

THE PRINCIPLE OF *NEMO TENETUR SE DETEGERE* IN THE AGE OF DATA

Agnese DEL GIUDICE*

ABSTRACT: *The objective of the present article is to examine the manner in which the Italian criminal justice system protects the nemo tenetur se detegere principle in the digital era, with a view to providing an insight into this approach for an international audience. In doing so, the article will also consider the experience of other legal systems and the jurisprudence of the courts. In Italy, the nemo tenetur is a right that has its origins in the constitutional protection of the right of defense and the presumption of innocence. There is considerable debate surrounding the extent to which the right should be safeguarded. While the majority of scholarship advocates for the broadest possible extension of the right, this view is not universally accepted: the Cassation court has recently adopted a more lenient approach to the protection of the privilege against self-incrimination, which may permit the use of the suspect's refusal to cooperate as grounds for adverse consequences. The issue arises in instances where law enforcement officials require evidence stored on a laptop or mobile phone that cannot be retrieved without a password, or without the potential for irreparable data loss. Questions arise. Does the obligation to disclose one's password constitute a form of self-incrimination or a violation of the right to remain silent? Would granting police the power to compel passwords cross a line centuries old against forcing a person to speak to build the case against them? What are the differences between traditional passwords and biometrical authentication, and what difference does this make for the privilege against self-incrimination?*

Keywords: *new technologies and criminal proceedings; right to silence, investigations; traditional encryption, biometrical authentication.*

JEL code: K14, K33, K40

DOI: 10.62838/cjjc-2024-0023

1. THE TRADITIONAL BOUNDARIES OF A MULTIFACETED RIGHT

In the context of criminal justice practice, there is a recurring phenomenon whereby investigating bodies are exposed to the temptation to extrapolate the truth from the person being prosecuted. This phenomenon has consistently presented a challenge for systems seeking to maintain the integrity of the justice process (Ferrajoli, 1996; Illuminati, 2002).

* Research fellow (temporary) in Criminal Procedural Law at the Department of Legal Sciences, University of Salento, Lecce, ITALY.

The suspect or defendant is presumed to possess knowledge that, if revealed at trial, would ensure a favourable outcome (Cordero, 1987; Illuminati, 2012). Consequently, the acquisition of information held by the suspect or defendant has been a consistent objective since antiquity¹.

Since its historic enshrinement in the Fifth Amendment to the U.S. Constitution in 1791 (which states in part that «[n]o person [...] shall be compelled [by the government] in any criminal case to be a witness against himself»), the principle of *nemo tenetur* – of which *ius tacendi* is an expression – has been affirmed in all European democratic societies as a guarantee. In regard to the “individual-authority” dialectic, it is incumbent upon the prosecution to provide irrefutable proof of the fact and the relationship between this and the perpetrator. This is an essential aspect of their institutional responsibility, and it cannot be circumvented through coercive mechanisms of cooperation from the offender (Canestrari, 2006). The *nemo tenetur* is a complex principle in criminal proceedings due to the difficulty in defining its precise scope. Traditionally, the *nemo tenetur se detegere* has been understood to entail three distinct privileges: the privilege against self-incrimination, the right not to be questioned, and the right to silence (Gradi, 2018; Ferrua, 1989).

The *nemo tenetur* is a fundamental tenet of the Italian criminal trial, primarily as an expression of the individual’s freedom of self-determination and human dignity (Catalano, 1995; Luparia, 2006); it is also an essential corollary of the inviolability of the right of defense (Cordero, 1987; Illuminati, 2012; Grevi, 1972; Paladin, 1965; Illuminati, 1999; Moscarini, 2010; Mazza, 2004; Patanè, 2006; Biral, 2015; Petrelli, 2019) under art. 24 of the Constitution², the presumption of innocence under art. 27(2) of the Constitution (Illuminati, 1975; Moscarini, 2006), and finally, the due process of law (Amodio, 2001; Illuminati, 1975; Grevi, 1972; Mazza, 2004) under art. 111 of the Constitution. The Italian Constitution does not expressly provide for the right to silence. Indeed, the traceability of this right to constitutional or para-constitutional parameters is entrusted almost exclusively to case law (Lasagni, 2020). Furthermore, such a right is not explicitly enshrined in the European Convention on Human Rights and Fundamental Freedoms (ECHR) or the Charter of Fundamental Rights of the European Union (CFREU). Nevertheless, it can be inferred from case law at the supranational level based on the principles of due process set forth in art. 6(1) ECHR (and art. 47 CFREU) and the presumption of innocence outlined in art. 6(2)³ ECHR (and art. 48 CFREU)⁴: the *nemo tenetur* principle ensures the overall

¹ On the use of coercive means to obtain the testimony of the accused at common law, see inter alia (Grevi, 1972).

² Constitutional Court, 10 May 2019, n. 117, in *ForoPlus*, para. 7.1. Previously, Constitutional Court, 26 June 2002, n. 291, *ivi*; Constitutional Court, 26 November 2002, n. 485, *ivi*.

³ The ECtHR has repeatedly held, starting with the Funke case, that the *ius tacendi* is the “heart” of the notion of procedural fairness in art. 6(1) ECHR, as it protects the accused from abusive coercion by the authority and at the same time avoids possible miscarriages of justice: cfr. ECHR, 25 February 1993, case of Funke v. France, in www.hudoc.echr.coe.int; ECHR, GC, 11 June 2006, case of Jalloh v. Germany, in www.hudoc.echr.coe.int, para. 100; ECHR, 8 April 2004, case of Weh v. Austria, *ivi*, para. 39; ECHR, GC, 8 February 1996, case of J. Murray v. United Kingdom, *ivi*, para. 45, which also states that the right to silence is a «universally recognised international norm that lies at the heart of the notion of “fair trial”». Since the principle *nemo tenetur se detegere* translates into the right not to be compelled to give evidence contra se, it is closely related to the presumption of innocence in art. 6(2) ECHR (Ubertain & Viganò, 2022).

⁴ The homogeneity clause suggests that artt. 47 and 48 CFREU also include the right to silence. This approach is also enshrined in Directive 2016/343/EU, which is one of the instruments giving concrete effect to art. 47 and 48 CFREU, and which contains an explicit affirmation of the right to silence (Amati, 2022; Pivaty, et al., 2021).

fairness of the proceedings; this is because it «presupposes the possibility for the accused not to co-operate in the conduct of the investigation» and implies that «the prosecution's case is based on evidence obtained without resorting to means of coercion or oppression» (Manes & Caianiello, 2020). An explicit provision on *ius tacendi* is included in art. 14(3)(g) of the International Covenant on Civil and Political Rights (ICCPR), which was approved by the UN General Assembly on 16 December 1966. This article guarantees every individual accused of a crime the right «not to be compelled to testify against himself or to confess guilt». Additionally, this right is enshrined in art. 55(1)(a) of the Statute of the International Criminal Court enshrines the right of any person subject to the jurisdiction of the Court not to «testify against himself or to plead guilty» (Fanchiotti, 2007).

The privilege in question is undoubtedly a fundamental right of a polyvalent nature (Amodio, 1974; Catalano, 2011; Marafioti, 2000). Nevertheless, the essence of this right, namely the refusal to cooperate with the judicial authority, which is expressed in the right not to answer investigators questions (*verbum argentum, sed silentium aurum est*), continues to be a source of contention for interpreters⁵.

The interpretative path on *nemo tenetur*, which tends to safeguard the applicative scope of the principle, is not always straightforward, especially if one considers the perspective of the Strasbourg Court (Caianiello, 2017; Lasagni, 2020; Manes & Caianiello, 2020) it is not the case that every form of coercion adopted in order to obtain information from the accused is considered a violation of the right to silence; consequently, the choice not to cooperate in situations «which clearly call for an explanation» may also have unfavourable implications for the accused under certain conditions (Febbo, 2021).

In the well-known case of *Murray v. United Kingdom*⁶, the judges of the European Court of Human Rights introduced a distinction between “proper” and “improper” forms of coercion. They also considered it acceptable for the silence of the accused to be considered as incriminating evidence, albeit with certain limits⁷. In their view, only in the case of “improper” coercion, i.e. coercion capable of «destroying the very essence» of the right against self-incrimination, can a violation of the conventional parameter be found⁸.

Aware of the lack of precision in the application of this criterion, the ECHR has, over time, developed a list of factors to be examined, albeit not exhaustive, including, as summarized in the *Ibrahim* judgement⁹: the potentially vulnerable status of the accused; the conformity of the investigative act with the legal framework governing the pre-trial proceedings; and, in the event that the evidence was obtained unlawfully, the nature of the

⁵ It should be pointed out that the protection of the right to silence is difficult to establish in concrete judicial practice and does not guarantee satisfactory margins of effectiveness (Mazza, 2004). In some cases, pre-trial detention has been used as a means of facilitating the co-operation of the person under investigation (Amodio, 2006; Marzaduri, 2006; Luparia, 2006; Illuminati, 2012; Amodio, 2010). Consider, once again, the numerous conflicts between the right to silence and the guilty plea agreement in the case of an «admission of guilt or confession of the defendant» for the purposes of the agreement with the prosecution, which is subsequently not concluded or rejected by the court (Coman, 2019).

⁶ ECHR, GC, 8 February 1996, case of *J. Murray v. United Kingdom*, in www.hudoc.echr.coe.int.

⁷ In order to assess silence *contra reum*, it would be necessary, on the one hand, that it does not constitute the sole basis for the conviction and, on the other hand, that the accused has been duly warned of this possible consequence and is in a situation, with regard to the judicial findings concerning him, “which clearly requires an explanation from him”: cfr. ECHR, GC, 8 February 1996, case of *J. Murray v. United Kingdom*, cit., para. 47.

⁸ ECHR, GC, 8 February 1996, case of *J. Murray v. United Kingdom*, cit., para. 49.

⁹ ECHR, 13 September 2016, case of *Ibrahim et al. v. United Kingdom*, in www.hudoc.echr.coe.int, para. 274.

unlawfulness in question. Furthermore, the possibility for the accused to challenge the authenticity of the evidence so obtained and to object to its use (and, if so, whether it was promptly withdrawn or modified by the accused) must be considered; an examination of the circumstances under which the evidence was obtained is necessary to ascertain whether there is any reason to doubt its reliability or accuracy. In addition, the weight of the evidence obtained in support of a conviction must be considered in light of the strength of the other evidence in the case; furthermore, the weight of the public interest in the investigation and punishment of the specific offence in question must be considered.

In the *Ibrahim v. United Kingdom* judgment, the judges of the European Court of Human Rights also reiterated that coercion is considered “improper” in the following circumstances (Manes & Caianiello, 2020): compulsion to make statements under threat of punishment¹⁰; exercise of physical or psychological pressure, often in connection with the prohibition of torture and inhuman and degrading treatment under art. 3 ECHR¹¹; use by the prosecuting authority of ‘deception’ to extract from the accused information otherwise not disclosed¹². The aforementioned limitations are applicable to all requests for information by the prosecuting authorities, including requests for the production of documents made against the accused¹³.

However, on occasion, the ECHR has also stated that the right does not extend to material obtainable from the accused that exists independently of the latter's will. This includes DNA-material, blood or documents «acquired by virtue of a warrant»¹⁴. However, on other occasions, the Court has censured documentary production orders addressed to the accused for the imposition of sanctions in the face of his refusal to comply with the authorities' requests: in the case of *J.B. v. Switzerland*¹⁵, for instance, the Strasbourg Court ruled that sanctioning the applicant's refusal to produce documents that would have contributed to incriminating him constituted a violation of the right to silence, given the substantially criminal nature of the sanction envisaged for the tax evasion¹⁶ of which the applicant was suspected. Similarly, the *Chambaz v. Switzerland*¹⁷ ruling indicates that the right to remain silent extends “beyond the context” of criminal proceedings.

When considered in its entirety, the case law of the Convention demonstrates an approach to the protection of *nemo tenetur se detegere* that is undoubtedly ambiguous. This is because, on the one hand, the European Court of Human Rights recognize that the silence of an accused person can be taken into account in the overall assessment of evidence, without necessarily violating the right to silence and the principle of presumption of innocence, thereby exhibiting minimal sensitivity to the defendant's decision to remain

¹⁰ Previously, ECHR, 17 December 1996, case of *Saunders v. United Kingdom*, in www.hudoc.echr.coe.int; ECHR, 14 October 2010, case of *Heaney et McGuinness v. Ireland*, *ivi*.

¹¹ ECHR, 11 July 2006, case of *Jalloh v. Germany*, in www.hudoc.echr.coe.int.

¹² ECHR, 5 November 2002, case of *Allan v. United Kingdom*, in www.hudoc.echr.coe.int.

¹³ ECHR, 25 February 1993, case of *Funke v. France*, *cit.*, para. 44.

¹⁴ ECHR, 17 December 1996, case of *Saunders v. United Kingdom*, *cit.*

¹⁵ ECHR, 3 May 2001, case of *J.B. v. Switzerland*, in www.hudoc.echr.coe.int.

¹⁶ The *Chambaz v. Switzerland* decision of 2012 is another important step in the jurisprudential development followed by the Court in the area of administrative investigations and tax penalties (Borgia, 2016): ECHR, 5 April 2012, case of *J.B. v. Switzerland*, in www.hudoc.echr.coe.int. It has been noted in academic circles that the judgment casts a shadow of illegality over all national provisions which, directly or indirectly, penalize the non-cooperation of taxpayers (Piantavigna, 2013). *Nemo tenetur* also applies to tax matters (Coman, 2018).

¹⁷ ECHR, 5 April 2012, case of *J.B. v. Switzerland*, *cit.*

entirely passive (even in criminal proceedings in the strict sense); conversely, the Court has consistently held that the imposition of sanctions (even formally administrative sanctions) against the accused for his refusal to cooperate constitutes a form of “improper” coercion, which is in conflict with the right not to incriminate oneself (Lasagni, 2020).

In terms of the applicative latitude of the right to silence in the context of EU law, the case law of the EU Court has developed significantly over time. In the field of antitrust matters, the Luxembourg judges have consistently upheld the existence of an obligation to cooperate, providing information and documents, even in instances where the administrative liability of the company in question may be derived from such actions¹⁸. It was only recently, following a dialogue initiated by the Italian Constitutional Court¹⁹, that the EU Court of Justice²⁰ enhanced the protection of the right beyond the confines of criminal proceedings *stricto sensu* (Mangiaracina, 2021).

Nevertheless, the scope for further development of the protection afforded by the principle of *nemo tenetur se detegere* is evident, particularly in areas where technological advancement and the absence of regulatory oversight increase the risk of circumvention of these guarantees. This is a largely uncharted legal territory, where the aftershocks are still being felt.

2. SCOPE OF THE NEMO TENETUR IN A DIGITAL WORLD

The traditional adage, “a man’s home is his castle” has long been a cornerstone of social and cultural discourse. In the contemporary era, the mobile phone has become a significant extension of the modern man’s personal domain. The use of smartphones has increased significantly in today’s society, with these devices being utilized for a variety of purposes. Given that these smartphones save and store vast amounts of private data, users tend to prefer to keep this data private and not easily accessible by others. On the one hand, smartphones are used for a variety of functions, including internet browsing, emailing, photography, message sending, account balance checking, and phone calls made using the digital address book.

¹⁸ Cfr. EU Court, 18 October 1989, *Orkem v. Commission of the European Communities*, ECLI:EU:C:1989:387, para. 35; EU Court, 15 October 2002, *Limburgse Vinyl Maatschappij NV (LVM) et al. v. Commission of the European Communities*, ECLI:EU:C:2002:582, para. 274-279; EU Court, 29 April 2004, *Tokai Carbon Co. Ltd et al. v. Commission of the European Communities*, ECLI:EU:T:2004:118, para. 402-406; *Commission of the European Communities v. SGL Carbon AG*, 29 June 2006, ECLI:EU:C:2006:432, para. 35-49; EU Court, 25 January 2007, *Dalmine SPA v. Commission of the European Communities*, ECLI:EU:C:2007:53, para. 34.

¹⁹ This is the preliminary question raised by the Constitutional Court in 2019 in order to obtain two clarifications: first, whether an obligation to sanction the defendant’s refusal to cooperate does indeed derive from EU market abuse law; second, subject to a positive answer to the first question, whether such secondary legislation can be said to be compatible with art. 47 and 48 of the Charter of Fundamental Rights of the European Union, also in the light of the case law of the Strasbourg Court: v. Constitutional Court, 10 May 2019, n. 117, in *ForoPlus*. The verdict was widely commented on (Bonzano, 2019; Fares, 2020; Galiberti, 2019; Ruggeri, 2019).

²⁰ EU Court, GC, 2 February 2021, case of *DB v. Consob*, C-481/19: in particular, it was held that both «art. 14(3) of Directive 2003/6 and art. 30(1)(b) of Regulation n. 596/2014 are capable of being interpreted in a manner consistent with art. 47 and 48 of the Charter, in that they do not require a natural person to be penalized for refusing to provide the competent authority with answers from which his liability for an offence punishable by administrative sanctions of a criminal nature or his criminal liability could be inferred». The verdict has been widely discussed (Aranci, 2021; Baldari, 2021).

Technological developments give rise to persistent tensions in the various domains of law, placing them under the strain of “modernity stress”.

The field of criminal procedural law, particularly the regulation of evidence, is the area in which these tensions are most evident. Indeed, the advancement of technology has reinvigorated the debate concerning the accused's right to withhold evidence of their possible guilt.

Until recently, the *nemo tenetur* principle was intended to prevail even in instances where acquiring evidence was not feasible. This pertains to declarative evidence, which was regarded as the gold standard in a trial system and a world where the human body and corporeality were central to daily life. Consequently, the aforementioned guarantee was previously confined to the right to remain silent. In the contemporary era, digital evidence has emerged as the archetypal form of global evidence.

The implementation of the *nemo tenetur se degere*, in light of the potential offered by new and highly effective investigative tools (Scalfati, 2019; Daniele, 2018), serves to reinforce the importance of the method in order to prevent any justification of investigative techniques that may be deemed acceptable, but which are nevertheless capable of facilitating a «process that is ultimately humiliating to our civilization» (Cordero, 1996): the objective of the process is not to pursue absolute truth at any cost, but rather to attain a truth that is founded on an unquestionable moral standard; the methodology employed in the investigation must be regarded as a value in itself (Nobili, 2004; Giostra, 1986).

In this regard, there is a paucity of certainties. One might consider the reservations that surround the implementation of novel concepts, such as “digital identity”, within established frameworks, such as those pertaining to “physical or registry” identity. In the event that we were to consider enrolling the nickname or avatar of those who engage in activities on the web in the category of information pertaining to the “generalities” of the suspect and any other data that could “be of value in identifying him/her”, in accordance with art. 66(1) of the Italian Code of Criminal Procedure, the individual in question would be entitled to exercise their right to silence (Signorato, 2018)²¹. This option is unlikely to be feasible if one considers the potential consequences of such revelations in the context of proceedings for offences committed by computer. Consequently, it seems reasonable to conclude that this course of action should be rejected.

This remains an area of legal uncertainty, as evidenced by the recent ruling of the Italian Constitutional Court on the right of the defendant or suspect not to answer questions pertaining to the personal circumstances outlined in Article 21 of the Rules Implementing the Code of Criminal Procedure (RICCP)²².

In the Italian system, the suspect (art. 349 of the Code of Criminal Procedure) and the accused (art. 66 of the Code of Criminal Procedure) are required to provide their personal details. Refusal to do so (art. 651 of the Criminal Code makes it an offence to refuse to provide one's identification information) or the provision of false statements to a public officer (art. 495 of the Criminal Code) is a criminal offence. Consequently, the right not to answer does not apply to questions pertaining to one's personal identity. In order to

²¹ An expansive interpretation of the rule – designed to identify a natural person – «could lead to an erosion of the right to silence, the limits of which (as an exception) should be precisely provided for and not extendable beyond the limits expressly set by law» (Cesari, 2019).

²² Constitutional Court, 10 May 2019, n. 117, in *ForoPlus*.

facilitate complete identification, the suspect or defendant is required to provide a comprehensive range of information, as outlined in art. 21 RICCP. This includes details about any nicknames or pseudonyms, any assets at their disposal, individual, family, and social conditions, as well as questions on whether they are currently subject to other criminal proceedings, whether they have ever been convicted of a crime either in Italy or abroad, and whether they hold or have held public office or positions or carried out public services or public duties.

The Constitutional Court ruled that the extant corpus of living law fails to afford adequate protection for the right to silence, which is an essential part of the broader right of defense enshrined in art. 24 of the Italian Constitution, art. 14(3)(g) of the International Covenant on Civil and Political Rights (ICCPR) and art. 6 ECHR. Consequently, the Court ruled that art. 64(3) of the Code of Criminal Procedure is partially unconstitutional as it does not stipulate that the warnings outlined therein are directed to the individual under investigation or the defendant prior to requesting the information specified in art. 21 RICCP. The Court also declared the art. 495(1) of the Criminal Code partially unconstitutional, to the extent it does not create an exception to liability for suspects or defendants who make false statements when asked to provide the information described in art. 21 RICCP, but were not previously given the warnings referred to in art. 64(3) of the Code of Criminal Procedure.

It is imperative that a person who is under investigation or charged in a criminal trial be explicitly informed of their right to remain silent with regard to any questions pertaining to their personal circumstances. This is because there is no obligation on the part of the suspect or defendant to cooperate with the investigation and trial against them. Furthermore, it is essential to exclude their punishability in the event that they provide false information without having been duly warned of their right to remain silent.

In light of this judgment, it becomes crucial to ascertain whether the pseudonym or avatar of individuals engaged in online activities should be categorized as information pertaining to the “generalities” of the suspect, which are excluded from the scope of the right to silence under art. 66(1) of the Code of Criminal Procedure, or alternatively, as pseudonyms under art. 21 of the Code of Criminal Procedure. In this latter category, the suspect or defendant has the right to remain silent and, in the absence of advice regarding this right and the consequence of making false statements, prosecution is not possible.

Italian doctrine is uncertain as to the precise extent of the principle of *nemo tenetur*, particularly in the context of activities that exploit the unwitting cooperation of the accused. This is because it is challenging to reconcile the right to remain silent with the need to maintain the efficacy of investigative tools.

This is exemplified by the use of computer viruses (“trojan horse”) and their inoculation into a device with the unwitting cooperation of the recipient. This individual is misled and, upon accessing a link contained in an e-mail or updating software or an application, downloads the capturer into their computer device (Bontempelli, 2018). In light of this, it is proposed that the principle of *nemo tenetur se detegere* should be interpreted in a broad sense, extending beyond the right not to make self-incriminating statements to encompass the right not to perform self-incriminating actions. It is further argued that in order to safeguard the legitimate use of the tool for these purposes, it should be demonstrated that the technology allows for remote inoculation in a covert manner, without the active collaboration of the investigative target; In the event that the police

employed deceit to gain possession of the portable electronic device, which would be handed over through the active cooperation of the investigative target, in violation of the latter's freedom of self-determination, the individual in question would be deemed to have fallen into the category of the "fraudulent capturer" (Bontempelli, 2018); nevertheless, there are those who hold an opposing view: «all uncertainty must be eliminated. The intrinsic, covert nature of the computer-capturing device provides the most robust assurance of the individual's volitional process integrity. This process, operating without awareness of its manipulation, will manifest as a wholly natural behaviour, uninfluenced by external factors» (Torre, 2017).

3. FROM (NON) *DICERE* TO (NON) *FACERE*: THE TRADITIONAL ENCRYPTION...

The advent of new digital technologies gives rise to a number of questions in the context of the right to silence. The most pertinent issues pertain to the advancement of cryptography, a technique that, on the one hand, facilitates the safeguarding of digital security; on the other, presents a potential impediment to the conduct of investigative activities²³. While encryption technology does not, in and of itself, provide an effective solution to the challenge of ensuring the security of data and systems, it is nevertheless at the heart of digital security. As a result, it has become an integral part of our daily lives, driving developments in this area of technology and others that rely on it. Concurrently, the broader utilization of encryption technology is being increasingly exploited by criminals, both as part of their *modus operandi* and as a means of enabling secret communication and illicit activities, thereby placing them beyond the reach of law enforcement. This continues to present challenges for both the law enforcement and the judiciary communities, significantly impeding their ability to investigate and prosecute. In the context of an investigation, a smartphone device can typically be seized and searched in order to utilize the data as evidence.

In many jurisdictions around the world the question arose as to whether suspects can be forced to give access to their IT system in a criminal procedure, and whether forcing a suspect to provide access to a locked smartphone amounts to a violation of the right to silence and the privilege against self-incrimination: is a password a form of testimony? Does the accused help to create the case against them by unlocking a phone? And what is the state's interest here? Does encryption pose an insurmountable hurdle to prosecution, or is it often only a matter of convenience?

In this regard, a distinction is made between providing a password or PIN-code on the one hand, and unlocking the phone with a fingerprint (or other biometric modality such as face recognition or iris scan) on the other.

The access to electronic device passwords safeguards fundamental rights, such as the right to security, and the protection of citizens, by preventing, detecting and prosecuting crimes; but other fundamental rights, such as the *nemo tenetur* principle, cannot be neglected. It is crucial to strike a balance between these rights.

²³ Europol-Eurojust, Joint Report, *Second Report of the observatory function on encryption*, February 2020; v., also, Europol, *Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement*, 2019.

From the perspective of the investigators the cooperation of the suspect by disclosing their access credentials to the computer system can become a crucial element: in cases where short passwords are used, a brute-force decryption method (allowed by the Italian system in art. 247(1-*bis*) and art. 352(1-*bis*) of the Code of Criminal Procedure: he perceives it as a method of «“legalized” cracking» (Marafioti, 2011)) can potentially remove such obstacles; however, in other cases, it is not possible²⁴ for investigators to overcome the protection measures in place (Pittiruti, 2017).

To date, the most prominent question surrounding cryptography and the right to silence is the following: if the government seeks as evidence an IT-system file that is encrypted using a key derived from a password, can the government compel the device's owner to use her password in order to decrypt the file? Does the right to silence extend to self-incriminating actions as well as self-incriminating oral statements²⁵? The answer to this question is more subtle because the rights to silence and to avoid self-incrimination are not absolute.

Italian doctrine is unequivocal in its stance on the matter: it is of paramount importance to define the content of the notices that judicial police officers are obliged to provide to suspects in the event of a search and subsequent seizure of electronic devices protected by encryption keys or passwords.

It can be observed that Italian legislation is lacking in certain respects. Pursuant to art. 352 of the Code of Criminal Procedure, the suspect subjected to a search is only provided with notice of their right to appoint a defense counsel (art. 356 of the Code of Criminal Procedure, art. 114 of the Code of Criminal Procedure). Notwithstanding the possibility for police authority to surmount any IT-related impediments in accordance with art. 352(1-*bis*) of the Code of Criminal Procedure, an operation that is becoming increasingly intricate due to the advent of sophisticated encryption techniques employed by criminals, it is imperative to exclude the notion that the suspect is obliged to divulge the contents of passwords and access keys to the system. These elements serve to safeguard the electronic data created by the suspect, and therefore, their disclosure is not a prerequisite (Mangiaracina, 2021).

In order to fully respect the right of defense, the request to hand over the passwords should be preceded by a warning of the right not to answer, as set forth in art. 64(3)(b) of the Code of Criminal Procedure and referenced in art. 350(1) of the Code of Criminal Procedure. This would result in the data collected and subsequent investigations carried out on the IT system being rendered useless (Luparia, 2001): the right not to cooperate is also incumbent on those who risk having their criminal liability revealed by unveiling the access codes to their devices²⁶.

²⁴ A pertinent reference can be found in the Court of Cassation, section V, 30 May 2017, n. 48370, Occhionero, in *CED Cass.*, n. 271412, para. 13: «without saying [...] that the search and seizure measures were taken, but had no or little effect due to the obstructive behavior of the two brothers who managed – Giulio Occhionero thanks also to a sophisticated video surveillance system of the house – to cleverly block the operation of their electronic equipment, refusing then, in the exercise of the right of defense, to provide the relevant access passwords».

²⁵ The necessity to redefine the concept of the right to voluntarily disclose only information pertaining to one's individual identity may require a re-evaluation in light of the advent of the digital age, where the notion of the self has undergone a significant expansion (Luparia, 2019).

²⁶ Conversely, a different conclusion should be reached in the event that the password was offered 'spontaneously' by the suspect, even disregarding the immediacy of the commission of the offence. This is due to the fact that there is no legal obligation to inform the judicial police of the *ius tacendi* (among other factors, Court of Cassation, section

In principle, an accused person's exercise of their right not to provide the unlock codes of the seized computer devices should not be interpreted as an admission of guilt or as an incriminating or aggravating circumstance. It is therefore the responsibility of the prosecuting authorities, and the courts in particular, to respect this right and refrain from drawing negative inferences from the accused's refusal. However, exceptions to this rule do exist, and in this case, we may refer to them as the "boomerang effect" of the *nemo tenetur*. Indeed, in certain circumstances, the act of refusing to cooperate can be taken into account in the overall assessment of the evidence, or even become an incriminating circumstance.

Italian jurisprudence has, in fact, adopted a different approach in order to avoid any prejudice to investigative activities.

A recent judgement of the Italian Court of Cassation²⁷ has determined that the suspect's refusal to provide the unlocking codes of the seized computer devices constitutes an element that may be used to infer the potential for evidential pollution, as outlined in art. 274 of the Code of Criminal Procedure. In instances where the other prerequisites, namely the seriousness of the offence and substantial indications of guilt, are met, this judgement allows for the imposition of a measure limiting personal freedom. In particular, the judges of legitimacy consider that the obstacle placed by the suspect in the way of the public prosecutor's access to the data contained in the file would make it possible for the suspect to attempt to access the data remotely, even with the help of third parties, in order to delete them, should they be released on bail.

The question then arises: admitting harmful consequences for the suspect (or defendant) due to refusal to provide access codes means dealing a "mortal blow" to the *nemo tenetur* principle and, more generally, to the right of defense? In this case, the suspect is confronted with a binary choice between cooperation in the investigation and the restriction of their personal liberty. This is the pivotal point of contention, as this restrictive trend appears to be advancing rapidly, even at the supranational level.

The subject has generated considerable interest in a number of countries, indicating the need for further investigation, including in regard to the implications for judicial cooperation between states²⁸. Both the court system and scholars with expertise in law and

III, 14 March 2018, n. 29641, Ermo, in *CED Cass.*, n. 273209). Nevertheless, in light of the increasingly blurred distinction between provocation and spontaneity, the judge was compelled to acknowledge that the subject had exercised their free will in making the spontaneous statement, without any form of external influence or solicitation. This decision was made in accordance with the understanding that the statement in question did not necessitate the involvement of defense assistance:: Court of Cassation, section I, 8 November 2019, n. 15197, Fornaro, in *CED Cass.*, n. 279125; Court of Cassation, section III, 3 April 2019, n. 20466, S., *ivi*, n. 275752; Court of Cassation, section V, 15 March 2018, n. 32015, Carlucci, *ivi*, n. 273642. The potential for conditioning spontaneous statements in the context of preliminary investigations has been consistently highlighted in doctrinal discourse (Marafioti, 2011). As highlighted in the European Agency for Fundamental Rights' monitoring of the implementation of the directive on the presumption of innocence, the potential for undue forms of "pressure" is not merely hypothetical. This is particularly relevant when considering the experiences of other legal systems: European Union Agency for Fundamental Rights (FRA), *Presumption of Innocence and related rights-Professional perspectives*, 2021, p. 78 ss.

²⁷ Court of Cassation, section II, 24 November 2020, n. 7568, in *Diritto di internet*, 12 March 2021 (Pittiruti, 2021).

²⁸ It was determined that a set of minimum evidentiary exclusion rules was necessary in the context of evidence obtained «in breach of, for example, torture, police incitement, the infringement of the privilege of self-incrimination, the right to silence or the right to legal assistance»: v. European Parliament, *Criminal procedural*

technology have divided on this question, and they all provide different arguments about how to extend existing norms and principles surrounding the right to silence so that they apply to cryptography.

In Europe, a significant number of states have enacted legislation that requires individuals accused of a crime to provide access to their computer system²⁹; this obligation to disclose access keys is also observed in the United Kingdom, where failure to comply with this legal requirement constitutes a criminal offence (Keenan, 2020)³⁰; Australia recently passed a law that allows police to compel decryption, which means forcing an accused person to provide their password or unlock a device; in Canada³¹ and the United States (Sacharoff, 2018; Wiseman, 2015) courts are divided on whether compelling a person to reveal their password should be legal.

In Belgium, the question arose whether suspects can be compelled to give the police access to their IT system. Art. 88quater of the Belgian Code of Criminal Procedure contains a duty of cooperation: people who are presumed to have special knowledge of an IT system or of the services that are used to secure the data that are saved, processed or transferred by the IT system, can be ordered to provide information on the manner to access it or the data in an intelligible form; failure to comply with this order is an offense punishable with up to three years imprisonment and/or a criminal fine. In a judgment of 4 February 2020³², the Belgian Court of Cassation ruled that nothing precludes the application of art. 88quater of the Belgian Code of Criminal Procedure on suspects because this practice does not violate the right to silent.

laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation, August 2018, pp. 47 e 188.

²⁹ These are Croatia (Section 257 of the Criminal Procedure Code), France (Section 434-15-2 of the Criminal Code) and Ireland (Section 48 of the Criminal Justice Theft and Fraud Offences Act 2001 and Section 7 of the Criminal Justice Offences Relating to Information Systems Act 2017).

³⁰ Cfr. Part III Regulation of Investigatory Powers Act 2000; Section 49 del Regulation of Investigatory Powers Act 2000.

³¹ The right to silence is a fundamental principle of Canadian criminal law that protects suspects and accused persons from being compelled to incriminate themselves. It also carries the right to keep electronic device passwords secret and, as the Ontario Court of Appeal recently affirmed in *R. v. O'Brien*, 2023 ONCA 197 (“*O’Brien case*”), it prevents law enforcement from using pressure tactics to mislead suspects into believing that they are obliged to disclose their passwords. The decision is a rebuke of law enforcement’s practice of taking advantage of the psychological impact of raids in order to pressure suspects, in the heat of the moment, into “volunteering” their passwords without concern for their informed consent. The Ontario Court of Appeal added that the primary impact of the s. 10(b) breach, however, arises from the fact that Mr. O’Brien was conscripted to assist in the investigation against him by providing his passwords, without having had a reasonable opportunity to consult counsel. As I have explained, the police wanted the password as a means of gaining access to incriminating information. By asking Mr. O’Brien to provide that password they were seeking self-incriminating information from him. The indignity of being conscripted to assist in one’s own incrimination in this way, in violation of s. 10(b) of the *Charter*, is not an insignificant deprivation of Mr. O’Brien’s *Charter*-protected interests, even in the absence of a causal connection between that breach and the evidence sought to be admitted. O’Brien marks an important development in the law of electronic search and seizure. It has been understood, at least since the Québec Court of Appeal’s decision in *R. v. Boudreau-Fontaine*, 2010 QCCA 1108, that search warrants cannot order a suspect to disclose their electronic device passwords to law enforcement. O’Brien goes further and bars law enforcement from taking advantage of the psychological impact of police raids to induce suspects to disclose their passwords. In doing so, the decision acknowledges that the inherently coercive nature of police raids may diminish or even nullify the voluntariness of incriminating disclosures during warrant execution.

³² Hof van Cassatie, arrest nr. N-20200204-5 (P.19.1086.N) dd. 4 February 2020; cfr., also, Constitutional Court, 20 February 2020, nr. 28/2020.

Three short observations can be made regarding this case. The Court asserts that access codes exist independent of the will of the suspect, a criterion that is in line with the Saunders judgement of the ECHR³³.

This means that where material that is considered to exist independently from the will of the suspect (e.g. DNA, blood and breath, but also information to access a smartphone), the *nemo tenetur* principle does not apply, and the suspect is obliged to cooperate. It is important to note, however, that passwords cannot be directly compared to the coercive acquisition of biological samples, such as saliva, blood, and urine, for DNA testing purposes (Fanuele, 2019; Pansini, 2019): rather, passwords can be seen as an element that exists only when there is an intention to use them, and not as an independent entity.

The *Belgian* Court of Cassation differentiates between the access codes, which are neutral, and the potentially incriminating information that can be retrieved by using the IT system. The information requested (i.e. the code) and its use, are limited, the Court continues. The defendant retains the right to defend himself fully concerning the information which is retrieved. However, this argument is based on a false premise: the data is closely linked to the password because, in providing the password the subject places the evidence against him in the hands of the investigators.

Finally, the Court notes that current technologies make it very difficult, or even impossible, to access an IT system that is protected by an encryption application, while such applications are freely available; the information requested from the defendant is therefore essential to unearth the truth. The aforementioned passage of the decision unambiguously demonstrates the Belgian judges' decision to prioritize the imperative of security, whereby the acquisition of the requested information is deemed a necessity for the establishment of truth, irrespective of whether the right to silence is infringed.

Another short observation can be made regarding this case. The *Belgian* Court of Cassation remains silent about biometric encryption. It always speaks about codes or passwords, but many people use their fingerprint, face scan, etc. to unlock encrypted data. If all the aforementioned arguments regarding codes can also be used for biometric data, so presumably suspects can also be forced to provide this "key" when ordered to.

4. ... ABOUT BIOMETRICAL AUTHENTICATION.

Technological advancement has facilitated the exploitation of individual physical attributes, thereby establishing an almost indissoluble bond between humans and machines. The use of PIN codes and passwords has been superseded by the use of fingerprints, facial recognition and iris scan, which are employed for the protection of computer data.

Such biometric security measures are a positive development to prevent a cybercriminal or street robber from gaining access to someone's smartphone. However, for digital

³³ ECHR, 17 December 1996, case of Saunders v. United Kingdom, cit, para. 69: «The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material 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, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing». A similar assertion is made by the English courts in their judgments: cfr., *ex plurimis*, High Court, Greater Manchester Police v. Andrews, 23 May 2011, [2011], EWHC 1966.

investigation, biometric authentication is increasingly problematic, and it raises questions of possibilities to enforce cooperation.

What are the differences between traditional passwords and biometrical authentication, and what difference does this make for the privilege against self-incrimination?

In the Italian system, the judicial police are also permitted to proceed with the identification of the person under investigation through the utilization of «fingerprinting, photographic and anthropometric surveys» (art. 349(2) of the Code of Criminal Procedure), in addition to other investigative measures. The explicit objective of the rule precludes the possibility of the utilization of fingerprints for purposes other than that which it was collected for.

A rather limited interpretation – and thus the lack of added protection from the privilege against self-incrimination – is well illustrated in recent case law of Netherlands on the forced unlocking of smartphones (ter Vrugt, 2021).

The Netherlands has diligently implemented the relevant EU Directives and the ECtHR case law in legislation and/or through case law, including the case law on adverse inferences. However, tensions with the right to silence arise indirectly through legislative provisions and case law.

In 2019, the District Court of North Holland rendered a judgement which permitted the police to forcefully press a suspect's thumb (by using handcuffs) on their smartphone in order to unlock it and extract data for the purpose of the investigation³⁴. In its decision, the Court relied on the interpretation of the privilege against self-incrimination given earlier by the Dutch Supreme Court derived from the Saunders judgement of the ECtHR. The Dutch Supreme Court endorsed the reasoning of the lower court. It found that – as a rule – forcing a suspect to provide biometric material to unlock an electronic device does not violate the Saunders criteria, because the material exists independently from the suspect's will³⁵.

The Dutch Supreme Court draws a distinction between unlocking a smartphone using the passcode and unlocking it using a biometric technique such as a fingerprint scanner or facial recognition software. While the former is protected by the right to silence, the latter is exempted by the court's interpretation that the suspect has no control over the existence of his fingerprint or iris scan (Van Toor, 2017). The right to silence does not play a significant role in the context of biometric authentication because the suspect is not compelled to speak or reveal his knowledge when he is compelled to give his fingerprint or iris scan. As a result, the suspect may be compelled to provide such data to the investigating authorities³⁶.

It is worth noting that this scenario, in which the suspect is handcuffed with his thumb on the fingerprint scanner, was considered different from unlocking the phone by exchanging the password.

The problem that data encryption poses for law enforcement continues to be a challenge. For a society that values the rule of law, it will force us to make difficult choices between liberty and justice. The legal interpretations adopted in the three jurisdictions analyzed tend to reflect a narrow reading of the relevant ECHR jurisprudence, according

³⁴ District Court of Noord-Holland, case of 28 February 2019, ECLI:NL:RBNHO:2019:1568.

³⁵ Dutch Supreme Court, case of 9 February 2021, NJB 2021/588.

³⁶ District Court of The Hague, case of 12 March 2018, ECLI:NL:RBDHA:2018:2983.

to which material other than oral statements does not fall within the scope of the privilege against self-incrimination.

REFERENCES

- Amati, E., 2022. *Dinamiche evolutive del diritto al silenzio*. Torino: Giappichelli.
- Amodio, E., 1974. Diritto al silenzio o dovere di collaborazione?. *Rivista di diritto processuale*, p. 412.
- Amodio, E., 2001. Giusto processo, diritto di difesa e obblighi di verità dell'imputato sul fatto proprio. *Cassazione penale*, p. 3587 ss.
- Amodio, E., 2006. Note sul futuribile delle misure cautelari. *Legislazione penale*, p. 373.
- Amodio, E., 2010. Verso una storia della giustizia penale in età moderna e contemporanea. *Criminalia*, p. 16 ss.
- Aranci, M., 2021. Diritto al silenzio e illecito amministrativo punitivo: la risposta della Corte di Giustizia. *Sistema penale*, Issue 2, p. 73 ss.
- Baldari, M., 2021. *Giustizia insieme*. [Online] Available at: <https://www.giustiziainsieme.it/it/diritto-e-processo-amministrativo/1595-la-cgue-riconosce-il-diritto-al-silenzio-nei-procedimenti-sanzionatori-dinnanzi-alla-consob-nota-a-cgue-sentenza-2-febbraio-2021-causa-c-481-19>
- Biral, M., 2015. L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali. *Rivista italiana di diritto e procedura penale*, p. 1842 ss.
- Bontempelli, M., 2018. Il captatore informatico in attesa della riforma. *Diritto penale contemporaneo*, p. 14.
- Bonzano, C., 2019. Nemo tenetur se detegere e procedimento amministrativo: per la Consulta, la sanzione "punitiva" impone il due process of law. *Processo penale e giustizia*, p. 1448 ss.
- Borgia, C., 2016. *L'effettività dei diritti alla luce della giurisprudenza della Corte europea dei diritti dell'uomo di Strasburgo – CEDU*. [Online] Available at: <https://diritti-cedu.unipg.it/>
- Caianiello, M., 2017. You can't always counterbalance what you want. *European Journal of Crime, Criminal Law and Criminal Justice*, p. 284 ss.
- Canestrari, S., 2006. Laicità e diritto penale nelle democrazie costituzionali. In: E. Dolcini & C. E. Paliero, a cura di *Studi in onore di Giorgio Marinucci*. Milano: Giuffrè, p. 139 ss..
- Catalano, E. M., 1995. Confronti coatti e libertà morale dell'imputato. *Cassazione penale*, p. 2240 ss.
- Catalano, E. M., 2011. Diritto al silenzio, right not to be questioned e tutela della autoincriminazione. Note storico-comparative. *Cassazione penale*, p. 4019 ss.
- Cesari, C., 2019. L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite. *Revista Brasileira de Direito Processual Penal*, 5(3), p. 1180 ss.
- Coman, R. M., 2019. The implications of the procedure of guilty plea agreement on the presumption of innocence. *Journal of the Faculty of Law Oradea*, Issue 2, p. 20 ss.

- Coman, R. M., 2018. "The presumption of guilt" in the investigation of tax evasion crimes. *Revista Tribuna Juridica*, Issue 8, p. 31 ss.
- Cordero, F., 1987. *Procedura penale*. IX a cura di Milano: Giuffrè.
- Cordero, F., 1996. Diatribe sul processo accusatorio. In: F. Cordero, a cura di *Ideologie del processo penale*. Milano: Giuffrè, p. 220 ss.
- Corso, P., 2000. Diritto al silenzio: garanzia da difendere o ingombro processuale da rimuovere?. In: AA.VV., a cura di *Studi in ricordo di Giandomenico Pisapia*. Milano: Giuffrè, p. 172.
- Daniele, M., 2018. La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge. *Processo penale e giustizia*, p. 831 ss.
- Fanchiotti, V., 2007. Il processo davanti alla Corte penale internazionale: principi e garanzie. *Questione giustizia*, p. 93.
- Fanuele, C., 2019. L'acquisizione occulta di impronte digitali e materiale biologico. In: A. Scalfati, a cura di *Le indagini atipiche*. II a cura di Torino: Giappichelli, p. 418 ss.
- Fares, G., 2020. Diritto al silenzio, soluzioni interpretative e controllimiti: la Corte costituzionale chiama in causa la Corte di Giustizia. *Dirittifondamentali.it*, Issue 1.
- Febbo, F., 2021. *La tutela dei diritti umani alla luce del diritto europeo. I profili di natura processuale: il diritto al c.d. equo processo ex art. 6 paragrafi 2 e 3 C.E.D.U. e le sue declinazioni – Le garanzie difensive*. [Online] Available at: <https://dirittodidifesa.eu/la-tutela-dei-diritti-umani-alla-luce-del-diritto-europeo-i-profili-di-natura-processuale-il-diritto-al-c-d-equo-processo-ex-art-6-paragrafi-2-e-3-c-e-d-u-e-le-sue-declinazioni-le-garanz/>
- Ferrajoli, L., 1996. *Diritto e ragione. Teoria del garantismo penale*. III a cura di Bari-Roma: Editori Laterza.
- Ferrua, P., 1989. voce Difesa (diritto di). In: *Digesto delle discipline penalistiche*. Torino: Utet, p. 471 ss..
- Galiberti, M., 2019. La quiete dopo la tempesta? I diritti fondamentali alla prova della doppia pregiudizialità nella recente giurisprudenza costituzionale. *Dirittifondamentali.it*, Issue 2.
- Giostra, G., 1986. Valori ideali e prospettive metodologiche del contraddittorio in sede penale. *Politica del diritto*, p. 21.
- Gradi, M., 2018. *L'obbligo di verità delle parti*. Torino: Giappichelli.
- Grevi, V., 1972. «Nemo tenetur se detegere». *Interrogatorio dell'imputato e diritto al silenzio nel processo penale italiano*. Milano: Giuffrè.
- Illuminati, G., 1975. *La presunzione d'innocenza dell'imputato*. Bologna: Zanichelli.
- Illuminati, G., 1999. I principi generali del sistema processuale penale italiano. *Politica del diritto*, p. 305 ss.
- Illuminati, G., 2002. L'imputato che diventa testimone. *Indice penale*, p. 338 ss..
- Illuminati, G., 2012. Carcere e custodia cautelare. *Cassazione penale*, p. 2373 ss.
- Illuminati, G., 2012. Nemo tenetur se detegere: il pilastro dell'autodifesa nel pensiero di Vittorio Grevi. *Rivista di diritto processuale*, p. 1263 ss..
- Keenan, B., 2020. State access to encrypted data in the UK: the "Transparent" approach. *Common Law World Review*, Issue 49 (3-4), p. 230 ss.
- Lasagni, G., 2020. Prendendo sul serio il diritto al silenzio: commento a Corte cost., ord. 10 maggio 2019, n. 117. *Diritto penale contemporaneo*, Issue 2, p. 137 ss.

- Luparia, L., 2001. Computer crimes e procedimento penale. In: G. Garuti, a cura di *Modelli differenziati di accertamento*. Torino: Utet, p. 387 ss.
- Luparia, L., 2006. *La confessione dell'imputato nel sistema processuale penale*. Milano: Giuffrè.
- Luparia, L., 2019. *Diritto alla privacy*. Milano, Giuffrè, p. 113.
- Manes, V. & Caianiello, M., 2020. *Introduzione al diritto penale europeo. Fonti, metodi, istituti, casi*. Torino: Giappichelli.
- Mangiaracina, A., 2021. Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici...e non solo. *Processo penale e giustizia*, p. 729 ss.
- Marafioti, L., 2000. *Scelte autodifensive dell'indagato e diritto al silenzio*. Torino: Giappichelli.
- Marafioti, L., 2011. Digital evidence e processo penale. *Cassazione penale*, p. 4516 ss.
- Marzaduri, E., 2006. Note di sintesi (con alcune considerazioni a margine) del forum sulla disciplina delle misure cautelari personali. *Legislazione penale*, p. 394.
- Mazza, O., 2004. *L'interrogatorio e l'esame dell'imputato nel suo procedimento*. Milano: Giuffrè.
- Moscarini, P., 2006. Il silenzio dell'imputato sul fatto proprio secondo la Corte di Strasburgo e nell'esperienza italiana. *Rivista italiana di diritto e procedura penale*, p. 617 ss.
- Moscarini, P., 2010. Silenzio dell'imputato (diritto al). *Enciclopedia del diritto, Annali*, Volume III, p. 1083.
- Nobili, M., 2004. *Il principio del libero convincimento del giudice*. Milano: Giuffrè.
- Paladin, L., 1965. Autoincriminazione e diritto di difesa. *Giurisprudenza costituzionale*, p. 312.
- Pansini, C., 2019. Diritto di difesa. In: AA.VV., a cura di *Diritti della persona e nuove sfide del processo penale*. Milano: Giuffrè, p. 280 ss.
- Patanè, V., 2006. *Il diritto al silenzio dell'imputato*. Torino: Giappichelli.
- Petrelli, F., 2019. Ad armi pari? le "forme" della "parità" fra costituzione e processo. *Cassazione penale*, p. 1735 ss.
- Piantavigna, P., 2013. Il diritto del contribuente a non collaborare all'attività accertativa. *Rivista di diritto finanziario e scienza delle finanze*, Issue 2, p. 90 ss.
- Pittiruti, M., 2017. *Digital evidence e procedimento penale*. Torino: Giappichelli.
- Pittiruti, M., 2021. Rifiutare di fornire i codici di sblocco della strumentazione informatica in sequestro e pericolo di inquinamento probatorio: addio al nemo tenetur se detegere?. *Diritto di internet*.
- Pivaty, A. et al., 2021. Strengthening the protection of the right to remain silent at the investigative stage: What role for the EU legislator?. *New Journal of European Criminal Law*, Volume 12(3), p. 427 ss.
- Ruggeri, A., 2019. *Consulta Online*. [Online] Available at: <https://giurcost.org/contents/giurcost/studi/ruggeri90.pdf>
- Sacharoff, L., 2018. Unlocking the Fifth Amendment: Passwords and Encrypted Devices. *Fordham Law Review*, Volume 87, p. 203 ss.
- Scalfati, A., a cura di, 2019. *Le indagini atipiche*. II a cura di Torino: Giappichelli.
- Signorato, S., 2018. *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*. Torino: Giappichelli.

- ter Vrugt, P., 2021. A pragmatic attitude: the right to silence in the Netherlands. *New Journal of European Criminal Law*, Volume 0, p. 1 ss.
- Torre, M., 2017. *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*. Milano: Giuffrè.
- Ubertis, G., 1997. *Verso un "giusto processo" penale*. Torino: Giappichelli.
- Ubertis, G. & Viganò, F. a cura di, 2022. *Corte di Strasburgo e giustizia penale*. Torino: Giappichelli.
- Van Toor, D., 2017. De vergrendelde smartphone als object van strafvorderlijk onderzoek. *Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht*, Issue 1, p. 3 ss.
- Van Toor, D., 2017. De vergrendelde smartphone als object van strafvorderlijk onderzoek. *Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht*, Issue 1, p. 3 ss.
- Wiseman, T. A., 2015. Encryption, Forced Decryption and the Constitution. *Journal of law and policy for the national society*, Volume 11, p. 525 ss.
-
-
-