 (M_1): The privilege against self-incrimination applies to evidence that does not exist independently of the suspect's will.

Formula: $\forall x(\neg W(x) \rightarrow P(x))$

Premise 2 (M_2): Data stored on a mobile phone does not exist independently of the suspect's will, because it only exists due to the suspect's conscious actions and will to create it, install apps, and take photos.

Formula: $\forall x(D(x) \rightarrow \neg W(x))$

Premise 3 (M_3): The evidence requested (m) is data stored on a mobile phone.

Formula: $D(m)$

Conclusion (C_{Minteh}): The privilege against self-incrimination applies to Lamin Minteh's mobile phone data.

Formula: $P(m)$

4 Semantic Tableau Validity Analysis

4.1 Validity Test of the Court's Argument

To test the validity of the Court's argument, we negate the conclusion:

$$\neg C_{\text{Court}} \equiv \neg\neg P(m) \equiv P(m)$$

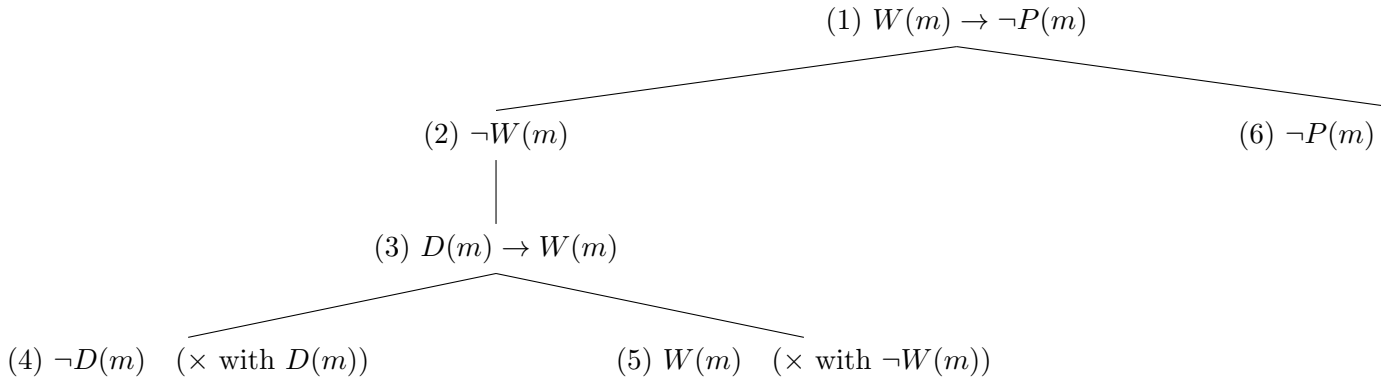
We now construct the semantic tableau for the set of formulas containing the premises and the negated conclusion:

$$\{\forall x(W(x) \rightarrow \neg P(x)), \quad \forall x(D(x) \rightarrow W(x)), \quad D(m), \quad P(m)\}$$

Since m is the only individual constant already in use (from $D(m)$ and $P(m)$), we perform universal instantiation on the first universal statement (Pr_1) with $x = m$:

$$(1) \quad W(m) \rightarrow \neg P(m)$$

This triggers a branching rule for implication. The resulting semantic tree is shown below:



4.1.1 Tree Explanation:

- At the root, we instantiate Pr_1 to $W(m) \rightarrow \neg P(m)$.
- **Right Branch:** Resolving the implication splits the tree. The right branch yields $\neg P(m)$. This directly contradicts our negated conclusion (Premise 4), $P(m)$. Thus, the right branch immediately **closes** ($\times$).
- **Left Branch:** The left branch yields $\neg W(m)$. We then instantiate the second universal statement (Pr_2) for $x = m$, yielding $D(m) \rightarrow W(m)$.
- This implication splits the left branch into two sub-branches:
 - **Left-Left Branch:** Yields $\neg D(m)$. This contradicts Premise 3, $D(m)$. The branch **closes** ($\times$).
 - **Left-Right Branch:** Yields $W(m)$. This contradicts the parent formula $\neg W(m)$ on the left branch. The branch **closes** ($\times$).

Because all branches of the tableau are closed, the set of sentences is inconsistent. In accordance with Step III of the validity test, the Court's argument is logically **valid**.

4.2 Validity Test of the Applicant's Argument

To test the validity of the applicant's argument, we negate his conclusion:

$$\neg C_{\text{Minteh}} \equiv \neg P(m)$$

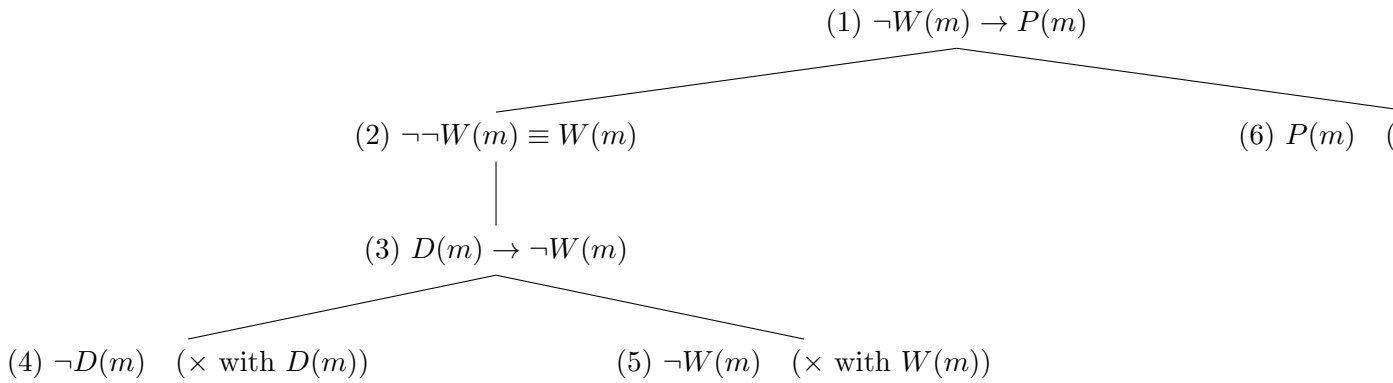
We construct the tableau for the set containing Minteh's premises and his negated conclusion:

$$\{\forall x(\neg W(x) \rightarrow P(x)), \quad \forall x(D(x) \rightarrow \neg W(x)), \quad D(m), \quad \neg P(m)\}$$

We instantiate the first universal statement (M_1) for $x = m$:

$$(1) \quad \neg W(m) \rightarrow P(m)$$

The resulting semantic tree is shown below:



4.2.1 Tree Explanation:

- At the root, we instantiate M_1 to $\neg W(m) \rightarrow P(m)$.
- **Right Branch:** Yields $P(m)$, which contradicts our negated conclusion $\neg P(m)$. The branch immediately **closes** ($\times$).
- **Left Branch:** Yields $\neg\neg W(m)$, which simplifies to $W(m)$. We then instantiate M_2 for $x = m$, yielding $D(m) \rightarrow \neg W(m)$.
- This implication splits the left branch:
 - **Left-Left Branch:** Yields $\neg D(m)$. This contradicts Premise 3, $D(m)$. The branch **closes** ($\times$).
 - **Left-Right Branch:** Yields $\neg W(m)$. This directly contradicts the parent formula $W(m)$ on the left branch. The branch **closes** ($\times$).

Since all branches are closed, the negated conclusion is inconsistent with the premises. Thus, Lamin Minteh's argument is also logically **valid**.

5 Logico-Legal Synthesis: Validity vs. Soundness

The semantic tableau analysis yields a highly compelling result: ****both the European Court of Human Rights and the applicant, Lamin Minteh, developed logically valid arguments****. In formal logic, an argument is valid if the conclusion must follow from the premises. However, because they lead to contradictory conclusions ($\neg P(m)$ vs. $P(m)$), they cannot both be ****sound**** (a sound argument must be logically valid ***and*** have true premises).

The absolute point of divergence is isolated in their respective second premises:

The Court’s Premise 2: $\forall x(D(x) \rightarrow W(x))$

Data stored on a mobile phone exists independently of the suspect’s will.

The Applicant’s Premise 2: $\forall x(D(x) \rightarrow \neg W(x))$

Data stored on a mobile phone does not exist independently of the suspect’s will.

The entire legal battle in *Minteh v. France* was not about logical coherence, but about this fundamental philosophical and legal premise: ****Does encrypted digital data exist independently of the suspect’s will?****

5.1 Why the ECHR Ruled the Court’s Premise is True

The ECHR aligned with the French Constitutional Council, the Paris Court of Appeal, and the Court of Cassation in holding that the data stored on mobile phones does exist independently of the applicant’s will:

1. **Physical Fixation:** The data is “already fixed on a medium” and exists physically and digitally on the device independently of what the suspect thinks or does.
2. **Forensic Extractability:** The Court noted that the data on the mobile phones could be obtained by other technical means (such as forensic computer analysis), regardless of whether the suspect provides the passcode. The fact that the police in this specific case chose not to perform this analysis due to the overwhelming independent evidence already collected does not alter the fact that the data is theoretically extractable without his active mental participation.
3. **Distinction Between Key and Data:** The Court clarified that while a decryption key or passcode is a mental concept, the legal complaint relates to the *data* contained within the phone, which exists independently of the will, rather than the key itself.

Thus, the ECHR declared that the privilege against self-incrimination does not apply to this data, rendering the Court’s argument both valid and sound, while Minteh’s argument is unsound due to a false Premise 2.

6 Broader Implications and Procedural Safeguards

While the ECHR restricted the scope of Article 6 § 1 (self-incrimination) by treating mobile phone data as independent physical evidence, the legal protection of mobile phone data in Europe remains complex and highly regulated.

6.1 The Article 8 Procedural Gate

The applicant also raised a substantive challenge under Article 8 of the Convention (Right to respect for private life), arguing that Article 434-15-2 of the French Criminal Code did not define the concepts of “cryptographic means” and “secret decryption key” with sufficient precision and lacked adequate safeguards.

However, the ECHR dismissed this complaint for failure to exhaust domestic remedies (under Article 35 §§ 1 and 4). Before the French Court of Cassation, Minteh’s appeal only challenged whether the data existed independently of his will and whether disclosure would force him to reveal non-independent information. He did not explicitly raise the lack of legal precision or the inadequacy of safeguards. This highlights the strictness of the ECHR’s procedural gates: national courts must be given the first opportunity to address and rectify alleged violations before they can be brought to Strasbourg.

6.2 The European Union Legal Context

Although the ECHR declared Minteh’s application inadmissible, broader European Union law provides separate, rigorous procedural constraints on police access to mobile phone data. In the landmark case *Bezirkshauptmannschaft Landeck* (C-548/21), decided on 4 October 2024, the Grand Chamber of the Court of Justice of the European Union (CJEU) clarified that:

- National rules permitting police access to mobile data must define with sufficient precision the nature or categories of offences concerned.
- Reliance on such access must respect the principle of proportionality.
- Access must be subject to prior review by a judge or an independent administrative body, except in duly justified cases of urgency.

This shows that while a refusal to provide a passcode can be penalized under domestic criminal law without violating the privilege against self-incrimination (according to ECHR standards), the police’s actual access to the phone’s contents is heavily constrained by EU data protection law (Directive 2016/680) and judicial review requirements.

7 Conclusion

By applying the stepwise Semantic Tableau method to *Minteh v. France*, we have demonstrated that both the ECHR and the applicant developed perfectly valid logical frameworks. The decision of the ECHR to reject Minteh’s application represents a major legal precedent: digital data on mobile phones is classified as independent evidence, analogous to blood samples or documents found during a physical search. Consequently, refusing to provide a decryption passcode can be prosecuted as an independent offence under Article 434-15-2 of the French Criminal Code, provided that the necessary procedural safeguards (such as involvement of a judicial authority and proof of device use in the offence) are respected.