Lamin MINTEH v. France (No. 23624/20)
(Fifth Section)
Written submission of Fair Trials

BACKGROUND

These written comments are submitted by Fair Trials, in accordance with the leave to intervene granted by the President of the Fifth Section and notified to Fair Trials by a letter of 31 January 2022 in accordance with Article 44§3(a) of the Rules of Court.

Fair Trials' work focuses on the right to a fair trial protected by Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the Convention). We intervene in this case because it raises important questions concerning the privilege against self-incrimination and right to silence under Article 6§1. The case gives the Court an opportunity to clarify the applicability of Article 6 to the widespread practice across Europe by police and law enforcement authorities of requesting or requiring suspects or accused persons to hand over the access codes of their mobile devices containing potentially incriminating information, including, as is the case in France, under threat of a criminal sanction.

INTRODUCTION

In this case, the applicant was charged and sentenced pursuant to Article 434-15-2 of the French Criminal Code for refusing to communicate the access code to his mobile telephone to police officers while in police custody.[1] In these submissions, we will focus on the Court's question to the parties, as to whether the applicant's criminal conviction for refusing to disclose the access code to his mobile phone to the police infringes his right to remain silent and not to contribute to his own incrimination as guaranteed by Article 6 of the Convention.

Fair Trials has been monitoring practices across Europe related to so-called 'decryption orders', understood as requests for suspects or accused persons to unlock their mobile devices either by providing passcode or biometric (facial recognition or fingerprints) access under threat of a criminal sanction or execution of the order by force. To date, national legal frameworks and case law vary as to the compatibility of such practices with the privilege against self-incrimination and right to remain silent.

We will first draw the Court's attention to the existing practices in relation to decryption orders we have observed in the Contracting Parties (Part 1). We will then address why decryption orders do not fall within the acceptable exceptions to the privilege against self-incrimination and right to silence under Article 6(1) (Part 2). Finally, in Part 3 we will draw the Court's attention to the shortcomings in the practical application of safeguards both prior (*ex ante*) and after (*ex post*) the issuing and execution of a decryption order and subsequent searches of mobile devices. In view of the risks involved in sanctioning such practices, particularly in light of the highly private nature of the information that is likely to be contained in mobile phones,

[1] Article 434-15-2 of the French Criminal Code provides that : «*le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités (…)*».

we urge the Court to take a principled approach aimed at preserving a robust standard of the privilege against self-incrimination, to prevent incentives to rely on coercive investigative methods in cases where traditional methods of investigation present additional difficulties.

PART 1 – OVERVIEW OF STATE OF PLAY IN SEVERAL CONTRACTING PARTIES

By way of background, mobile devices have become an indispensable part of our lives. Given the amount of information, including highly sensitive personal data they contain, investigative authorities have an increasing interest in securing access to their contents. National practices in this respect vary. In this first part, we will highlight how different courts concluded that the privilege against self-incrimination does not apply. In France, Belgium and England & Wales, courts have considered that the privilege against self-incrimination does not apply to the request of a passcode or it is not substantially infringed. Interestingly however, the courts in the Netherlands and the Ombudsperson in Sweden did not adopt the same approach.

France

Law enforcement authorities may compel suspects to provide the passcode to their mobile device under threat of a legal sanction pursuant to Article 434-15-2 paragraph 1 of the French Criminal Code,[2] which was introduced by *Law No: 2016-731 of June 3, 2016 strengthening the fight against organized crime, terrorism and their financing*. The request must be sanctioned by a judicial authority, and in order to prosecute a person under this provision, judicial authorities must show that the refusal of the request to unlock the mobile device is intentional. In addition, the offence implies that an encryption method is used to prepare, facilitate or commit a crime or offence. On 13 October 2020 the Criminal Chamber of the French Court of Cassation (*Cour de Cassation*) ruled that the code to a mobile phone constitutes such an encryption method. The existence of such a method can be inferred from the characteristics of the device or the software it is equipped with, *inter alia*.

On 30 March 2018, the French Constitutional Council (*Conseil Constitutionnel*), in the priority preliminary ruling on constitutionality No. 2018-696, decided that the obligation to provide a decryption key under Article 434-15-2 of the French Criminal Code does not infringe the right against self-incrimination, respect for privacy and secrecy of correspondence, the rights of the defence, the principle of constitutionality of sentence and freedom of expression, nor any other right or freedom guaranteed by the French Constitution.

The French courts recognise that a refusal to reveal the passcode to a mobile phone may therefore constitute an offence under Article 434-15-2 of the French Criminal Code. This means that suspects and accused persons may be subject to (and threatened with) an obligation to unlock their mobile devices, which potentially contain incriminating information, or face a criminal prosection and conviction carrying the potential sentence of imprisonment up to 3 years and EUR 270 000 in fine.

Belgium

[2] This provision states that: "*[a]nyone who has knowledge of the secret agreement to decrypt a cryptology method that may have been used to prepare, facilitate or commit a crime or offence, shall be required to hand over the said agreement to the judicial authorities or to implement it, pursuant to orders from these authorities issued under Titles II and III of Book I of the French Code of Criminal Procedure*."

The applicability of the privilege against self-incrimination to obtain access to mobile phone devices was also recently assessed in Belgium. In a case concerning a drug trafficking offence, the accused person was prosecuted for refusing to reveal the passwords of two mobile phones found at his premises.[3] The accused was first acquitted by the Ghent Court of Appeal on the basis that the decryption order violated his right to remain silent and the prohibition of self-incrimination,[4] which stems from the presumption of innocence as set out in Article 6§2 of the Convention. Previous court decisions had also considered that a passcode exists independently from the person's will and, therefore, was subject to the privilege against self-incrimination.[5]

However, on appeal, the Belgian Court of Cassation considered that the privilege against self-incrimination and the presumption of innocence are not absolute and needed to be weighed against other rights such as the right to freedom and security guaranteed by Article 5 and the prohibition of abuse of rights detailed in Article 17 of the Convention. The court confirmed that an investigating judge may order, subject to a criminal sanction, including imprisonment, a suspect to provide the passcode to his mobile phone where decryption is vital for truth finding.[6] This was treated as an "informational" obligation rather than an obligation to cooperate with the investigation.

It is apparent from the Belgian court's assessment that the right not to incriminate oneself primarily aims to avoid false statements made under coercion and, thus, produce unreliable evidence. That court treated the passcode as "static evidence" which exists independently of the suspect's will, so there is no risk of it being unreliable. The code is "neutral" (as opposed to the information that may be contained in the phone) and cannot, in itself, be considered as self-incriminating. The court stressed that the investigator had already located the device at the time the password was requested without subjecting the person to coercion and that the prosecuting authority demonstrated that the person in question knew the access code without reasonable doubt.

The court also noted that the current state of technology made it difficult, if not impossible, for investigators to gain access to a computer system protected by an encryption application, while such applications are readily available. Therefore, the passcode was necessary to establish the truth.[7]

In parallel, the Belgian Constitutional Court was asked whether the relevant provision violated the principle of equality and the right to a fair trial. The question was asked because a refusal to provide information on how to access a computer system or how it operates (obligation to provide information) is always criminally punishable, whereas the refusal to collaborate by activating the computer system or performing certain operations on it (obligation to cooperate) is not criminally punishable for the suspect and their relatives. The court held that the difference of treatment was reasonably justified since: "[i]n the first case, the accused is asked to provide information enabling access to a particular computer system, provided that this information exists independently of his or her will, so that the right not to contribute to his or

[3] As can be required by an investigative judge pursuant to Article 88*quater* of the Belgian *Code d'instruction criminelle.*
[4] Stibbe, *Supreme Court approves criminal liability of suspect refusing to unlock his smartphone,* 6 February 2020.
[5] See e.g. Corr. Anvers, 11 janvier 2018, N.C., n°5, p.515; Corr. Termonde, 17 novembre 2014, T.Strafr., 2016, n°3, p. 258.
[6] Article 88*quater* of the Belgian *Code d'instruction criminelle.*
[7] Hof v. Belgium Court of Cassation, Decision of 4 February 2020, P.19.1086.N, § 8.

her own accusation does not apply, whereas in the second case, he or she is asked to participate actively in the operations carried out in the computer system, i.e. to take an active part in the collection of evidence of the offence, which would be likely to lead him or her to contribute to his or her own accusation. [Our translation]".[8] The court concluded that requests for mobile phone passcodes were, therefore, compatible with the Belgian Constitution.

England and Wales

In England and Wales, police authorities can formally demand access to electronic data held on phones, laptops or other electronic devices, which are protected by encryption, that police have seized as part of an investigation, under the Regulation of Investigatory Powers Act (RIPA) 2000. Originally introduced as an anti-terrorism power, it is increasingly used by police investigating a broad range of criminal offences.

If the police have seized an electronic device belonging to a person under investigation which is protected by encryption via a 'key', the police will request the key. A key can be a code, password, algorithm or other data (including cryptographic process), the use of which, by itself or with another key or keys, allows protected electronic data to be accessed.[9] If the person does not provide the key, police may then make an application to the court for written permission to serve a formal 'notice requiring disclosure' under Section 49 of RIPA. Permission must be granted by a judge. In case of failure to comply with a notice to disclose under section 49 RIPA 2000, the maximum sentence is two years, or if the case concerns 'national security' or 'child indecency', the maximum sentence is 5 years. In 2019, all approvals of section 49 notices (139 out of 139) were granted, none were refused.[10]

There have been multiple cases dealing with the obligation to unlock mobile devices in England and Wales[11] with most judgments finding the obligation to reveal a mobile phone passcode compatible with the privilege against self incrimination. For example in *R. v S. and A.* Sir Igor Judge concluded: "[o]n analysis, the key which provides access to protected data, like the data itself, exists separately from each appellant's "will". Even if it is true that each created his own key, once created, the key to the data, remains independent of the appellant's "will" even when it is retained only in his memory, at any rate until it is changed."[12]

The Netherlands

There is no legal obligation on a suspect to provide a passcode. However, the case law recognises that a suspect may be physically coerced to provide biometric data for the purposes of unlocking the phone. The Supreme Court of the Netherlands (*Hoge Raad der Nederlanden*) in its decision[13] of 9 February 2021 concluded that forcing suspects to provide access to their smartphone with a fingerprint is not a breach of the privilege against self-incrimination. The case concerned a forced unlocking of a seized suspect's smartphone using his fingerprint. After his refusal to unlock the phone, the suspect was handcuffed and his thumb placed on the fingerprint scanner of the phone. The suspect filed a complaint to the Court of

[8] Constitutional Court of Belgium, Judgment No. 28/2020 of 20 February 2020, § B.6.2.
[9] Home Office, "Investigation of Protected Electronic Information - Revised Code of Practice", August 2018.
[10] Investigatory Powers Commissioner's Office, "Annual Report of the Investigatory Powers Commissioner 2019", HC 1039, 15 December 2020.
[11] See e.g., *R v S and A* [2008] EWCA Crim 2177, All ER (D) 89 (Oct); *R v Kearns* [2002] EWCA Crim 748; *R v Rabbani* [2018] EWHC 1156 (Admin).
[12] *R v S and A* [2008] EWCA Crim 2177, All ER (D) 89 (Oct), § 20.
[13] Supreme Court of the Netherlands, Decision No. 19/05471 CW, 9 February 2021.

North Holland and subsequently to the Supreme Court of the Netherlands. The Supreme Court upheld the reasoning of the Court of North Holland and held that the privilege against self-incrimination mainly covers statements made under duress and is primarily concerned with respecting the will of an accused person to remain silent. Material that exists independently of the suspect's will may be obtained under coercion, as for instance applies to blood and urine samples.

However, the court distinguished the taking of fingerprints and the request for a passcode. Unlike the situation in which the accused is forced to give the access code of his phone, which requires a statement by the accused, placing a thumb on the phone does not, in the opinion of the court, violate the right not to incriminate oneself. The Supreme Court considered that this is because it involves merely tolerating an investigative measure that does not require the active cooperation of the suspect. In addition, the fingerprint was obtained with a very small degree of coercion. The fact that after placing the suspect's thumb on the phone, investigators accessed data that may be incriminating was not a decisive factor.[14]

Sweden

In relation to the taking of fingerprints, the Swedish Parliamentary Ombudsman (*Riksdagens Ombudsmän or Justitieombudsmannen*), in its decision[15] of 3 June 2020, examined a case where a prosecutor granted a request from the Swedish Customs Office to put the finger of a suspect on his phone in order to unlock a specific application on the phone. The person in question was suspected of serious smuggling of doping substances.[16] During a house search, the suspect's computer and phone had been seized and the suspect had refused to unlock his phone.[17] He was then informed about the order to unlock his phone and asked to consult his lawyer, which was refused.[18] The Prosecutor had based the order on Chapter 28, Article 14 of the Swedish Code of Criminal Procedure (RB 28:14) which allows for the collection of fingerprints from a suspect where they are necessary for comparative forensic analysis in the course of the investigation. However, the Ombudsman was of the opinion that the aim of the provision was to collect information about the fingerprint pattern which is unique to each person and which is found on the person's finger. The image of this pattern could be saved and used for comparison with prints taken earlier.[19]

The Ombudsman noted that in this case, the purpose of taking the suspect's fingerprint was essentially different from the one envisaged in Chapter 28, Article 14 of the Code of Criminal Procedure. Namely, the purpose was to unlock an application stored on his phone in order to access messages which could be of significance for the investigation.[20] Requesting a fingerprint for this reason and putting it on the phone did not have a direct purpose in the investigation (collection of evidence directly). Instead, the taking of the fingerprint was a means to unlock the phone and enable the investigators to go through its content.[21] The Ombudsman based its decision on Chapter 2 Article 6 of the Instrument of Government, which forms a part of the Swedish Constitution and requires that any provision that allows for a violation of a

[14] Supreme Court of the Netherlands, Decision No. 19/05471 CW, 9 February 2021, § 4.
[15] Riksdagens Ombudsmän, JO Decision, No. 6849-2018, 3 June 2020.
[16] Riksdagens Ombudsmän, JO Decision, No. 6849-2018, 3 June 2020, p. 1 – 2.
[17] Ibid.
[18] Ibid., p. 2.
[19] Ibid., p. 8.
[20] Ibid., p. 8 – 9.
[21] Riksdagens Ombudsmän, JO Decision, No. 6849-2018, 3 June 2020, p. 9.

person's physical integrity must be interpreted restrictively.[22]

In view of such diverging approaches in Contracting States, there is a need for clarity from the Court on the applicability of the privilege against self-incrimination to requests for passcodes to mobile phone devices from suspects.

PART 2 – APPLICABILITY OF THE PRIVILEGE AGAINST SELF-INCRIMINATION

While the Court has addressed the privilege against self-incrimination and the right to silence on multiple occasions, it has not previously dealt with the matter of whether compelling a suspect to provide the authorities with the password to their mobile phone falls within the scope of these rights. In this part, we explain why we consider that the privilege against self-incrimination applies to so-called 'decryption orders' and does not fall within acceptable exceptions to the privilege against self-incrimination and right to silence. More specifically, we explain why an obligation to disclose a mobile phone passcode in a form of a statement is substantively and practically incomparable with the other accepted exceptions from the privilege against self-incrimination.

Scope of the privilege against self-incrimination and right to silence

The right to remain silent and the privilege against self-incrimination are recognised international standards that form an integral part of a fair criminal process and is guaranteed to all persons charged with a criminal offence. This right is expressly protected by Article 48 of the Charter of Fundamental Rights of the European Union and laid out in more detail in Article 7 of the Presumption of Innocence Directive of the European Union (EU).[23] On an international level, both the International Covenant on Civil and Political Rights (Article 14(3)(g)) and the American Convention on Human Rights (Article 8(2)(g)(3)) contain the right to not be compelled to incriminate oneself. Neither of the two rights are expressly mentioned in the Convention, however the case-law of this Court has made it clear that this right is protected under Article 6(1).[24]

The privilege against self-incrimination lays at the heart of the notion of a fair procedure under Article 6[25] and plays a fundamental role in protecting defendants against abuses of power in criminal investigations. The Court has recognised that the main rationale for the privilege against self-incrimination is the protection of the accused against the improper compulsion by investigation authorities, thereby contributing to the avoidance of miscarriages of justice and the fulfilment of the aims of Article 6.[26] The privilege against self-incrimination essentially means that the prosecution cannot seek to prove its case in a criminal trial based on evidence "obtained through methods of coercion or oppression in defiance of the will of the accused."[27]

In addition, this Court has recognised that the privilege against self-incrimination extends not only to statements (evidence) that are directly incriminatory, but also to other information which, although not directly incriminatory, can be used against the accused to contradict or cast doubt on other statements of the accused or evidence given by them during the trial, or

[22] Instrument of Government (Regeringsformen) (1974:152), Chapter 2, Article 6.
[23] Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings.
[24] *Funke v. France*, App. No. 10828/84, 25 February 1993, § 44.
[25] *Pishchalnikov v. Russia*, App. No. 7025/04, 24 September 2009, § 77.
[26] *Ibid.,* § 77.
[27] *Saunders v. the United Kingdom* [GC], App. No. 19187/91, 17 December 1996, § 68.

to otherwise undermine their credibility.[28] The defendant's privilege against self-incrimination is intended to protect them from being coerced or pressured into contributing to their own conviction by assisting the investigative authorities to obtain information that can be used against them in a criminal trial.

It is well-recognised that the privilege against self-incrimination is not absolute. In *Saunders v. the United Kingdom*, for example, the Court listed types of material which exist independently of the will of a suspect and fall outside the scope of the right, such as documents acquired pursuant to a warrant, breath, blood, DNA or urine examples.[29] The exceptions are based on the recognition that, although they may be acquired through the use of compulsory powers, they have an existence independent of the will of the suspect.[30] Blood, DNA, urine and similar samples in particular are taken from the accused person to compare with samples that are already collected at the crime scene or other relevant locations during a criminal investigation.

The Court has also recognised other limited exceptions where the person charged with a criminal offence may be requested to provide information or actively cooperate with the investigation. Generally, these exceptions relate to information that may benefit the accused, for example, to refute a legal presumption that a car owner (registered keeper) is responsible for traffic violations committed with their car unless they can identify the driver.[31] Another common example of such exception is the obligation to provide an alibi or refute certain legal presumptions in relation to proceeds of crime.

An obligation to provide a passcode is not covered by the exceptions

In our view, a request to provide a passcode to unlock a mobile device does not fall within acceptable exceptions to the privilege against self-incrimination as it undermines the very essence of the privilege against self-incrimination.

First, a passcode cannot be said to exist independently of a person's will as, for instance, biometric data. Security settings such as passcodes and access mechanisms using biometric data are designed to protect mobile devices and information stored on them from unauthorised access by other persons. They serve as a key ensuring that only the person(s) in possession of such a key can use the mobile device and access the information stored therein. A person makes a voluntary decision to set up a passcode and makes a choice of a passcode among different available security mechanisms. The person can also change the code as and when they decide to.

Access details therefore do not exist independently of the accused person's will in the same sense as forensic comparative samples. To rule otherwise would open the door for sanctioning court-imposed legal obligations to reveal the location or give access to any object that exists in its physical form 'independently of the will of the accused' such as tools used for the commission of a crime, location of crime proceeds, a body or any other similar evidence.

Second, a legal obligation to provide a passcode is essentially a requirement for the suspect to hand over, through a statement, a key to information which may directly contribute to the collection of incriminating evidence contained in the phone. Such a requirement inevitably involves an obligation for the suspect to actively assist the investigation against them, by

[28] *Ibid.,* § 69.
[29] *Saunders v. the United Kingdom* [GC], App. No. 19187/91, 17 December 1996, § 69.
[30] Ibid.
[31] *O'Halloran and Francis v. the United Kingdom* [GC], App. Nos. 15809/02, 25624/02, 29 June 2007.

providing access to information that would otherwise be difficult for the investigators to obtain through other means. Thus, the obligation to provide a passcode serves only the purpose of facilitating the investigation against the will of the accused to remain silent. This was noted by the Belgian Court of Cassation in its decision mentioned in Part 1 where it observed that "the current state of technology makes it very difficult, if not impossible, to gain access to a computer system protected by an encryption application, while such applications are readily available."[32]

Establishing the truth must remain the obligation of the investigative authorities and cannot be transferred to the suspect, at the expense of the privilege against self-incrimination and right to silence in cases where the investigation faces practical difficulties.

Third, a legal obligation to provide a passcode to a mobile device (or any other biometric data for the purpose of unlocking the phone) is fundamentally different from an obligation to provide a comparative sample such as fingerprints, DNA, blood, urine or similar samples taken from a person's body. The purpose of collecting the latter is to obtain a comparative sample, thus the fingerprint, DNA, blood or urine sample and, more specifically, information they provide after forensic analysis is the information sought by the investigation. This material only exists in (or is produced by) the body of the accused person and genuinely cannot be obtained by any other means. These samples cannot be produced or accessed in any other way and are themselves part of the 'real' evidence in the case.

This is not the case for a passcode which needs to be obtained for the purposes of accessing the contents of a phone, since law enforcement may be authorised to use forensic tools to access information on electronic devices without compelling the disclosure of a passcode. For instance, in Belgium, investigative authorities may instead employ the necessary forensic tools to "hack" a mobile device.[33]

Finally, coercion is inextricably linked to an obligation on a suspect to make a statement, in the form of a passcode, in the same way as the Court recognised in *Funke v. France.* In that case, the applicant was convicted for a failure to comply with a legal obligation to provide potentially incriminating documents to investigative (customs) authorities. The Court noted that "being unable or unwilling to procure them by some other means, they [customs authorities] attempted to compel the applicant himself to provide the evidence of offences he had allegedly committed."[34] In the Court's view, special features of customs law could not justify such an infringement of the privilege against self-incrimination and found a violation of Article 6(1) of the Convention.[35]

An obligation to provide a passcode in the form of a statement (either verbally or by entering the code directly in the device) presents risks of ill-treatment. It has been a long-standing view of the Court that statements obtained from suspects or accused persons by means of threats or other forms coercion or ill-treatment cannot be used to secure a conviction.[36] This extends to statements that are indirectly incriminating or can otherwise be used against the accused.[37] Reliance on confessions or other incriminating statements to speed up investigations in

[32] *Hof v. Belgium,* Court of Cassation of Belgium, Decision of 4 February 2020, P.19.1086.N, § 8.
[33] Article 39bis of the Belgian *Code d'instruction Criminelle*.
[34] *Funke v. France*, App. No. 10828/84, 25 February 1993, § 44., see also *J.B. v. Switzerland,* App. No. 31827/96, 03 May 2001, §§ 63-71.
[35] Ibid., § 45.
[36] See *Jalloh, v. Germany* [GC], App. No. 54810/00, 11July 2006 , § 110., see also *Gäfgen v. Germany* [GC], App. No. 22978/05, 1 June 2010, § 166.
[37] *Saunders v. the United Kingdom* [GC], App. No. 19187/91, 17 December 1996, § 69.

criminal proceedings have been recognised as a particular contributing factor to a heightened risk of ill-treatment.[38]

Therefore, the privilege against self-incrimination, which is designed to protect against undue coercion, should fully apply to any obligation to reveal access details to mobile devices to investigative authorities.

PART 3 – BROADER IMPLICATIONS ON THE OVERALL FAIRNESS OF PROCEEDINGS

The importance of extending the privilege against self-incrimination to phone passcodes can be emphasised by reference to the broader context and risks involved in searches of digital devices. The possibility to obtain an *ex post* remedy at trial (if a trial ensues) in the form of exclusion of evidence gathered in violation of defendant's rights, in particular the right to privacy, would be wholly insufficient. The privilege against self-incrimination helps instead prevent violations of rights *ex ante* in the evidence gathering process.

Although searches of digital devices for investigative purposes have been carried out for decades, the functions, uses and storage capacity of devices such as smart phones has grown exponentially. The privacy interests at stake are significant because "smartphones are in fact minicomputers that also happen to have the capacity to be used as a telephone".[39] Today, mobile phones contain not only personal correspondence on various platforms (emails, messaging apps, social media, text messages), but also potentially information about banking transactions, personal videos and photographs, health and medical information, activity and movement patterns and a vast amount of other private information. Therefore, smartphones are becoming an increasingly attractive source of information to investigative authorities and have an enormous potential to contain information that can be used against the suspect (or others) either directly or indirectly.

National legal frameworks may provide prior safeguards for any search of digital devices, including the requirement for a judicial decision ordering access to the phone, involving a necessity and proportionality assessment. However, such a safeguard does not change the nature of the obligation to reveal the passcode and its fundamental incompatibility with privilege against self-incrimination. In addition, any search of a digital device must be accompanied by appropriate safeguards regardless of whether the access to such device is provided by the suspect or gained by investigative authorities through other means. The Court has observed in relation to a warrant issued for the search of premises that "whilst a highly relevant consideration, the fact that an application for a warrant has been subject to judicial scrutiny will not in itself necessarily amount to a sufficient safeguard against abuse."[40]

In order to determine whether a search ensured adequate safeguards against abuse, a number of factors need to be assessed, including the circumstances in which the warrant was issued, in particular the other evidence available at the time, the content and scope of the warrant, the way in which the search was carried out, including the presence or absence of independent observers, and the extent of the possible repercussions on the work and reputation of the person targeted by the search.[41] The Court has also stressed that "effective supervision" of measures infringing Article 8 of the Convention is an important guarantee

[38] Fair Trials and REDRESS, *Tainted by Torture. Examining the Use of Torture Evidence*, 2018, p. 44; Fair Trials, *Efficiency over Justice: Insights into Trial Waiver Systems in Europe*, 2021, p. 34.
[39] United States Supreme Court, *Riley v. California*, 573 U.S. 373, 393, 134 S.Ct. 2473, 189 L.Ed.2d 430, (2014).
[40] *K.S. and M.S. v. Germany*, App. No. 33696/11, 6 October 2016, § 45.
[41] *Modestou c. Grèce*, App. No. 51693/13, 16 March 2017, §§ 42-43.

against abuse.[42] However, the existence of such safeguards, while instrumental in protecting the right to a privacy, does not alter the fact that incriminating evidence may be found on the mobile device and therefore the suspect should not be legally obliged to provide access to such evidence in disregard of their right to remain silent.

Finally, the extremely limited possibility to obtain the exclusion of evidence obtained in violation of a suspect's rights should be taken into account in this case. Fair Trials' recent report on unlawfully obtained evidence in five European states shows that the possibility to conduct an effective judicial review of the legality of evidence and obtain an effective remedy in the form of exclusion of illegally obtained evidence is extremely difficult, if not impossible. The legality of evidence is not independently reviewed at the pre-trial stage, therefore unlawfully obtained information (evidence) can lead to other evidence and become the foundation of the entire case file.[43]

In addition, legal systems give judges broad discretion to decide whether to admit unlawful evidence. In practice, this discretion is typically used to admit evidence, with the exclusion of unlawful evidence being an exception rather than the norm.[44] Even where there are seemingly clear obligations to exclude evidence, in practice the law is often interpreted to include conditions such as 'substantive violations' or 'fundamental breaches' to allow courts to rely on evidence.[45] The practice of this Court also shows that in cases where evidence has been obtained in breach of the right to privacy, it can nevertheless be used in a criminal trial. Having applied the "overall fairness" test, the Court generally finds that there has been no violation of the right to a fair trial in instances where evidence is obtained in violation of the right to privacy.[46] This has been applied mostly in cases concerning secret surveillance[47] and evidence obtained through illegal searches.[48] In the absence of any indications of tampering with digital evidence, it is generally considered reliable and can therefore be used, even in a decisive role for conviction.[49] In other words, the application of the privilege against self-incrimination to requests to access phone passcodes would help prevent violations of defence rights and the rights to privacy, which are rarely remediable *ex post* in criminal proceedings.

In conclusion, the Court must ensure that rapid advances in technology do not erode Convention rights. In view of the need to prevent coercive investigative practices and protect the highly private nature of information that is likely to be contained in mobile phones, we invite the Court to take a principled approach aimed at preserving a robust standard of the privilege against self-incrimination.

[42] Ibid.
[43] Fair Trials, Unlawful Evidence un Europe's Courts: principles, practice and remedies, 2021, p. 42.
[44] Ibid., pp. 38-39.
[45] Ibid., pp. 38-39.
[46] See e.g., *Lee Davies v. Belgium*, App. No, 18704/05, 28 July 2009, § 54; *Dragojević v. Croatia*, App. No. 68955/11, 15 January 2015, §§ 131-135; *Prade v. Germany*, App. No. 7215/10, 3 March 2016, §§ 35 and 41; *Kalneniene v. Belgium*, App. No. 40233/07, 31 January 2017, §§ 40 and 54.; see also analysis in Fair Trials, Unlawful Evidence un Europe's Courts: principles, practice and remedies, 2021, p. 21.
[47] *Dragojević v. Croatia*, App. No. 68955/11, 15 January 2015, §§ 131 – 135; *Hambardzumyan v. Armenia*, App. No. 43478/11, 5 December 2019, §§ 78 – 81.
[48] *Lee Davies v. Belgium*, App. No. 18704/05, 28 September 2009; *Prade v. Germany*, App. No. 7215/10, 3 March 2016; *Kalneniene v. Belgium*, App. No. 40233/07, 31 January 2017.
[49] See e.g., *Bykov v. Russia* [GC], App. No. 4378/02,10 March 2009.