

RETHINKING “CRYPTO-PRIVILEGE”: A BRIEF LOOK AT THIRD PARTIES*

di Alessandro Malacarne
(*PhD in Criminal procedure,*
University of Genoa)

The paper analyses the applicability of the privilege against self-incrimination to third parties who are not the subjects of a criminal investigation, with particular reference to situations in which they are required to disclose passwords relating to crypto-assets.

Il contributo esamina la possibilità di estendere il diritto a non autoincriminarsi anche a soggetti terzi non sottoposti a indagine penale, con specifico riguardo alle ipotesi in cui venga loro richiesto di rivelare le password di accesso a portafogli di criptovalute.

Privilege against self-incrimination; password; third parties; crypto-assets

Diritto al silenzio, codici di accesso, terzi non coinvolti nelle indagini, crypto-assets

Contents: 1. Framing the issue. – 2. The regulation framework. – 3. Proposals.

1. The seizure of crypto-assets has recently become a key topic in academic research and case law at the Italian, European, and international levels. This trend is driven by the growing use of these digital tools and the increasing number of crimes in which they are involved, either as the means or the target of the offence¹.

In this context, an important issue is how law enforcement authorities can obtain credentials and passwords needed to access a crypto wallet during a criminal investigation.

From a technical standpoint, virtual assets are transferred through the use of a wallet, namely a device or software application that stores the keys required to operate on the network. Transactions rely on a system of asymmetric cryptography, which presupposes the coordinated use of a pair of mathematically related, yet functionally distinct, keys: a public key and a private key². The former is used to derive the wallet address – that is,

* The paper was carried out within the project CRYPTOSAFE (Towards a Safe Seizure and Confiscation of Crypto-Assets in Criminal Proceedings), Project Code P2022HW85A, CUP D53D23022280001.

¹ J. Della Torre, *Cripto-attività e giustizia penale*, Milano 2026, 45 ff. See also, on a number of more specifically substantive criminal-law issues, including those arising from the recent implementation of the MiCA Regulation, J. Della Torre, G. Pontepino, *Commento al d.lgs. 129 del 2024 di attuazione del regolamento UE sui mercati delle crypto-attività. Le novità sul versante penalistico e amministrativo punitivo*, in *ivi*, 18.2.2025; G. Pontepino, *Autoriciclaggio e (in)sussistenza del reato presupposto. il riflesso dell'incerta evoluzione normativa in materia di cryptoattività*, in *DPP* 2026, 77 ff.

² J. Della Torre, *Spunti in tema di crypto-attività e procedimento penale*, in www.la legislazione penale.eu, 28.2.2025,

the alphanumeric string to which assets may be sent – and to encrypt transaction-related information. The latter, which is kept secret by the holder, is used to generate the digital signature authorising the transfer of the resources associated with that address.

As a consequence, the effective control over crypto-assets does not depend on the physical possession of any tangible item, but rather on exclusive control over the private key associated with the relevant address. It is this key, in fact, that enables the holder to dispose of the assets recorded on the blockchain and to authorise their transfer.

These features are equally decisive from the standpoint of criminal procedure, since they explain why access to a wallet – and thus the seizure of the underlying intangible assets – is, in practice, conditional upon knowledge or availability of the relevant cryptographic credentials³.

In legal terms, where the wallet is self-hosted, obtaining the private key – whether represented on a physical medium (for example, a piece of paper) or stored within a device (such as a smartphone or hardware token) – typically presupposes some form of cooperation by the person who has full control over it. Although the investigating authorities may in some cases resort to forms of “legalised cracking”, by using technical tools designed to overcome digital security barriers, the risk of investigative deadlock remains far from remote in practice. Indeed, any attempt by law enforcement authorities to force access to the device – for instance, by repeatedly guessing the password – may ultimately result in the irreversible loss of all data stored on it.

To date, this issue has been examined primarily in relation to situations in which the suspect or accused person is the recipient of an order or request to reveal the credentials⁴. In that setting, the central tension lies between the interests of criminal investigation and enforcement, on the one hand, and defence rights, most notably the right to remain silent, on the other. It should be noted, moreover, that this is merely one manifestation of a broader phenomenon, concerning any fixed or mobile device – including smartphones, tablets, wearable devices or social network accounts – in which user-generated contents are stored⁵.

¹².

³ P. Dal Checco, *Sequestro e confisca: tecnica e procedura*, in *Criptoattività, criptovalute e Bitcoin*, a cura di S. Carpaccioli, Milano 2021, 329.

⁴ J. Della Torre, *Cripto-attività e giustizia penale*, cit., 492 ff., 567 ff.

⁵ See, *ex multis*, G. Cotti, *Accesso ai dispositivi elettronici e principio nemo tenetur se detergere: passwords biometriche ed alfanumeriche, ordini di decrittazione e di produzione*, in www.archiviopenale.it 17.7.2025; J. Escobar Veas, *Smartphone decryption via forced fingerprinting and the right against self-incrimination: The*

Although this perspective is undoubtedly important, it does not cover all the situations that may arise in investigative practice. In practice, it is not uncommon for the private key to a wallet to be under the factual or legal control of someone other than the suspect – such as a family member, employee, business partner, professional adviser, or custodian service provider – and for the authorities to seek disclosure directly from that third party.

In such cases, the issue takes on distinctive features because of the conceptual distinction between the suspect’s right to silence and the third party’s privilege against self-incrimination⁶. As leading scholarship has pointed out, it is necessary to distinguish between, on the one hand, the privilege against self-incrimination in the strict sense, namely the right not to provide answers capable of revealing liability for facts not yet the subject of formal procedural scrutiny, and, on the other hand, the right to remain silent – that is, the privilege against self-incrimination in a broader sense – aimed at preventing an individual from contributing to his or her own conviction in respect of facts already formally alleged⁷.

The underlying question, therefore, is whether, and to what extent, a third party may invoke a form of privilege against self-incrimination that is distinct from the suspect’s right to silence, yet rooted in the same fundamental guarantee protecting the individual’s freedom of will and moral autonomy⁸.

German federal court (BGH) addresses the problem, in Computer Law & Security Review 2025, 7 ff.; A. Mangiaracina, Nuove fisionomie del diritto al silenzio. Un’occasione per riflettere sui vuoti domestici... e non solo, in PPG 2021, 736 s.; F.N. Ricotta, Obblighi di collaborazione con l’autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l’auto-incriminazione, in CP 2022, 880 ff.; D.A.G. Van Toor, G. Pesselse, Unlocking the Meaning of the Privilege against Self-Incrimination for Biometrically Secured Smartphones, in European Journal of Crime, Criminal Law and Criminal Justice 2025, 285 ff.; W. Zontek, Biometric Encryption of Smart Devices and the Prohibition against Self-incrimination in Criminal Procedure. Old Guarantees in the New World, ivi 2024, 156 ff.

⁶ E. Amodio, *Diritto al silenzio o dovere di collaborazione? A proposito dell’interrogatorio dell’imputato in un libro recente*, in RIDPP 1974, 412; L. Marafioti, *Scelte autodifensive dell’indagato e alternative al silenzio*, Torino 2000, 115; V. Patanè, *Il diritto al silenzio dell’imputato*, Torino, 2006, 2. Cfr., *amplius*, A. Giarda, *Persistendo ‘l reo nella negativa*, Milano 1980; V. Grevi, *Nemo tenetur se detegere: interrogatorio dell’imputato e diritto al silenzio nel processo penale italiano*, Milano 1972.

⁷ O. Mazza, *L’interrogatorio e l’esame dell’imputato nel suo procedimento*, Milano 2004, 50 nt. 148. See also F.M.W. Billing, *The Right to Silence in Transnational Criminal Proceedings. Comparative Law Perspectives*, Cham 2016, 8-9.

⁸ C. cost., 4.4.1973 n. 34, see V. Grevi, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in GCost 1973, 317 ff., where the Court established that the aim of the *nemo tenetur* is «rafforzare la libertà morale dell’imputato per sollevarlo dallo stato di soggezione psicologica in cui possa venire a trovarsi al cospetto dell’autorità e per porlo al riparo da eventuali pressioni che su di lui possano essere esercitate». On the concept of *libertà morale*, see G. Vassalli, *Il diritto alla libertà morale*, in *Scritti giuridici*, III, *Il processo e la libertà*, Milano 1997, 306 ff.

2. It is well known that a person not under investigation who is called upon to provide information to the authorities during the pre-trial or trial stage is, in principle, subject to a general duty of cooperation. Such a person is required to contribute to the establishment of the facts at issue in the proceedings. This proposition may be traced back to the broader non-derogable duty of social solidarity enshrined in Article 2 of the Italian Constitution and traditionally expressed through the notion of the third party’s “servitude to justice”⁹.

That general principle, however, is limited by Articles 63 and 198 of the Italian Code of Criminal Procedure, insofar as they recognise a privilege against self-incrimination in favour of a person who is not formally under investigation but is called upon to testify. This guarantee implies that no one, not even a witness, may be compelled to make statements from which indications of his or her own criminal liability might emerge¹⁰.

The extension of this privilege to persons who are not formally subject to criminal proceedings has recently been endorsed by the Italian Constitutional Court¹¹, which, drawing on considerations previously advanced by the Court of Justice of the European Union¹², extended the scope of the right in question to requests for information

⁹ P. Tonini, C. Conti, *Il diritto delle prove penali*, Milano 2014, 191; C. Conti, *Il corpo dell'imputato come prova: il diritto di non collaborare tra prospettive sovraordinate, suggestioni storiche e polifunzionalità dei dati*, in *DPP* 2024, 118.

¹⁰ According to L. Lupária, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in L. Lupária-G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano 2007, 160, «il diritto a non collaborare spetta non solo alla persona indagata, ma anche a chi rischia di far emergere una sua responsabilità penale attraverso la dazione di codici». Cfr. also F. Salimi, *Legal Challenges in Dealing with Electronic Evidence in Criminal Proceedings*, in *Admissibility of Evidence in EU Cross-Border Criminal Proceedings. Electronic Evidence, Efficiency and Fair Trial Rights*, a cura di L. Bachmaier Winter-F. Salimi, Londra 2024, 53.

¹¹ Corte cost., 30 aprile 2021, n. 84, in *Giur. cost.*, 2021, 1028 ff. See M. Allena, S. Vaccari, *Diritto al silenzio e autorità di vigilanza dei mercati finanziari*, in *Rivista di diritto bancario* 2022, 689 ff.; E. Andolina, *Dichiarazioni rese dinanzi ad autorità diverse da quella penale*, in *RIDPP* 2024, 71 ff.; E. Bindi, *Diritto fondamentale al silenzio e poteri d'indagine di Banca d'Italia e Consob*, in *GC* 2021, 1048 ff.; C. Bonzano, “Matière pénale” e diritto al silenzio: la Consulta mette un punto fermo... o quasi, in *DPP* 2022, 47 ff.; E. Brugiotti, *Diritto al silenzio. La sentenza delle Sezioni riunite della Corte dei conti in sede giurisdizionale n. 2/2017 alla luce del dialogo fra le Corti. Possibili aperture all'orizzonte?*, in *Rivista della Corte dei conti* 2022, 117 ff.; R. Casiraghi, Art. 6, in *Corte di Strasburgo e giustizia penale*, a cura di G. Ubertis, F. Viganò, Torino 2022, 243; S. Catalano, *La vicenda decisa dalla sentenza n. 84 del 2021 della Corte costituzionale: un esempio di “buon dialogo” fra Corti*, in *Forum di Quaderni Costituzionali* 2021, 296 ff.; P. Gambatesa, *Riflessioni sulla prima occasione di “dialogo” tra Corte costituzionale e Corte di giustizia in casi di doppia pregiudizialità*, in *www.federalismi.it*, 6.10.2021; G. Spangher, *Nel dialogo tra le Corti si consolida il diritto al silenzio*, in *GC* 2021, 1046 ff.

¹² Corte giust., GS, 2 febbraio 2021, DB c. Consob, C-481/19, whit observations of M. Aranci, *Diritto al silenzio e illecito amministrativo punitivo: la risposta della Corte di giustizia*, in *www.sistemapenale.it*, 2021, 2, 73 ff.; E. Basile, *La Corte di giustizia riconosce il diritto al silenzio nell'ambito dei procedimenti amministrativi “punitivi”*,

addressed by an inspection authority in the context of supervisory activity, not only after the formal allegation of an offence, but also – and this is the aspect most relevant here – where the examination is aimed at discovering offences and identifying those responsible.

From this perspective, *nemo tenetur se detegere* may not be limited to “cover” only confession-like statements, but may instead assume a broader scope, encompassing the right of every individual not to provide information capable of leading to his or her incrimination, understood as the opening of criminal proceedings against that person¹³. On this view, the disclosure of the access credentials to an online wallet might itself have to be regarded as a form of potentially self-incriminating conduct.

There is, however, one aspect that seems to place this scenario outside the immediate scope of Articles 63 and 198 of the Code of Criminal Procedure.

First: those provisions refer exclusively to “statements”, and not to affirmative acts lacking an obvious communicative dimension, as the conduct at issue here might (perhaps) be characterised. Second: the sanction of *inutilizzabilità* laid down therein presupposes that indications of criminal liability emerge at the very moment the oral contribution is made, which is not what occurs where the individual merely hands over a password.

Even if one were legitimately inclined to interpret the notion of “statement” broadly enough to include any proactive conduct, there is no doubt that, on a markedly formal reading, the object protected by the privilege against self-incrimination is the act of revealing the digital access codes itself. This is no minor point, since such conduct might, in and of itself, be characterised as “neutral”, in that it does not directly amount either to a confession or, more generally, to anything inherently self-incriminating. In other words, the potentially incriminating significance of the conduct would emerge only as a result of the subsequent forensic examination of the wallet.

That said, it should not be overlooked that even such an act may still interfere with the guarantee in question, at least if the privilege is interpreted in a broader sense, namely as the right not to cooperate in any way in the emergence of incriminating evidence against oneself. Viewed in this light, the acquisition of the password would form part of a composite investigative operation, in which the request for disclosure

ivi, 3.2.2021; G. Caneschi, *La Corte di giustizia sul diritto al silenzio: un primo passo verso il “giusto procedimento” amministrativo punitivo*, in RIDPP 2021, 568 ff.

¹³ O. Mazza, *Presunzione d’innocenza e diritto di difesa*, in DPP 2014, 1409. See also C. eur., 4 ottobre 2005, *Shannon c. Regno Unito*.

functions as a preliminary step towards obtaining information that may ultimately prove self-incriminating¹⁴.

3. Against this background, a *de lege ferenda* solution would be to introduce a legislative rule providing for a form of *inutilizzabilità soggettiva relativa*¹⁵ in respect of self-incriminating information obtained through the analysis of the wallet, while at the same time preserving the full procedural usability of evidence incriminating third parties. At first sight, such a compromise might appear capable of reconciling the need to protect the third party’s privilege against self-incrimination with the equally important need to ensure genuinely effective criminal investigations¹⁶.

Even so, that solution does not appear entirely satisfactory.

The public authorities could still use the material extracted from the digital wallet as an investigative lead for inquiries directed against the third party, or even as a genuine *notitia criminis*, thereby depriving the principle of *nemo tenetur se detegere* of much of its intrinsic protective value¹⁷.

In order to avert that risk, attention must shift to the need for an *ex ante* safeguard, namely a legal mechanism capable of preventing the danger of arbitrary intrusion into private life.

In this regard, reference should be made to Article 19, paragraph 4 of the Budapest Convention on Cybercrime, under which the States are required to adopt such legislative measures as may be necessary to empower the competent authorities to order «any person» who has knowledge of the functioning of the computer system or of the measures applied to protect the computer data contained therein to provide all information reasonably necessary to enable the search or seizure of such devices¹⁸. In

¹⁴ A. Mangiaracina, *op. cit.*, 739.

¹⁵ C. Conti, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova 2007, 29: «è soggettivamente relativa l’inutilizzabilità che rende l’atto invalido nei confronti di determinate persone».

¹⁶ G. Cotti, *op. cit.*, 34; F.N. Ricotta, *op. cit.*, 893 ff.

¹⁷ O. Mazza, *L’interrogatorio e l’esame dell’imputato*, cit., 388.

¹⁸ The subject-centred wording “any person” has enabled a number of legal systems to introduce forms of disclosure requirement, often backed by criminal sanctions in the event of refusal to surrender the password. This is the case, in particular, in Belgium (Article 88-*quater* of the Code of Criminal Procedure), which provides that the investigating judge, or a judicial police officer acting in support of the public prosecutor, may order «à quiconque dont il présume qu’il a connaissance particulière du système informatique» to provide information concerning the operation of the computer system and the means of accessing it. In its decision of 4 February 2020 (Hof van Cassatie), the Belgian Supreme Court held that this provision may also be applied to the suspect, who may not invoke the right to silence in order to resist compliance. Comparable mechanisms also exist in Croatia (Article 257 of the Code of Criminal Procedure), France (Article 434-15-2 of the Penal Code), Ireland

substantially similar terms, it is worth noting, Article 28, paragraph 4 of the United Nations Convention against Cybercrime, adopted on 24 December 2024 with the aim of facilitating international cooperation in the prevention and repression of cybercrime, points in the same direction¹⁹.

These provisions clearly reveal the growing centrality of the principle of proportionality as a guiding and limiting standard for investigative operations involving digital artefacts or, more broadly, the acquisition of digital data²⁰. Rooted in theoretical constructs developed within German legal thought, proportionality has, as is well known, gradually assumed a position of primary importance at the European level, especially in the jurisprudence of the highest courts, to the point of becoming one of the defining features of contemporary neo-constitutionalism²¹.

(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), and the United Kingdom (Section 49 of the Regulation of Investigatory Powers Act 2000). As regards the French position, the *Conseil constitutionnel*, in decision no. 2018-696 of 30 March 2018, held that the relevant provision does not infringe the guarantee embodied in the principle of *nemo tenetur se detegere*. English case law has reached a similar conclusion. Relying on the case law of the European Court of Human Rights – to which reference will be made below – the English courts have excluded any incompatibility with the privilege against self-incrimination on the ground that a password constitutes a material fact existing independently of the defendant’s will: *R v S and A* [2008] EWCA Crim 2177, [2009] 1 All ER 716. See also B. Keenan, *State Access to Encrypted Data in the UK: The ‘Transparent’ Approach*, in *Common Law World Review*, 2020, p. 230 ff. It should, however, be emphasised that the existence of criminal sanctions for failure to disclose the relevant code necessarily places on the prosecuting authorities the burden of proving that the suspect actually knew the password in question, since no one may be punished for failing to provide information that he or she does not possess. Even so, the manner in which such proof is to be established remains uncertain. It is, after all, for the prosecution to prove the existence of such knowledge, yet that task is inherently difficult, since a person’s mental state cannot be directly observed. One might therefore ask whether it is legitimate to presume that an individual knows the access code to his or her own smartphone or computer. And even if such a presumption were accepted, the further question would remain as to how it might be rebutted in practice.

¹⁹ A. Balsamo, C. Ponti, *La Convenzione delle Nazioni Unite contro il cybercrime e lo sviluppo delle suppression conventions sui crimini transnazionali. Rilievi teorici e implicazioni pratico-operative*, in www.lalegislazionepenale.eu 19.2.2026.

²⁰ L. Belvini, *Principio di proporzionalità e attività investigativa*, Napoli 2022, *passim*; F. Nicolichia, *Il principio di proporzionalità nell’era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in archivioppc.dirittopenaleuomo.org, 8.1.2018, 1 ff.; S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino 2018, 262 ff. See, *amplius*, M. Caianiello, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont., Riv. trim.*, 2014, 3-4, 144 ff.; D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *RIDPP* 2020, 3 ff.; R. Orlandi, *Postulati del processo penale contemporaneo tra principi “naturali” e concezioni normative*, *ivi* 2024, p. 465 ff.; G. Ubetis, *Prova penale e proporzionalità*, in www.sistemapenale.it 23.1.2025.

²¹ M. Cartabia, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, in *Atti della Conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola*, 24-26 ottobre 2013, at https://www.cortecostituzionale.it/documenti/convegni_seminari/RI_Cartabia_Roma2013.pdf.

If that principle is taken seriously²², the requirement of “reasonable necessity” justifying the intrusion might, in a *de iure condendo* perspective, be calibrated differently depending on the type of interest at stake²³.

In some circumstances, the disclosure of passwords should be regarded as legitimately compellable, albeit always subject to the provision of an *ex post* safeguard – namely, a rule of inadmissibility.

In others, by contrast, such interference might prove disproportionate to the objective pursued. In those cases, the disclosure of the “necessary information” should instead consist merely in the production of the specific evidentiary material concretely requested by the authorities, without requiring the surrender of the access credentials themselves.

In other words, the logic of proportionality should make it possible to modulate the degree of enforceable cooperation according to both the nature of the data sought and the seriousness of the offence under investigation²⁴. Along the lines of what leading scholarship has described as a “graduated protection” of liberty rights, it is necessary to identify clear limits beyond which public power may not extend, even in pursuit of the legitimate aim of criminal enforcement²⁵.

Support for the proposal advanced here may, moreover, be found in solutions already adopted in other legal systems.

One may think, for example, of Article 588 sexies c) of the Spanish Code of Criminal Procedure. In implementing Article 19, paragraph 4 of the Budapest Convention, that provision gives concrete expression to a general duty of cooperation with the administration of justice by establishing that investigators may order any person who is aware of the protective measures applied to digital devices to provide the

²² § 146 of *Explanatory Report to the Convention on Cybercrime*: «the powers and procedures shall “incorporate the principle of proportionality”. Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law».

²³ See, in a different perspective, F.N. Ricotta, *op. cit.*, 894.

²⁴ See L. Marafioti, *Scelte autodifensive dell’indagato e alternative al silenzio*, cit., 117, who had already emphasised that any restrictions on the right not to cooperate with the judicial authorities must be based on «specifiche e tassative previsioni processuali e risultare “proporzionali” al peso degli elementi a carico raccolti nei confronti della persona sospettata».

²⁵ R. Orlandi, *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *RIDPP* 2014, 1133 ff. and, in particular, 1151, where the author highlights how the adjective progressive is intended to signal both the emergence of new rights – particularly in the face of the new intrusive capabilities inherent in evidence-gathering methods 2.0 – and the need to monitor the shifting boundary that separates the sphere of inviolable rights from that of their restriction, justified by the need to suppress and/or prevent criminal activity’.

relevant unlocking codes, «*siempre que de ello no derive una carga desproporcionada para el afectado*»²⁶. Quite apart from the criticisms raised by part of the literature²⁷, the reference to a “disproportionate burden” on the affected person – here, the third party not under investigation – offers a particularly valuable point of reflection.

In the Italian context, this approach could usefully be received by articulating a principle of non-intrusion into the sphere of confidentiality and privacy of those persons subject to the so-called servitude to justice, the concrete degree of enforceability of which would find its most convincing justification precisely in the principle of proportionality.

²⁶ Please note: the second paragraph of the provision stipulates that «*esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional*».

²⁷ The objection relates, in particular, to the use of the phrase ‘any person’, which is considered overly broad and potentially capable of including individuals who are completely unconnected to the investigations: «*¿qué perfil tiene esa persona? Al hablarse de un cualquier no se acota la identidad de ese sujeto, ¿se está hablando de un ingeniero informático profesional? O por el contrario ¿se abre la puerta al fichaje de hackers que actúen sin fines éticos e incluso criminales?*»: F. Bueno De Mata, *Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*, in *Diario la Ley*, 19.10.2015, § 5. One also wonders whether the obligation to cooperate imposed on ‘anyone’ also includes the duty to provide, upon request, to the investigating authority, specific software capable of cracking and unlocking the device: P. Martín Ríos, *op. cit.*, 116 ff.