GIACOMO COTTI

Accesso ai dispositivi elettronici e principio *nemo tenetur se detegere*: *passwords* biometriche ed alfanumeriche, ordini di decrittazione e di produzione

Il presente articolo si propone di analizzare il fenomeno dell'accesso forzoso ai dispositivi elettronici alla luce del principio processual-penalistico che riconosce la libertà dall'autoincriminazione. In particolare, lo studio, valorizzando la veste processuale che può assumere il destinatario di una richiesta di collaborazione e il tipo di condotta lui domandata, esamina le forme e i limiti con cui il *nemo tenetur* potrebbe essere invocato nel corso di indagini svolte sugli *electronic devices*. Questa verifica viene condotta avendo ad oggetto l'ordinamento italiano, letto in controluce rispetto allo scenario sovranazionale e comparato. Peculiare attenzione è poi dedicata a distinguere la richiesta di una password alfanumerica dal ricorso alla matrice biometrica in funzione di chiave d'accesso al dispositivo, giacché trattasi di un discrimine in grado di incidere notevolmente sulla possibilità di avvalersi del diritto al silenzio.

Access to electronic devices and the principle nemo tenetur se detegere: biometric and alphanumeric passwords, decryption and production orders.

This article aims to analyse the phenomenon of forced access to electronic devices in the light of the criminal procedural principle that recognises the freedom from self-incrimination. In particular, the study, valuing the procedural role that the addressee of a request for collaboration may assume and the type of conduct requested of him, examines the forms and limits with which the nemo tenetur guarantee could be invoked during investigations carried out on electronic devices. This examination is conducted by focusing on the Italian legal system, read against the backdrop of the supranational and comparative scenario. Particular attention is then devoted to distinguishing the request for an alphanumeric password from the use of the biometric feature as an access key to the device, since this is a discriminating factor capable of significantly affecting the possibility of availing oneself of the right to silence.

SOMMARIO: 1. L'accesso ai dispositivi elettronici: una sfida per la giustizia penale. – 2. Il versante sovranazionale... – 3. (Segue) Uno sguardo comparato. – 4. Obbligo di rivelazione della *password* e diritto al silenzio: codici alfanumerici – 5. (Segue) Chiavi d'accesso biometriche. – 6. Obblighi di decrittazione e di produzione. – 7. Collaborazione "spontanea" e valutazione del "silenzio". – 8. Cooperazione "fittizia" e attacchi a "forza bruta". – 9. Obbligo di rivelazione della *password* e privilegio contro l'autoincriminazione. – 10. Conclusioni.

1. *L'accesso ai dispositivi elettronici: una sfida per la giustizia penale.*

[1]Il contributo costituisce il frutto della ricerca svolta dall'Autore nell'ambito del progetto dal titolo "*Dispositivi indossabili e accertamento penale*". Finanziato dall'Unione europea – *NextGenerationEU* a valere sul *Piano Nazionale di Ripresa e Resilienza* (PNRR) – Missione 4 Istruzione e ricerca – Componente 2 *Dalla ricerca all'impresa* – Investimento 1.1, Avviso PRIN 2022 DD N. 104 del 02/02/2022, dal titolo "*Nuove tecnologie, dati biometrici e procedimenti penali*", codice progetto MUR 2022CWNCH8 – CUP J53D23005360006.

L'evoluzione tecnologica ha modificato la maniera di intendere il procedimento e il processo penale. La quantità di informazioni disponibili su fatti e persone è accresciuta vertiginosamente dall'onnipresenza di dispositivi quali cellulari, *tablet* e *computer*; le indagini condotte su tali apparecchi sono divenute ordinaria amministrazione; la valutazione delle prove da essi estratte è ormai appannaggio di esperti (periti e consulenti tecnici), rispetto alle cui conoscenze specialistiche giudici e parti appaiono sempre più ridotti al rango di discenti.

Questo stato di cose apre notevoli problemi giuridici, a partire da quello che si colloca *in apicibus*, ossia l'individuazione dei valori – costituzionali, internazionali, convenzionali – in grado di governare l'indagine condotta su questi apparecchi: molti di essi possono infatti costituire, ad un tempo, vere e proprie "estensioni" del corpo umano (art. 13 Cost.), in quanto appendici ormai inseparabili dall'utente[2]; "luoghi" meritevoli di tutela, in quanto proiezioni dell'individuo nello spazio virtuale (art. 14 Cost.)[3]; "mezzi di comunicazione", data la loro diffusa idoneità ad inviare, ricevere e conservare messaggi (art. 15 Cost.)[4]; manifestazioni d'una «libertà informatica» di nuovo conio, discendente dal catalogo aperto dei diritti inviolabili (artt. 2 Cost. – 8 C.E.D.U.) ed idonea a proteggere l'uso riservato delle tecnologie

[2] TORRE, Privacy *e indagini penali*, Milano, 2020, 27; PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. giust.*, 2020, n. 2, 295-298. Tale assetto è particolarmente evidente nel caso degli *smartphone*: cfr. Corte cost., 31 marzo 1987, n. 88, punto 2 del *Considerato in diritto*. In dottrina, CAMON, *Cavalli di Troia in Cassazione*, in *Arch. nuova proc. pen.*, 2017, n. 1, 95.

[3] Per tutti, PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 38.

[4] Vista anche la nozione ampia di "comunicazione" da ultimo sposata da Corte cost., 27 luglio 2023, n. 170. A favore della parificazione fra intercettazioni e sequestri di *smartphone*, *tablet*, *computer*, o di «*device* dalle funzioni similari» si veda ad esempio LA REGINA, *Il sequestro dei dispositivi di archiviazione digitale*, in *Penale. Diritto e procedura*, 12 ottobre 2023, p. 3, https://www.penaledp.it/il-sequestro-dei-dispositivi-di-archiviazione-digitale/?print-posts=pdf.

dell'informazione (ICT)[5], a tutelare la *privacy*[6], ovvero a preservare la «intangibilità della vita digitale»[7].
A questo tema di fondo se ne aggiungono ulteriori, più specifici. Si pensi alla scarsa consapevolezza da parte degli utenti circa il fatto che i dati raccolti potrebbero venir scoperti, o che talune funzionalità dei dispositivi potrebbero esser sfruttate a scopo investigativo (con possibile apertura di spazi alle indagini atipiche o ad attività meramente esplorative); alla difficoltà di tracciare una linea di demarcazione fra dati ostensibili e dati privilegiati (con possibile lesione della disciplina dei segreti); al rischio di elusione dei limiti posti dalla legge a tutela delle corrispondenti prove nel mondo "fisico" (con potenziale aggiramento dei divieti probatori); nonché all'incertezza circa la affidabilità dei dati estratti dai dispositivi e dei metodi acquisitivi impiegati (con i relativi problemi in ordine alla valutazione giudiziale della prova scientifica/tecnologica).
Tutti questi aspetti meriterebbero un separato approfondimento. Oggetto della presente trattazione sarà, invece, un punto ulteriore, in un certo senso prodromico rispetto a quelli elencati, riassumibile nel seguente quesito: se sia legittimo – ed eventualmente, a quali condizioni – forzare l'utente a far accedere gli investigatori al proprio dispositivo.
Gli apparecchi in parola presentano infatti un rapporto conflittuale con i sistemi di sicurezza.
Da una parte, è facoltà dell'utente, nella maggior parte dei modelli, inserire una misura di blocco in modo da favorire la protezione dei dati personali e da

---

[5] Così ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen.*, 2018, n. 2, 540 ss., il quale opera una comparazione con la giurisprudenza costituzionale tedesca, che in una celebre decisione (*Bundesverfassungsgericht*, 27 febbraio 2008, in *Riv. trim. dir. pen. econ.,* 2009, n. 3, 679 ss., con nota di FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* Online Durchsuchung*. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona*) ha riconosciuto l'esistenza di un "nuovo" diritto all'uso riservato dei sistemi informatici, in grado di comprendere e superare nell'ambiente digitale sia la classica libertà di domicilio, sia la protezione delle comunicazioni.

[6] Nella Costituzione non è presente una tutela esplicita del diritto alla *privacy*, ma quest'ultima è stata ricondotta, da alcuni studiosi, alla manifestazione di uno (o più) diritti inviolabili, quali gli artt. 13, 14, 15, 21 Cost., oppure direttamente all'art. 2 Cost., come affermato pure dalla Corte costituzionale (Corte cost., 4 dicembre 2009, n. 320). Per una ricostruzione del sottostante dibattito, si veda CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, a cura di Negri, Aprilia, 2007, 9 ss.

[7] SIGNORATO, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, Torino, 2018, 69-71.

prevenire l'uso del *device* da parte di terzi. Ciò può avvenire nelle forme di una *password* alfanumerica (combinazione di lettere, numeri e/o altri caratteri)[8] o, sempre più spesso, biometrica (scansione della retina, dell'iride, delle impronte digitali, dei tratti somatici, del padiglione auricolare, o ancora riconoscimento di un campione vocale, dell'andatura, finanche della battitura o della firma, solo per fare alcuni esempi)[9].

Dall'altra, la lecita barriera posta dal privato a tutela di ingressi non desiderati rischia di scontrarsi con l'altrettanto legittimo interesse pubblico alla repressione degli illeciti penali. Se è vero che tra i doveri di carattere "sociale" richiamati dall'art. 2 Cost. ed esigibili dai consociati va annoverato anche il contributo all'accertamento del fatto[10], è doveroso chiedersi come tale obbligo vada modulato in ragione della veste processuale assunta dal destinatario della richiesta della *password* e in virtù del tipo di prestazione domandata.

Lo studio va quindi impostato tenendo presente che a chiavi diverse possono corrispondere comportamenti diversi: quelle alfanumeriche permettono infatti una autenticazione basata su qualcosa che l'utente "ha" o "conosce" – vale a dire una parola d'ordine o un codice PIN; quelle biometriche, al contrario, valorizzano qualcosa che l'utente "è" – ossia, verificano la dichiarazione d'identità tramite il confronto fra la caratteristica soggettiva (*feature*) rilevata dal sensore e un campione comparativo (*template*) in precedenza memorizzato dal *device*[11].

Non stupisce che proprio queste ultime misure di sblocco siano arrivate a diffondersi rapidamente nel campo degli apparecchi elettronici, in quanto appaiono in grado di offrire, rispetto ai tradizionali codici, molteplici vantaggi: risultano infatti più difficili da compromettere o da rubare, e sono quindi più sicure; velocizzano l'accesso al dispositivo, non richiedendo alcuno sforzo mnemonico; non ammettono condivisione, poiché basate su caratteri fisionomici o comportamentali esclusivi dell'utente. In virtù di questi punti di forza, le *passwords* biometriche appaiono sempre più appetibili anche nel caso degli apparecchi elettronici di nuova generazione, ossia i c.d. dispositivi indossabili (es. i *fitness trackers*), viste le ridotte dimensioni di questi ultimi e la loro fisiologica capacità di raccogliere e conservare proprio i dati

---

[8] In questa categoria ci si sente di includere pure la *password* grafica, la quale permette di sbloccare il dispositivo tracciando un certo segno sullo schermo, visto che pare suscettibile di venir immessa materialmente o comunicata alla stessa stregua di un codice tradizionale.

[9] Per questa ultima elencazione, si veda MARCIALIS, *La sicurezza informatica di frontiera*, in *Sicurezza, informazioni e giustizia penale*, a cura di Colaiacovo, Pisa, 2023, 394.

[10] Per tutti, ALESCI, *Il corpo umano come fonte di prova*, Padova, 2017, 22.

[11] MARCIALIS, *La sicurezza informatica di frontiera*, cit., 392 ss.

biometrici[12].
Il problema non è però di carattere settoriale, essendo un quesito che ha parimenti modo di porsi per la generalità degli *electronic devices* (soprattutto *computer*, *smartphone* e *tablet*) recanti contenuti appetibili a fini di giustizia. Si cercherà perciò di tematizzare l'argomento in un'ottica di ampio respiro.

2. Il versante sovranazionale... Prima di esaminare la normativa primaria italiana occorre chiedersi se una soluzione non si possa trovare già sul piano delle fonti sovranazionali. L'ubiquità della tecnologia e le conseguenti sfide impongono infatti di provare a dare una risposta che trascenda le scelte del singolo ordinamento.
In quest'ottica, significativo pare l'art. 19, § 4, della Convenzione di Budapest sulla criminalità informatica, che impone agli Stati parte di introdurre misure volte a «consentire alle proprie competenti autorità di ordinare ad ogni soggetto che abbia conoscenza del funzionamento del sistema informatico o delle misure utilizzate per proteggere i dati [...] in esso contenuti, di mettere a disposizione tutte le informazioni ragionevolmente necessarie [...]» al sequestro e alla perquisizione di supporti o sistemi. La platea di potenziali destinatari individuata da un così generico riferimento permette di sorreggere la scelta, compiuta da numerosi stati aderenti, di introdurre veri e propri *decryption orders* la cui inottemperanza talvolta è penalmente sanzionata, attivando così un rischio di contrasto con il *nemo tenetur* dei destinatari di simili provvedimenti.
Tuttavia, il riferimento dell'articolo (§ 5) alle condizioni e tutele di cui all'art. 15 del medesimo documento – il quale a sua volta richiama espressamente la Convenzione europea dei diritti dell'uomo quale base inderogabile per l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste dal trattato[13] – potrebbe implicare che una simile richiesta non possa venir rivolta ad un indagato, in quanto potenzialmente lesiva del suo diritto a

[12] Cfr. BIANCHI - OAKLEY, *Wearable authentication: trends and opportunities*, 58 *Information Technology* 255, 2016, 255 ss.

[13] Convenzione del Consiglio d'Europa sulla criminalità informatica, Budapest, 23 novembre 2001, art. 15, § 1, secondo cui «[o]gni Parte deve assicurarsi che l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste in questa sezione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un'adeguata tutela dei diritti umani e delle libertà, in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e agli altri strumenti internazionali applicabili in materia di diritti umani, e che deve considerare il principio di proporzionalità».

non autoincriminarsi[14].
Ciò sposta inevitabilmente l'attenzione sulla norma di rinvio, vale a dire la garanzia euro-convenzionale del diritto al silenzio. La Corte di Strasburgo ha infatti da tempo ricavato in via implicita questa cautela dal diritto ad un processo equo (art. 6, § 1, C.E.D.U.)[15] e dalla presunzione di innocenza (art. 6, § 2), ritenendola funzionale ad evitare errori giudiziari e a mantenere l'onere della prova in capo all'accusa[16].
Il diritto in parola, se pur talvolta è stato esteso fino a coprire anche la consegna di documenti[17], va comunque incontro a diversi limiti. Innanzi tutto, non risulta in grado di impedire l'uso nei procedimenti penali di evidenze ottenute coattivamente e al di fuori della volontà dell'accusato[18]; inoltre, anche una volta che una compressione sia stata riscontrata, non è detto che questa risulti "impropria"[19], cioè in grado di condurre all'annientamento dell'essenza stessa della garanzia[20]. Difatti, a giustificare la costrizione potranno esser sufficienti, oltre all'esame della natura e del grado dell'interferenza, l'efficacia delle cautele procedurali apprestate e l'uso fatto delle informazioni così ottenute[21].
Non è quindi chiaro come potrà orientarsi la Corte europea sul punto, anche se la questione già è stata proposta[22]. Da un lato, i giudici alsaziani potrebbero

---

[14] OERLEMANS - GALIČ, *Cybercrime investigations*, in Van der Wagen - Oerlemans - Kranenbarg (eds.), *Essentials in cybercrime. A criminological overview for education and practice*, Utrecht, 2022, 238; HILDEBRANDT, *Law for computer scientists and other folk*, Oxford, 2020, 180-181.
[15] Corte EDU, 25 febbraio 1993, *Funke c. Francia*, 44.
[16] Corte EDU, Grande Camera, 17 dicembre 1996, *Saunders c. Regno Unito*, 68.
[17] Corte EDU, 3 maggio 2001, *J.B. c. Svizzera*, 63-71; C. EDU, 5 aprile 2012, *Chambaz c. Svizzera*, 50-58.
[18] Corte EDU, *Saunders c. Regno Unito*, cit., 69.
[19] Corte EDU, Grande Camera, 8 aprile 1996, *John Murray c. Regno Unito*, 45.
[20] Secondo Corte EDU, Grande Camera, 13 settembre 2016, *Ibrahim e altri c. Regno Unito*, 267, questa situazione potrebbe verificarsi, ad esempio, ove il sospettato venga spinto a testimoniare a fronte della minaccia di subire una sanzione, oppure venga punito proprio per via del rifiuto opposto; laddove venga assoggettato a pressioni fisiche o psicologiche implicanti la lesione dell'art. 3 C.E.D.U.; o ancora ove le autorità abbiano impiegato sotterfugi per acquisire da lui informazioni, poiché non in grado di ottenerle nelle sedi a ciò deputate.
[21] Corte EDU, Grande Camera, 11 luglio 2006, *Jalloh c. Germania*, 101. La Corte, nella stessa decisione, indica anche l'esistenza di un ulteriore criterio valutativo (§ 117), ossia «*the weight of the public interest in the investigation and punishment of the offence in issue*», il quale, tuttavia, non è stato ripreso dalla giurisprudenza successiva.
[22] *Lamin Minteh c. Francia*, richiesta n. 23624/20, presentata il 10 giugno 2020, comunicata il 31 maggio 2021. Il ricorso interroga la Corte sulla compatibilità con il diritto all'equo processo (art. 6 § 1 C.E.D.U.) e con il rispetto della vita privata e della corrispondenza (art. 8 C.E.D.U.

accettare la distinzione – già menzionata, e che sarà approfondita con più calma nel prosieguo – fra *passwords* alfanumeriche e chiavi d'accesso biometriche, proteggendo le prime in quanto prove dipendenti dalla volontà dell'accusato (*will-dependent*), poiché veicolate tramite dichiarazioni, e non le seconde, per la ragione opposta (*will-independent*), poiché trattasi di dati corporei; dall'altro, potrebbero ritenere che in entrambi i casi una coercizione possa venir ammessa quando opportunamente salvaguardata (tramite efficaci garanzie procedurali e nel rispetto del principio di proporzionalità)[23].

Non è nemmeno escluso che la Corte europea opti per una tutela massimalistica delle *passwords* biometriche, ritenendole incoercibili al pari delle informazioni orali. Questa soluzione sembra invero più difficile, in quanto tali chiavi d'accesso paiono comunque costituite da elementi ottenibili senza la collaborazione dell'accusato, occorrendo al limite un modesto uso della forza – fermo restando il divieto di dar luogo a trattamenti inumani e degradanti (art. 3 C.E.D.U.). Tuttavia, l'art. 6 C.E.D.U., proprio perché non menziona il *nemo tenetur*, non prevede alcuna esplicita barriera, lasciando così la porta aperta anche ad una lettura estensiva della garanzia[24].

Indicazioni più solide non sembrano poi provenire dall'ordinamento euro-unitario, se si osserva come la stessa Direttiva 343/2016/UE, art. 7, pur riconoscendo ad indagati ed imputati il diritto a restare in silenzio (§ 1) e a non autoincriminarsi (§ 2), escluda l'incompatibilità dello *ius tacendi* con la raccolta di «prove che possono essere ottenute lecitamente ricorrendo a poteri coercitivi legali e che esistono indipendentemente dalla volontà» del prevenuto (§ 3), tra le quali si annoverano i materiali acquisibili in forza di un mandato, o per cui sussista un obbligo legale di conservazione e di produzione, ovvero le analisi dell'aria alveolare espirata, del sangue, delle urine o dei tessuti corporei necessari ad eseguire la prova del DNA (*Considerando* n. 29). Non è chiaro se l'elencazione delle evidenze coercibili sia tassativa o meramente esemplificativa, e perciò suscettibile di integrazione: in quest'ultimo caso, non può escludersi che gli Stati membri impieghino questo inciso come base legale per costringere

) di una condanna penale inflitta ad un soggetto sottoposto a custodia (*garde à vue*) che si sia rifiutato di rivelare la *password* del proprio *smartphone* agli inquirenti.

[23] Con riferimento a quest'ultima ipotesi, pare possibilista HILDEBRANDT, *Law for computer scientists and other folk*, cit., 181.

[24] In questo senso si veda ZONTEK, *Biometric Encryption of Smart Devices and the Prohibition against Self-incrimination in Criminal Procedure. Old Guarantees in the New World*, 32 *European Journal of Crime, Criminal Law and Criminal Justice* 156, 2024, 170 ss.

l'imputato a rivelare la chiave di accesso al proprio dispositivo[25].
La giurisprudenza della Corte di giustizia dell'Unione europea, dal canto suo, non sembra aver affrontato espressamente la questione. In un recente arresto, relativo alle garanzie applicabili durante l'accesso ai dati contenuti nel cellulare dell'indagato[26], la facoltà di opporre il diritto al silenzio è stata infatti estromessa dal *thema decidendum*, poiché già rispettata nel procedimento *a quo*[27].
Insomma, se e come la disciplina europea (convenzionale e comunitaria) arriverà ad abbracciare la tutela delle chiavi d'accesso è materia controversa. Quel che appare chiaro dalle note che precedono è però la diffusa tendenza a operare un discrimine fra il "nucleo duro" del diritto al silenzio, basato su richieste di informazioni, e una sua "periferia" più flessibile, incentrata sull'acquisizione di *material evidence* – inidonea, in quanto tale, a costringere il prevenuto ad attivarsi.

3. (Segue) *Uno sguardo comparato.* Una volta delineato il quadro sovranazionale, occorre chiarire come i diversi ordinamenti si pongano dinanzi alla sfida comune posta dall'accesso ai dispositivi elettronici.
Volendo schematizzare, emerge un duplice approccio seguito nei Paesi dell'Europa continentale e nelle isole britanniche.
Innanzi tutto, si possono individuare Stati che, non operando alcuna distinzione in base al tipo di chiave d'accesso, pongono un obbligo generalizzato di collaborazione in capo al titolare del dispositivo o, in generale, ad ogni soggetto che abbia le conoscenze necessarie ad operare lo sblocco. In questa schiera si annoverano, ad esempio, ordinamenti quali Inghilterra e

[25] PIVATY et al., *Opening Pandora's box: The Right to Silence in Police Interrogations and the Directive 2016/343/EU*, in 12 *New Journal of European Criminal Law*, 2021, 339.
[26] Corte Giust. U.E., Grande Sezione, 4 ottobre 2024, *C.G. v Bezirkshauptmannschaft Landeck*, 81 ss. In particolare, la Direttiva 2016/680, letta alla luce degli artt. 47 e 52, § 1, della Carta di Nizza, è stata ritenuta ostativa ad una disciplina nazionale che consenta alle autorità procedenti di accedere ai dati contenuti in un cellulare, in assenza di una informazione agli interessati in ordine ai motivi sui quali l'autorizzazione, rilasciata da un giudice o da un'autorità amministrativa indipendente, si basa. Tale incombente, finalizzato a tutelare il diritto ad un ricorso effettivo, opera a partire dal momento in cui l'informazione non rischi più di compromettere le indagini condotte da tali autorità.
[27] *Ivi*, 21. In questa pronuncia, infatti, i vani tentativi della polizia austriaca di introdursi nel cellulare sequestrato scaturivano proprio dal legittimo rifiuto del ricorrente di consentire l'accesso ai propri dati.

Galles[28], Irlanda[29], Belgio e Francia.
Questi due ultimi appaiono particolarmente didascalici, vista la radicalità delle scelte effettuate. In Belgio, infatti, l'art. 88-*quater* del *code d'instruction criminelle* prevede un obbligo di cooperazione (introdotto proprio in virtù dell'art. 19, § 4, della Convenzione di Budapest)[30] in capo a coloro che si presume abbiano una conoscenza particolare di un sistema informatico o dei servizi utilizzati per proteggere i dati ivi memorizzati, elaborati o trasferiti. Ad essi può venir ordinato di fornire, in forma comprensibile, informazioni circa le modalità di accesso al sistema o ai dati (§ 1) ovvero di eseguire operazioni sul *computer* oggetto d'indagine, quali l'accesso, la copia, la rimozione, la crittazione o la decrittazione dei dati contenuti (§ 2). A tal fine è necessaria un'ordinanza del giudice istruttore, il mancato rispetto della quale costituisce reato punibile con la reclusione fino a tre anni e/o con sanzione pecuniaria; se, tuttavia, la collaborazione rifiutata avrebbe potuto ridurre e/o attenuare le conseguenze di un reato grave, la pena si può spingere sino a 5 anni di reclusione e alla irrogazione di un'ammenda compresa tra 50.000 e 500.000 euro (§ 3).
Le condotte di cui al secondo paragrafo, per espressa indicazione normativa, non possono venir imposte all'imputato. Non è chiaro invece se tale esenzione riguardi anche l'obbligo cooperativo indicato nel primo paragrafo. In effetti, è lecito presumere che i prevenuti siano dotati di una "conoscenza particolare" dei sistemi informatici nella loro disponibilità[31]. In tal senso sembra muoversi la giurisprudenza maggioritaria: smentendo un orientamento prima adottato da taluni tribunali inferiori[32], la Corte di cassazione belga ha di recente ritenuto che il privilegio contro l'autoincriminazione e la presunzione di innocenza non siano diritti assoluti, e che un giudice istruttore possa perciò ordinare

---

[28] In base al *Regulation of Investigatory Powers Act* (RIPA 2000), la polizia può richiedere l'accesso ai dati contenuti in dispositivi elettronici (sequestrati durante le indagini) protetti da crittografia. Ove l'imputato/indagato rifiuti di fornire il codice, la polizia ha la facoltà di chiedere al giudice l'emissione di un *notice requiring disclosure* ai sensi dell'articolo 49 RIPA. In caso di mancata ottemperanza a tale avviso, potrà essere inflitta una pena massima di 5 anni, qualora il procedimento riguardi casi di "*national security*" o "*child indecency*"; di 2 anni, nelle altre situazioni (art. 53 RIPA).

[29] *Section 48 Criminal Justice Theft and Fraud Offences Act* (2001); *Section 7 Criminal Justice Offences Relating to Information Systems Act* (2017).

[30] Cfr. *supra* par. 2.

[31] ROYER - YPERMAN, *You have the righet to remain silent...until we want your smartphone password*, in *CiTiP blog* (Feb. 13, 2020), https://www.law.kuleuven.be/citip/blog/you-have-the-right-to-remain-silent-until-we-want-your-smartphone-password/.

[32] Cfr. anche per i richiami giurisprudenziali BEAZLEY et al., *Silence with caution: the right to silence in police investigations in Belgium*, 12 *New Journal of European Criminal Law* 408, 2021, 422-423.

all'indagato – a pena di reclusione – di fornire il codice di accesso al suo telefono cellulare quando la decrittazione risulti fondamentale per scoprire la verità[33]. Il tribunale supremo ha quindi qualificato l'ordine in parola come un obbligo di carattere meramente "informativo", non implicante una cooperazione con le indagini: secondo la Corte, in breve, il codice di accesso integrerebbe di per sé un dato "neutro", privo di valenza autoincriminante[34]. Un simile assetto è stato peraltro accolto, nello stesso torno di tempo, pure dal locale giudice delle leggi[35].

In maniera ancor più diretta, in Francia, la Cassazione ha avuto di recente modo di ribadire che indagati e imputati possono esser obbligati a comunicare agli inquirenti le *passwords* del telefono cellulare (*passcode*)[36]. Secondo la motivazione addotta, il codice d'accesso costituirebbe infatti una *convention de déchiffrement*, ossia un mezzo di crittografia, una chiave volta a sbloccare lo schermo del telefono: dimodoché la garanzia contro l'autoincriminazione e il diritto di rimanere in silenzio non avrebbero modo di essere invocati, alla luce dell'art. 434-15-2 *code pénal*. Quest'ultimo punisce infatti il rifiuto di fornire la *password* con un'ammenda fino a 270.000 euro o 3 anni di reclusione (la pena è aumentata fino a 450.000 euro o a 5 anni di reclusione quando lo sblocco avrebbe potuto impedire un reato o ridurne i danni). Secondo la logica seguita (anche) dai giudici francesi, dunque, l'esame del telefono cellulare risulterebbe equiparabile ad una perquisizione, dal momento che il mezzo in parola corrisponderebbe ad uno spazio privato, non già ad un surrogato della persona indagata[37].

Un esito parzialmente diverso si può invece ravvisare presso un altro gruppo di Paesi, in cui il discrimine corre lungo la linea che divide *passwords* alfanumeriche e dati biometrici: ne fanno parte, ad esempio, Paesi Bassi[38] e

---

[33] *Hof v. Belgium*, Court of Cassation, decision 4 February 2020, P.19.1086.N.

[34] *Ibid.*

[35] Constitutional Court of Belgium, Judgement n. 28/2020 of 20 February 2020, § B.6.2. Secondo questa decisione, tale assetto normativo non violerebbe né il principio di uguaglianza, né il diritto ad un equo processo, né il diritto alla riservatezza.

[36] Cour de cassation, assemblée plénière, 7 nov. 2022, n° 21-83.146; nello stesso senso si vedano Crim. 12 janv. 2021, n° 20-84.045, D. 2021. 82; Crim., 10 déc, 2019, n° 18-86.878, D. 2019. 2410.

[37] Così PARIZOT, *Qu'est-ce qu'un téléphone portable?*, in *Revue de science criminelle et de droit pénal comparé*, 2021, 1, 129.

[38] È infatti vero che l'art. 125k del codice di procedura penale olandese esclude testualmente che un ordine di decrittazione possa venir impartito alla persona sottoposta ad indagini: nonostante ciò, questi può comunque venir fisicamente costretto a fornire dati biometrici per sbloccare il telefono. Il limite menzionato sembra infatti operare solo ove venga richiesta all'indagato una cooperazione attiva, non

Germania.
Particolarmente esplicativo appare l'approccio seguito in quest'ultimo ordinamento. Sebbene non sia possibile rinvenire un obbligo di *disclosure* della chiave d'accesso, il § 81b (1) StPO, relativo all'identificazione dell'indagato, è stato considerato in grado di legittimare le autorità a procedere allo sblocco dello *smartphone* mediante l'impiego di matrici biometriche[39]. La ragione di questa esegesi è intuibile, e risiede nell'assenza d'una richiesta di cooperazione attiva rivolta al prevenuto[40].
All'esito di questa sommaria indagine, il cui scopo è di esemplificare un *trend* e non già di fornire analisi esaustive, emerge chiaramente come gli ordinamenti europei oscillino fra l'assenza di copertura delle chiavi d'accesso da parte del *nemo tenetur* e l'applicazione di tale garanzia (quantomeno) con riferimento al codice alfanumerico.
Una posizione simile a quest'ultima si registra anche oltreoceano, negli Stati Uniti d'America, dove la maggior parte delle corti statali e federali aderisce alla tesi secondo cui il Quinto Emendamento – a mente del quale «[*n*]*o person* [...] *shall be compelled in any criminal case to be a witness against himself* [...]» – troverebbe applicazione solo dinanzi alla richiesta d'una testimonianza, orale

quando la chiave di accesso risulti indipendente dalla sua volontà e sia ottenibile mediante un uso proporzionato della forza.
Così Supreme Court of the Netherlands, decision 9 February 2021, n. 19/05471 CW. Cfr. anche il testo attuale dell'art. 558 del codice di procedura penale olandese, a seguito delle modifiche in vigore dal 1 ottobre 2022 (valide fino al 1 ottobre 2025): «*If a seized automated work is biometrically secured or the data are biometrically encrypted in the form of a fingerprint or an iris or facial image, the public prosecutor may order the investigating officer to undo this security or encryption. In order to execute this order, the investigating officer may take the measures that are reasonably necessary to do so, against the will of anyone who may reasonably be suspected of being able to undo this security or encryption*» (traduzione dall'olandese).
Per un approfondimento, si veda VRUGT, *A pragmatic attitude: the right to silence in the Netherlands*, 12 *New Journal of European Criminal Law* 389, 2021, 394-395, la quale sottolinea che in taluni casi le corti inferiori sono arrivate a riconoscere un tale obbligo anche in caso di *passwords* "tradizionali", ove la situazione risultasse connotata da particolare urgenza.

[39] In tal senso si veda LG Ravensburg (2023) 11 Gs 69/23 (*Regional Court of Ravensburg*), secondo cui il § 81 cit. consentirebbe la raccolta delle impronte finalizzata a sbloccare il cellulare.

[40] Non a caso, la Corte territoriale ha anche specificato che la medesima conclusione sarebbe stata raggiungibile pure nel caso in cui la polizia avesse proceduto a porre forzatamente il polpastrello a contatto con lo schermo. La decisione non è comunque andata esente da critiche in dottrina, dal momento che la norma invocata non farebbe menzione alcuna della possibilità di impiegare dati biometrici a fini di sblocco, essendo volta a disciplinare solo la raccolta di dati a fini di identificazione. Così F. NICOLAI et al., *When objects betray you: the Internet of Things and the privilege against self-incrimination*, 33 *Information & Communications Technology Law*, 2024, 255 ss.

o scritta, *contra se*[41]. Pertanto, il *privilege against self-incrimination* sarebbe in grado, in linea di principio, di coprire solo la rivelazione della *password* alfanumerica, non lo sblocco biometrico[42].

Questa prima impressione va però temperata alla luce della teoria giurisprudenziale nota come *act of production doctrine*, secondo cui atti di carattere "testimoniale" sarebbero tutti quelli in grado di veicolare, in maniera non dissimile da una dichiarazione, notizie circa l'esistenza, il possesso e l'autenticità dei contenuti cercati[43].

Una simile lettura solleva il dubbio che anche l'impiego della chiave d'accesso biometrica, non diversamente dall'esecuzione coattiva di altri comportamenti materiali – quali la decrittazione e la produzione – possa apparire un'attività gravida di significato, e risultare perciò meritevole di tutela. Sul punto non si registrano indirizzi univoci. Alcune corti hanno infatti ritenuto che costringere l'imputato a fornire un dato fisionomico come l'impronta digitale non lo porti, di per sé, ad autoincriminarsi[44]; altre hanno optato per la tesi contraria, affermando che essere obbligati a sbloccare il dispositivo equivarrebbe a dover fornire l'ubicazione e i contenuti (indizianti) d'un "archivio"[45].

---

[41] Perché sia invocabile il Quinto Emendamento occorre che si verifichino tre condizioni: l'individuo deve esser costretto per legge a collaborare con il Governo; la condotta obbligata deve essere di carattere testimoniale, ossia idonea a costringere una persona a rivelare il contenuto della propria mente; l'informazione veicolata deve essere incriminante. Cfr. es. *Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 189-190 (2004).

[42] *United States v. Doe (In re* Grand Jury Subpoena), 670 F.3d 1335, 1341 (11th Cir. 2012); *United States v. Kirschner*, 823 F. Supp. 2d 665 (E.D. Mich. 2010); *Commonwealth v. Baust*, 89 Va. Cir. 267 (2014). Di regola, infatti, il privilegio contro l'autoincriminazione non opera con riferimento alla raccolta di campioni corporei. Cfr. es. *Schmerber v. California*, 384 U.S. 757, 760-765 (1966).
Metaforicamente, occorre perciò distinguere la consegna della "chiave per una cassaforte" (*key to a strongbox*) dalla rivelazione di una "combinazione" (*combination to a wall safe*). Pur avendo il medesimo scopo, la prima appare neutra sul piano del diritto a tacere, risolvendosi in una operazione dal carattere prettamente materiale, mentre la seconda appare potenzialmente lesiva del *privilege against self-incrimination*, in quanto impone al prevenuto di svelare il contenuto della propria mente. Cfr. *Doe v. United States*, 487 U.S. 201, 210, n. 9, 219 (1988) (Stevens, J., dissenting); *United States v. Hubbell*, 530 U.S. 27, 43 (2000).

[43] *Fisher v. United States*, 425 U.S. 391, 1976, 410.

[44] *In Matter of Search Warrant Application for [redacted text]* 279 F. Supp. 3d 800 (N. D. Ill. 2017). Più di recente, si veda *United States v. Payne*, 99 F.4th 495, 508-513 (9th Cir. 2024), che, pur rigettando nel caso di specie il valore testimoniale dello sblocco biometrico, arriva ad affermare come ciò dipenda in gran parte dalle dinamiche fattuali.

[45] *In re Search of a Residence in Oakland* 354 F. Supp. 3d 1010 (N. D. Cal. 2019). Più di recente, si veda *United States v. Brown*, No. 23-3074, 23 ff. (D.C. Cir. Jan. 17, 2025). In dottrina, favorevoli a questa visione sono JACOBSON, *Face Off: Overcoming the Fifth Amendment Conflict Between Cybersecurity and Self-Incrimination*, 36 *Journal of Law and Health* 185, 2023, 201; CARNES, *Face ID and Fingerprints: Modernizing Fifth Amendment Protections for Cell Phones*, 66 *Loy. L. Rev.* 183, 2020,

Tuttavia, anche volendo optare per quest'ultima esegesi estensiva, una eccezione si può in ogni caso rinvenire quando si sia al cospetto di una *foregone conclusion*. Secondo questa lettura, anch'essa d'origine pretoria[46], quando l'autorità che procede è in grado di indicare con un ragionevole grado di precisione (*reasonable particularity*) che l'elemento incriminate esiste, è autentico ed è sotto il controllo dell'interessato, l'atto di produzione forzata non assume più natura testimoniale, poiché non in grado di aggiungere nulla alle informazioni a disposizione dell'accusa[47]. Quando tale esito si verifica, il valore dichiarativo dell'atto viene azzerato, e la cooperazione può conseguentemente venir imposta[48].

4. Obbligo di rivelazione della password *e diritto al silenzio: codici alfanumerici.* Per quanto riguarda invece l'ordinamento italiano, occorre partire dall'inesistenza, allo stato, di un obbligo di collaborazione in capo all'indagato/imputato relativo alla consegna della *password* alfanumerica.
L'unica disposizione rassomigliante ad un *decryption order* sembra essere l'art. 248 c.p.p., ossia l'invito a consegnare la cosa cercata tramite perquisizione – la quale però non rappresenta un obbligo per l'indagato, ed è comunque volta ad ottenere la *res*, più che la chiave per accedere ad essa[49].
Tuttavia, scorrendo il codice è possibile imbattersi anche in alcuni punti deboli, suscettibili di aprire spiragli coercitivi.
Si pensi innanzi tutto alla perquisizione dei dispositivi elettronici (artt. 247, co. 1-*bis*; 352, co. 1-*bis*,c.p.p.)[50]. Se è vero infatti che l'autorità procedente è tenuta,

---

202 ss; METZ, *Your Device Is Disabled: How and Why Compulsion of Biometrics to Unlock Devices Should Be Protected by the Fifth Amendment Privilege*, 53 *Val. U. L. Rev.* 427, 2019, 460 ss.

[46] Risalente a *Fisher v. United States*, cit., 411.

[47] Cfr. es. *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718, 3-4 (D. Vt. Feb. 19, 2009).

[48] È controverso se la *foregone conclusion* permetta anche la rivelazione diretta della *password* alfanumerica, e non solo la sua materiale immissione nel dispositivo. Alcune pronunce si sono espresse in senso favorevole, mentre altre hanno dissentito. Per un esempio delle prime, si veda *State v. Andrews*, 234 A.3d 1254 (N.J. 2020); per le seconde, invece, *Commonwealth v. Davis*, 220 A.3d 534, 2019, 548 ss.

[49] Un simile pensiero è stato espresso da ZAMPINI, nell'intervento alla conferenza *Dimensione giudiziaria e dimensione mediatica della presunzione d'innocenza*, EmpRiSe Project, Roma, 14 ottobre 2021. Attualmente non sono disponibili pubblicazioni o registrazioni in merito.

[50] Per l'osservazione secondo cui la distinzione tra perquisizione ed ispezione "informatica" si basa sulla presenza o meno di misure di sicurezza, si veda ad esempio FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, in *Cybercrime*, a cura di Cadoppi et al., 2ª ed., Milano, 2023, 1603. In senso contrario si pone chi invece ritiene che tale distinzione dovrebbe venir superata nel caso delle indagini digitali, in quanto ogni perlustrazione del contenuto del dispositivo consisterebbe necessariamente in una ricerca della prova e non in una mera constatazione dello stato delle cose. Così ad esempio MURRO,

anche in queste circostanze, ad avvertire l'indagato della facoltà di nominare un difensore di fiducia (artt. 356 c.p.p. - 114 disp. att. c.p.p.), lo stesso non può dirsi per quanto riguarda il diritto a tacere, del quale non viene fatta menzione[51].

Si pensi poi alla facoltà della polizia giudiziaria di richiedere alla persona sottoposta ad indagini, anche in assenza del difensore, «notizie e indicazioni» (art. 350, cc. 5 e 6, c.p.p.), ovvero di ricevere da essa dichiarazioni spontanee (art. 350, co. 7 c.p.p.), senza alcun previo avviso circa il diritto a restare in silenzio[52]. Le notizie così ottenute dagli operanti risultano certo inutilizzabili (co. 6) o al più spendibili in dibattimento mediante le contestazioni (co. 7, che richiama l'art. 503, co. 3, c.p.p.)[53]. La lacuna informativa, tuttavia, rischia di mascherare una surrettizia elusione dello *ius tacendi* ove tali conoscenze rappresentino lo spunto investigativo che porti ad acquisire ulteriori elementi di prova, dei quali non sarà poi possibile lamentare l'invalidità[54]. In altre parole, il contrappeso apprestato dal legislatore attraverso la comminatoria dell'inutilizzabilità – totale (co. 6) o parziale (co. 7) – pare pressoché inutile nel nostro caso, perché la *password* risulta comunque in grado di schiudere l'accesso ad una ricchissima platea di dati immuni da sanzioni processuali.

In termini concreti, ove gli inquirenti si trovino dinanzi alla difficoltà o impossibilità di superare le barriere poste all'ingresso nel dispositivo, potranno facilmente esser tentati di aggirare l'ostacolo stimolando il prevenuto a

---

Lo smartphone *come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Milano, 2024, pp. 124-125; SIGNORATO, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, cit., 210.

51 LARONGA, *Sul valore probatorio del contegno non collaborativo dell'imputato nell'accertamento del fatto proprio*, in *Quest. giust.*, 17 aprile 2014, 6, https://www.questionegiustizia.it/data/doc/415/nemo_tenetur_se_detegere_relazione_laronga.pdf. Cfr. anche MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, in *Proc. pen. giust.*, 2021, 4, 736-737.

52 *Ibid.* Si segnala che oggi, a seguito della riforma operata con art. 3, co. 1, lett. b) d.l. 16 settembre 2024, n. 131, convertito con modificazioni dalla L. 14 novembre 2024, n. 166, il co. 5 consente la richiesta di informazioni all'indagato sul luogo o nell'immediatezza del fatto «quando ciò è imposto dalla necessità di evitare un imminente pericolo per la libertà, l'integrità fisica o la vita di una persona oppure dalla necessità di compiere attività indispensabili al fine di evitare una grave compromissione delle indagini».

53 Le dichiarazioni spontanee possono però venir impiegate nella fase procedimentale, ossia in sede di incidente cautelare e nei riti a prova contratta. Cfr. es. Cass. pen., Sez. II, 13 marzo 2018, n. 14320, Rv. 272541 – 01.

54 LARONGA, *Sul valore probatorio del contegno non collaborativo dell'imputato nell'accertamento del fatto proprio*, cit., 6. Nello stesso senso si esprimeva già MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, 12, 4516.

rilasciare le suddette "indicazioni" volte a proseguire l'indagine, o a fornirle "spontaneamente" – informazioni che, nel caso di specie, sarebbero rappresentate proprio dalla *password* o da un altro mezzo di decrittazione[55].
A fronte di quanto esposto, è facile comprendere come mai si rinvenga in dottrina, in un'ottica ricostruttiva, un diffuso consenso circa la necessità di ricondurre la richiesta della *password* all'area del diritto al silenzio in senso stretto – tanto che, si afferma, anche in caso di atti "a sorpresa" quali sono le perquisizioni (pure di dispositivi elettronici), la polizia giudiziaria e il pubblico ministero dovrebbero avvisare l'indagato della facoltà di non rispondere (artt. 64, co. 3, lett. b) c.p.p. - 350, co. 1 c.p.p.) prima di domandargli la rivelazione della chiave di accesso[56]. Solo in tale maniera potrebbe dirsi tutelato lo *ius*

---

[55] *Ibid.*

[56] LUPÀRIA, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, VII, I, a cura di Garuti, Torino, 2001, 387-388; ID., *Processo penale e tecnologia informatica*, in *Dir. Internet*, 2008, 3, 227-228; ID., *Disciplina processuale e garanzie difensive*, in AA.VV., *Investigazione penale e tecnologia informatica: l'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, 159-160. Nello stesso senso si vedano ROMBI, *Mentire sui propri precedenti penali equivale a difendersi? La soluzione della Corte costituzionale a tutela del diritto al silenzio*, in *Proc. pen. giust.*, 2024, 1, 70-71, che osserva come «[i]n queste situazioni, il mancato avvertimento, laddove accompagnato dal possibile impiego di quanto dichiarato, magari anche solo a fini orientativi delle indagini, permette che si realizzi una censurabile rinuncia inconsapevole al diritto al silenzio»; DEL GIUDICE, *The principle of* nemo tenetur se detegere *in the age of data*, 98 *Revista "Curentul Juridic"* 76, 2024, 84, https://revcurentjur.ro/old/pms/uploads/recjurid243_8.pdf; RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, in *Cass. pen.*, 2022, 2, 889; SFORZA, *Il* nemo tenetur se detegere *nelle audizioni Consob e Banca d'Italia: uno statuto ancora da costruire*, in *Sistema penale*, 2022, 2, 100; MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., 737; CAJANI, *Le "nuove frontiere" dell'investigazione digitale alla luce della legge n. 48/2008, ovvero: quello che le norme (ancora) non dicono*, in Cyber forensics *e indagini digitali. Manuale tecnico-giuridico e casi pratici*, a cura di Aterno-Cajani-Costabile-Curtotti, Torino, 2021, 551; PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, cit., 295-296; SIGNORATO, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, cit., 33-34; PITTIRUTI, Digital evidence *e procedimento penale*, Torino, 2017, 103; RIVELLO, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 2013, 4, 1718; VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, in Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, a cura di Lupària, Milano, 2012, 133-134; MARAFIOTI, Digital evidence *e processo penale*, cit., 4515-4516.
In senso parzialmente contrario si veda FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, cit., p. 1629, nota 218, secondo cui il problema risiederebbe tutt'al più negli eventuali abusi commessi in fase investigativa, ove la cooperazione dell'interessato venisse coartata di fatto. D'altronde, se «è vero [...] che la collaborazione non può essere imposta, [...] è altrettanto vero che l'avvertimento del diritto al silenzio è garanzia delineata con riferimento agli atti di indagine in cui l'indagato interviene, non per propria scelta, come dichiarante. Appare significativo, d'altro canto, che l'avvertimento in questione

tacendi, a sua volta baluardo della libertà di autodeterminare le opzioni difensive nei confronti degli organi di giustizia penale. La mancata somministrazione dell'avvertimento dovrebbe pertanto comportare la inutilizzabilità del dato carpito (art. 64, co. 3-*bis* c.p.p.) e, «secondo l'orientamento più rigoroso, di tutti i risultati investigativi ottenuti [...] a seguito della violazione del divieto»[57].

Non potrebbe in senso contrario invocarsi l'art. 66, co. 1 c.p.p., che pone quale eccezione al diritto al silenzio dell'imputato l'esplicitazione delle sue generalità e di «quant'altro [possa] valere a identificarlo», dato che le *passwords*, «più che riguardare l'identità di un soggetto, sembrano finalizzate alla protezione delle informazioni elettroniche trasmesse o conservate [...]»[58].

---

non sia previsto per l'ipotesi delle dichiarazioni spontanee rese dall'indagato alla polizia giudiziaria ai sensi dell'ultimo comma dell'art. 350 c.p.p.».

[57] LUPÀRIA, Computer crimes *e procedimento penale*, cit., 159-160.

[58] SIGNORATO, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, cit., 34.

Questione ulteriore è la riconducibilità del *nickname* o dell'*avatar* – ossia rispettivamente del nome e dell'immagine con cui l'imputato si presenta e agisce nel *web* – al citato obbligo di identificazione.

La dottrina domestica sul punto pare divisa. Da una parte si è sostenuto che una lettura aggiornata all'evoluzione tecnologica imporrebbe di interpretare estensivamente il dettato dell'art. 66, co. 1 c.p.p., ricomprendendo nell'obbligo ostensivo, accanto alle identità fisica e anagrafica, pura quella "virtuale", costituita da *nickname* e *avatar* (*ivi*, 35); dall'altra, si è obiettato che la disposizione in parola, concepita avendo riguardo alla sola identità fisica e anagrafica, dovrebbe essere oggetto di stretta esegesi in quanto norma eccezionale. Un diverso esito non potrebbe quindi prescindere dall'intervento del legislatore (così CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, 5 *Rev. bras. de direito processual penal* 1167, 2019, 1180-1181); infine, vi è chi ha negato recisamente tale possibilità sottolineando come, nel caso di reati commessi tramite mezzi informatici, pretendere il disvelamento del *nickname* o dell'*avatar* equivarrebbe di fatto a costringere l'indagato ad ammettere l'addebito (MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., 736).

La seconda impostazione citata si lascia preferire, poiché maggiormente in linea con gli ordinari canoni interpretativi (art. 14 Preleggi): se il rapporto tra diritto al silenzio e obbligo *ex* art. 66 c.p.p. è un rapporto tra regola ed eccezione, occorre evitare che una lettura largheggiante della disciplina processuale possa comprimere lo *ius tacendi* al di fuori dei casi tassativamente indicati.

Naturalmente, tale conclusione non deve far presumere l'irrilevanza del contributo informativo in parola, che potrà comunque legittimamente venir richiesto dagli inquirenti ai sensi dell'art. 21 disp. att. c.p.p., ossia quando, in occasione del primo atto in cui è presente l'indagato o l'imputato, quest'ultimo viene invitato a rivelare ulteriori informazioni personali, tra cui, per quanto qui interessa, l'esistenza di un "soprannome" o di uno "pseudonimo". Se la disposizione eccezionale di cui all'art. 66 c.p.p. non può essere interpretata fino al punto di comprendere una "identità digitale" non ravvisata (allo stato) dal legislatore, lo stesso non potrebbe dirsi per i due concetti appena menzionati, la cui indeterminatezza anzi ben si attaglierebbe al *nickname* – che a tutti gli effetti è un "altro nome", non anagrafico, con cui l'individuo è conosciuto in una più o meno ampia comunità virtuale. Se si accetta di ricondurre il *nickname* alla norma di attuazione, allora anche la richiesta all'indagato di rivelare lo stesso dovrebbe venir preceduta, come ha chiarito di recente la Consulta (C. cost., 5 giugno 2023, n. 111), dall'avviso

La giurisprudenza della Cassazione, dal canto suo, sembra accogliere soluzioni non dissimili. Pur essendosi sinora occupata solo di rado della compatibilità di tali richieste collaborative con il principio del *nemo tenetur*, ha già avuto modo di affermare che il rifiuto di fornire le chiavi di accesso al dispositivo elettronico da parte dell'indagato rappresenti una legittima manifestazione del diritto di difesa[59]. Emblematico pare un recente caso, in cui la rivelazione del codice d'accesso ai documenti celati nel cellulare era stata sollecitata dalla polizia a seguito di perquisizione preventiva *ex* art. 103 d.P.R. n. 309/1990, la quale aveva portato a rinvenire una certa quantità di droga occultata sulla persona dell'utente[60]. Secondo i giudici supremi, ferma restando l'impossibilità di supplire tramite il consenso dell'indagato alla mancanza di una previa autorizzazione o di una convalida successiva dell'atto di indagine da parte dell'autorità giudiziaria, appariva chiaro che, a seguito dell'emersione di indizi di reato, «ogni ulteriore attività di indagine [...] richiede[nte] la collaborazione della persona indagata [avrebbe dovuto venir] espletata dopo la formale comunicazione degli avvisi di tutte le facoltà difensive ad essa spettanti, ivi compresa quella della facoltà di rifiutare tale collaborazione ed il diritto ad essere assistito da un difensore [...]»[61].

5. (Segue) *Chiavi d'accesso biometriche.* Maggiori spazi per la collaborazione coartata potrebbero invece aprirsi nel caso in cui il dispositivo risultasse

---

circa la facoltà di non rispondere, finendo perciò tutelata dal diritto al silenzio (sul punto pare possibilista DEL GIUDICE, *The principle of* nemo tenetur se detegere *in the age of data*, cit., 81-82).
Ad ogni modo, anche qualora si volesse ricondurre il *nickname* alla fattispecie aperta dell'art. 66 c.p.p. (secondo cui l'indagato è tenuto a rivelare, oltre alle generalità, pure «quant'altro può valere a identificarlo»), ciò potrebbe non bastare a ritenere del tutto inoperante il diritto al silenzio. È qui utile infatti richiamare quella visione dottrinale che da tempo auspica l'allargamento dello *ius tacendi* e del mendacio anche alla domanda sulle mere generalità, ove ciò sia imposto da una stretta necessità difensiva, come avverrebbe ad esempio nei casi di sostituzione di persona (art. 494 c.p.) (MAZZA, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, in *Trattato di procedura penale*, diretto da Ubertis-

Voena, VII.1, Milano, 2004, 112 ss.).

[59] Cass. pen., Sez. V, 30 maggio 2017, n. 48370, Rv. 271412. Nel caso di specie, la Cassazione osserva come i provvedimenti di perquisizione e sequestro avevano sortito effetti limitati proprio per via della condotta impeditiva degli imputati, che erano riusciti a bloccare tempestivamente i propri apparecchi elettronici per poi rifiutarsi, invocando il diritto di difesa, di rivelare le chiavi d' accesso ai medesimi.

[60] Cass. pen., Sez. VI, 20 novembre 2024, n. 1269, in *DeJure*.

[61] *Ibid.*

protetto non dalle tradizionali *passwords* alfanumeriche, ma da chiavi d'accesso biometriche.
Dinanzi a queste ultime, si è infatti osservato, l'imputato verrebbe in considerazione non quale "organo di prova", a cui viene richiesto di prestare un contributo attivo alle indagini, bensì come "oggetto di prova"[62], che deve semplicemente soggiacere all'acquisizione conoscitiva, senza che la sua volontà venga in alcun modo sollecitata[63].
L'argomento è semplice e lineare: a differenza di quanto accade per le *passwords* alfanumeriche, l'impiego di chiavi biometriche per sbloccare il dispositivo non imporrebbe all'indagato un *facere*, bensì un mero *pati*, il che escluderebbe la possibilità di invocare il diritto al silenzio[64]. Peraltro, dal momento che si renderebbe necessario esercitare una coazione – modica ma non insignificante – sul titolare (immobilizzarlo temporaneamente; forzarlo ad appoggiare il polpastrello sul rilevatore di impronte digitali; e così via) un simile assetto sarebbe legittimo, in forza dell'art. 13 Cost., soltanto in presenza di una previsione legislativa espressa, al momento assente. L'attività di identificazione dell'indagato a cui procede la polizia giudiziaria ai sensi dell'art. 349, co. 2 c.p.p. – mediante «rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti» – non potrebbe infatti essere piegata ad altri fini in via interpretativa[65].
S'aprirebbe così uno scenario per certi versi paradossale: le *passwords* biometriche, più forti delle controparti tradizionali dal punto di vista tecnico-informatico, risulterebbero più deboli dal punto di vista giuridico.
Questa visione, per quanto plausibile, non può dirsi pacifica. Diversi sono in effetti gli argomenti addotti in senso contrario.
È stata innanzi tutto prospettata una violazione del principio di uguaglianza (art. 3 Cost.), dal momento che pare irragionevole discriminare il livello di tutela del *nemo tenetur* in relazione alle diverse tipologie di chiave di accesso al dispositivo, visto che *passwords* biometriche e alfanumeriche svolgono la stessa funzione, e che in entrambi i casi la rivelazione del dato integra l'antecedente

---

[62] La distinzione fra imputato quale organo ed oggetto di prova si fa tradizionalmente risalire a FLORIAN, *Delle prove penali*, vol. II, Milano, 1924, 9.
[63] RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, cit., 890.
[64] *Ibid.* Nello stesso senso si veda DEL GIUDICE, *The principle of* nemo tenetur se detegere *in the age of data*, cit., 87-89.
[65] MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., 739.

necessario della ricerca della prova a proprio danno[66]; inoltre, la stessa qualifica dei dati biometrici quali elementi esistenti indipendentemente dalla volontà del prevenuto è stata messa in discussione, poiché gli stessi, «a differenza del campione sanguineo, sono stati "creati" *ad hoc* proprio da quest'ultimo, con il fine di proteggere informazioni a carattere riservato»[67]. Per l'effetto, non dovrebbe esserci una differenza di tutela per ciò che concerne il *nemo tenetur* fra *passwords* biometriche e alfanumeriche[68].

Entrambe le tesi indicate colgono qualche aspetto; forse, però, la verità sta nel mezzo.

La prima impostazione va infatti in parte rimeditata alla luce dell'ampiezza del diritto di difesa *ex* art. 24, co. 2 Cost., e in particolare del suo corollario, il principio *nemo tenetur se detegere*, la cui portata non può esser confinata alla sola dimensione dichiarativa (lo *ius tacendi* in senso stretto), ma deve includere anche il diritto di rifiutare una collaborazione attiva alla ricostruzione del fatto storico[69]. Se infatti il dettato codicistico richiama solo la mancata risposta alle domande dell'autorità inquirente (art. 64, co. 3, lett. b c.p.p.), la disciplina costituzionale – a mente della quale la difesa è "inviolabile in ogni stato e grado del procedimento" – permette invece di individuare un più vasto «diritto di "resistenza"»[70] che sorregge sia il contegno silenzioso, sia la facoltà di astenersi dal compiere quei movimenti corporei imposti dall'attività istruttoria (ad es., indossare vestiti o adottare una certa posa a fini ricognitivi, fornire al perito un campione vocale o un saggio grafico, ecc.)[71].

---

[66] MALACARNE, Social network *e giustizia penale. Nuovi scenari investigativi e probatori*, Tesi di dottorato, Università degli Studi di Genova, 2024, https://iris.unige.it/retrieve/d1775cdc-8644-4d1f-9856-eda125205dd4/phdunige_4969484.pdf.

[67] *Ibid.*

[68] A favore dell'irrilevanza fra le distinzioni tra tipi di chiavi sembra porsi anche MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., 740.

[69] CAMON, *La disciplina costituzionale*, in AA.VV. *Fondamenti di Procedura penale*, 4ª ed., Milano, 2023, 150. Nello stesso senso DEL MONACO, *L'accertamento dei reati di guida in stato di ebbrezza e alterazione da droghe*, Tesi di dottorato, Alma Mater Studiorum Università di Bologna, 2012, 61, https://amsdottorato.unibo.it/4510/1/del_monaco_roberta_tesi.pdf; più di recente, in tema di accertamenti medici coattivi, SPAGNOLO, *Gli accertamenti medici coattivi e le tecniche corporali intrusive*, in *Cass. pen.*, 2024, 1, 25.

[70] CAMON, *La disciplina costituzionale*, cit., 150.

[71] *Ibid.* Si vedano, per un simile approccio, anche BIRAL, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Riv. it. dir. proc. pen.*, 2015, 4, 1872-1873; FELICIONI, *Accertamenti sulla persona e processo penale*, Assago, 2007, 35; SCAPARONE, *Elementi di procedura penale. I principi costituzionali*, Milano, 1999, 123.

Per quanto qui interessa, quindi, se la garanzia contro l'autoincriminazione esclude l'esistenza di un dovere in capo al prevenuto di fornire prove a proprio carico, siano esse materiali o dichiarative, pare doveroso rileggere il concetto di collaborazione alla luce degli influssi che scienza e tecnica esercitano sull'accertamento penale, attesa la sempre maggiore capacità degli inquirenti di "interrogare" il corpo, prima ancora che l'intelletto[72]. In questi casi, infatti, la persona sottoposta ad indagini viene in rilievo quale «fonte di dati», prima ancora che di dichiarazioni[73].

In altre parole, ciò che consente di determinare il livello di protezione del *nemo tenetur* non dovrebbe esser tanto la natura della *password* (alfanumerica o biometrica), quanto piuttosto il tipo di condotta richiesta per mettere quest'ultima a disposizione degli inquirenti (attiva o passiva). Le chiavi d'accesso biometriche non dovrebbero quindi essere per ciò solo ricondotte allo schema dell'imputato quale "oggetto di prova", poiché ciò dipenderebbe essenzialmente dal contegno domandato. Qualora sia l'inserimento della *password* a richiedere un *facere*, il prevenuto diverrà soggetto di prova pure quando la chiave sia costituita da una parte del suo corpo o da un suo tratto fisionomico (es. campione vocale, compimento di specifici gesti)[74]; al contrario, la valorizzazione di tratti puramente esteriori, osservabili ad occhio nudo, non esigerà alcuna postura attiva all'imputato, che sarà chiamato solo ad un *pati* del tutto compatibile con il *nemo tenetur* (si pensi al caso della scansione facciale o della retina, o all'impiego della funzione *TouchID*)[75].

La seconda impostazione, a sua volta, intuisce in maniera condivisibile una comunanza di scopo fra le diverse possibili tipologie di accesso al dispositivo protetto. Tuttavia, gli argomenti suggeriti non paiono insuperabili. Se è vero che ragioni di giustizia sostanziale rendono eccentrica una distinzione fra livelli

---

[72] RODOTÀ, *Ipotesi sul corpo «giuridificato»*, in *Tecnologie e diritti*, Bologna, 1995, 204, secondo cui la dimensione corporea, elevata ad «oggetto giuridico nuovo», imporrebbe il riconoscimento al titolare di diritti volti a tutelarlo dalle intromissioni dell'autorità; GIALUZ, *Radiologia e accertamenti medici coattivi: il difficile equilibrio tra libertà della persona ed esigenze di prova*, in *Riv. it. dir. proc. pen.*, 2012, 2, 559 ss.

[73] GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, 57.

[74] Cfr., con riguardo a quest'ultima eventualità, il metodo di autenticazione basato sul movimento del braccio proposto per gli *smartwatches* da Zhao - Gao - Tu, *Smartwatch User Authentication Based on the Arm-Raising Gesture*, 32 *Interacting with Computers* 569, 2020, 569 ss.

[75] Quest'ultima matrice biometrica, a ben vedere, potrebbe astrattamente rientrare anche nella prima categoria, ove fossero gli inquirenti a richiedere al prevenuto di sbloccare il *device* tramite l'impronta digitale. La distinzione pare pressoché scolastica, nel senso che, in concreto, nessuna difficoltà avrà la p.g. ad applicare quella modica forza necessaria a porre il polpastrello dell'utente a contatto col *display*; tuttavia, sul piano dogmatico, è bene non tralasciare questa eventualità.

di tutela basata sul tipo di chiave di sicurezza impiegata (e magari configurata *by design* nel dispositivo), tale scelta potrebbe non essere del tutto irragionevole, atteso che la stessa situazione ha modo di verificarsi rispetto alle *passwords* alfanumeriche. Queste ultime, infatti, restano incoercibili finché esistono nella mente dell'imputato; una volta tradotte nel mondo esterno, possono invece essere oggetto di apprensione unilaterale da parte degli inquirenti come prove documentali (si pensi al codice di accesso che l'imputato lascia incautamente scritto nella propria agenda poi sequestrata). In un certo senso, dunque, il prevenuto che, per scelta o per negligenza, utilizza un dato biometrico come chiave di sblocco del proprio dispositivo, accetta che quest'ultima esista all'infuori di lui, e che possa perciò venir raccolta indipendentemente dalla sua volontà.
È chiaro poi che la natura *will-dependent* o meno di un certo elemento di prova, in questo caso la chiave, vada esaminata avendo riguardo alla richiesta di cooperazione, non già alla sua origine: a ragionar diversamente, pure ogni documento formato dall'imputato dovrebbe dirsi, per ciò solo, coperto dal diritto al silenzio.
Ancora una volta, dunque, l'attenzione si sposta sul comportamento richiesto all'imputato, più che sulla natura della chiave impiegata. In breve, le matrici biometriche dovrebbero poter vantare un livello di protezione uguale a quello delle *passwords* tradizionali ove gli inquirenti non possano ottenerle senza l'attiva cooperazione dell'imputato. In caso contrario, essendo richiesto un contegno puramente passivo, il *nemo tenetur* non dovrebbe poter operare.

6. Obblighi di decrittazione e di produzione. Occorre a questo punto chiedersi se fra i due estremi sopra considerati, ossia fra la richiesta di rivelare una *password* alfanumerica e l'obbligo di "sopportare" l'utilizzo di una chiave biometrica, non si possa scorgere una terza via, in cui la richiesta investigativa cada su qualcosa di diverso rispetto al codice di protezione: vale a dire, sull'accesso diretto al dispositivo o sulla consegna del suo contenuto[76].
In entrambi i casi infatti la *password*, sia essa alfanumerica o biometrica,

[76] Doveri di tal genere si stanno facendo strada in territori limitrofi al processo penale. È il caso dell'ispezione, prevista a fini identificativi, dei dispositivi o dei supporti elettronici o digitali in possesso dei migranti. L'art. 12 d.l. 11 ottobre 2024, n. 145, convertito con L. 9 dicembre 2024, n. 187, ha infatti previsto, sia per il richiedente asilo che per il migrante irregolare, così come per colui che richiede la protezione internazionale, un «obbligo di cooperare ai fini dell'accertamento dell'identità e di esibire o produrre gli elementi in suo possesso relativi all'età, all'identità e alla cittadinanza, nonché ai Paesi in cui ha soggiornato o è transitato [...]», che comprende, «quando è necessario per acquisire i predetti elementi, l'accesso ai dispositivi o supporti elettronici o digitali in suo possesso».

rimarrebbe impregiudicata e nella disponibilità esclusiva dell'utente; nondimeno, l'autorità penale riuscirebbe ad ottenere ciò che vuole mediante la cooperazione del prevenuto.
In altre parole, occorre domandarsi se siano compatibili con il *nemo tenetur* ordini di decrittazione o di produzione.
Gli ordinamenti che tendono a circoscrivere al diritto al silenzio il problema della collaborazione con l'autorità si mostrano, al riguardo, possibilisti. In tali ipotesi non verrebbe in effetti domandato alla persona sottoposta ad indagine di rivelare il contenuto della propria mente, non intaccandosi quindi il "nucleo duro" (dichiarativo) dello *ius tacendi*.
Si potrebbe perciò sostenere che la decrittazione di un dispositivo riesca a comunicare un unico fatto, cioè la conoscenza della *password*[77]. Per l'effetto, ulteriori inferenze, quali il controllo esercitato sul dispositivo o il possesso dei *files* in esso conservati, costituirebbero semplici deduzioni, in quanto tali prive di valore testimoniale[78].
Tale impostazione non è però pacifica, e viene contrastata rilevando come la conoscenza del codice non sarebbe l'unico fatto rivelato dall'apertura del dispositivo[79]. L'impiego di un codice comunicherebbe infatti anche che il *device* probabilmente appartiene alla persona a cui lo sblocco è stato richiesto, e che la medesima, consapevolmente o meno, possiede i *files* ivi conservati[80] – informazioni la cui pregnanza sarà suscettibile di esser apprezzata in concreto dal giudice.
Soprattutto, l'approccio nordamericano rischia di mostrarsi debole in quanto potenzialmente esposto allo stesso limite a cui la giurisprudenza d'oltreoceano assoggetta la protezione del Quinto Emendamento, ossia alla già citata *foregone conclusion doctrine*[81]. Se l'ottemperanza all'ordine conoscitivo poco o nulla aggiunge alle informazioni a disposizione dell'autorità procedente, si argomenta, il privilegio contro l'autoincriminazione non dovrebbe poter venire opposto, in quanto l'attività di ricerca della prova raggiungerebbe un esito, per

[77] KERR, *Compelled Decryption and the Privilege against Self-Incrimination*, 97 *Tex. L. Rev.* 767, 779 (2019).
[78] *Ivi*, 780.
[79] SACHAROFF, *What Am I Really Saying When I Open My Smartphone?: A Response to Professor Kerr*, 97 *Tex. L. Rev.* 63, 67 (2019).
[80] *Ibid.*
[81] Cfr, *supra* par. 3.

l'appunto, "scontato"[82].
Occorre perciò domandarsi se una simile eccezione sia ravvisabile nell'ordinamento domestico. Un inaspettato avallo potrebbe provenire dall'interpretazione offerta dalla Corte europea dei diritti dell'uomo nel recente caso *De Legé c. Paesi Bassi*[83], in cui i giudici strasburghesi hanno affermato che non viola il diritto all'equo processo, nel suo corollario del diritto a non autoincriminarsi, l'obbligo imposto all'interessato di fornire documenti a pena d'una sanzione tributaria – "punitiva" secondo i criteri *Engel* – «*where the authorities are able to show that the compulsion is aimed at obtaining specific pre-existing documents – thus, documents that have not been created as a result of the very compulsion for the purpose of the criminal proceedings – which documents are relevant for the investigation in question and of whose existence those authorities are aware*»[84].
È chiaro, dunque, il parallelismo con la citata teoria statunitense[85]: quando gli inquirenti sono in grado di indicare specificamente di quali prove reali sono alla ricerca, il diritto al silenzio non opera.
Si potrebbe perciò ammettere nel nostro ordinamento un'eccezione basata sulla regola *De Legé*, tale per cui l'indagato possa essere costretto, a certe condizioni, a consegnare dati contenuti nel suo dispositivo elettronico, ovvero a sbloccare il dispositivo?
Al riguardo si possono avanzare alcune perplessità.
Innanzi tutto, l'interpretazione formulata dai giudici alsaziani sembra lacunosa, in quanto non spiega perché il grado di conoscenza che l'autorità possiede riguardo una specifica prova dovrebbe rilevare nel determinare se l'imputato sia stato o meno illegittimamente costretto a contribuire alla propria condanna[86]. In particolare, non viene specificato quale sia lo *standard* di

---

[82] Naturalmente la richiesta dovrebbe venir diversamente articolata nel caso in cui venga domandata l'apertura del dispositivo e nel caso in cui venga chiesta la produzione di elementi in esso contenuti. Nella prima ipotesi, infatti, basterebbe dimostrare la conoscenza della *password* da parte del prevenuto; nella seconda, invece, occorrerebbe descrivere specificamente le prove cercate. Cfr. KERR, *Compelled Decryption and the Privilege against Self-Incrimination*, cit., 786-787.
[83] Corte EDU, 4 ottobre 2022, *De Legé c. Paesi Bassi*.
[84] *Ivi*, 76.
[85] Come osservato da ESCOBAR VEAS, De Legé v. the Netherlands*: The ECtHR adopts a line of reasoning similar to that of the United States Supreme Court on compelled production of real or physical evidence*, 30 *Maastricht Journal of European and Comparative Law* 653, 2023, 653 ss.
[86] *Ibid.*

giudizio che l'autorità dovrebbe rispettare per potersi dire effettivamente a conoscenza dell'esistenza delle prove reali[87], né quale sia la logica in grado di sorreggere quest'esegesi[88]. Al contrario, se è vero che il diritto all'autoincriminazione è legato alla presunzione d'innocenza, nel senso che l'accusa dovrebbe riuscire a dimostrare il suo caso senza ricorrere a evidenze ottenute mediante coercizione, come pacificamente affermato nella giurisprudenza della Corte di Strasburgo, allora non dovrebbe esservi spazio alcuno per la regola *De Legé*: in effetti, indipendentemente dal fatto che sia stata o meno consapevole della loro esistenza, ogni volta che l'autorità pubblica costringe l'imputato a produrre attivamente prove reali altro non fa che renderlo partecipe della costruzione dell'accusa nei propri confronti[89].

D'altronde, anche volendo ammettere la correttezza dell'interpretazione seguita dalla Corte europea, dubbi permarrebbero circa la sua effettiva applicabilità nell'ordinamento italiano. Le garanzie previste dalla C.E.D.U. sono infatti cautele minime, che non ostacolano l'introduzione di un maggior livello di tutela ad opera degli Stati parti: se il diritto a non collaborare è da considerare un corollario del diritto di difesa costituzionalmente riconosciuto all'imputato, allora il nostro sistema penale pare già ammettere, su questo punto, un livello di protezione superiore rispetto ai minimi *standard* convenzionali. Inoltre, la Consulta, pur confermando di non poter sindacare l'interpretazione offerta dalla Corte di Strasburgo, ha da tempo asserito che l'esegesi convenzionale diviene vincolante per il giudice comune, al fine di precisare e specificare il contenuto della norma pattizia, solo quando risulti indice d'un "diritto consolidato"[90].

Elementi idonei ad orientare il magistrato penale in questa valutazione sarebbero, per quanto qui interessa, «la creatività del principio affermato, rispetto al solco tradizionale della giurisprudenza europea» e «la circostanza

---

[87] *Ibid.*

[88] *Ibid.* L'Autore sottolinea in particolare come, a differenza del Quinto Emendamento della Costituzione degli Stati Uniti, che circoscrive la sua portata ad un diritto a non essere costretti a testimoniare contro sé stessi, l'art. 6 C.E.D.U. non prevede esplicitamente alcuna limitazione di tal genere, né la Corte europea si è mai espressa apertamente in favore di una simile opzione. Una teoria come la *foregone conclusion* assume perciò senz'altro significato ove la protezione offerta dal *nemo tenetur* coincida con il contenuto comunicativo dell'atto; ove si scinda questa endiadi, invece, tale teoria può apparire priva di una *ratio* giustificatrice.

[89] *Ibid.*

[90] Corte cost., 14 gennaio 2015, n. 45, punto 7 del Considerato in diritto.

che quanto deciso proman[i] da una sezione semplice, e non [abbia] ricevuto l'avallo della Grande camera»[91]. La sentenza *De Legé* parrebbe rispondere ad entrambi i criteri proposti, essendo stata pronunciata da una sezione semplice, la Quarta, e presentando profili innovativi: la situazione di "*fishing expedition*" infatti, nonostante qualche opinione favorevole in dottrina[92], mai era stata additata in via esplicita dalla Corte EDU quale presupposto necessario a legittimare la mancata consegna di prove reali da parte dell'accusato[93].
Relativizzata così la portata del precedente, ci si sente di concludere negativamente circa la applicabilità di una "eccezione di conoscenza" in ordine alla possibilità di avvalersi del *nemo tenetur* nel processo penale tradizionale[94].

7. Collaborazione "spontanea" e valutazione del "silenzio". Ad un diverso esito rispetto alle ricostruzioni offerte fin qui si deve giungere ove il prevenuto si determini spontaneamente a rivelare la *password* o ad immetterla lui stesso, trattandosi di una forma di abdicazione al diritto a non collaborare[95]. Il problema che qui si pone, piuttosto, è quello di verificare l'effettiva assenza di costrizioni o di pressioni indebite, visto l'incerto confine di un'effettiva spontaneità[96].
Il tema non è puramente teorico, dato che il ricorso a forme oblique di "*moral suasion*" ben può rappresentare un utile viatico per persuadere l'indagato a dismettere il proprio diritto senza che l'attività investigativa vada incontro ad alcuna formale sanzione[97]. Il comportamento collaborativo, se non può essere imposto dagli inquirenti, può infatti esser oggetto di una larvata "negoziazione"

---

91 *Ibid.*

92 In questo senso, ad esempio, STESSENS, *The obligation to produce documents versus the privilege against self-incrimination: human rights protection extended too far?*, 22 *European Law Review - Checklist no. 1* 45, 1997, 61, che tenta di riconciliare così i contrastanti precedenti *Funke* e *Saunders*.

93 Alcune decisioni, in cui le richieste dell'autorità pubblica erano state ritenute lesive del *nemo tenetur*, sembravano in effetti alludere ad un tale contesto di incertezza, senza però indicarlo testualmente come unico o principale criterio risolutivo. Cfr. es. *Funke c. Francia*, cit., 44; *J.B. c. Svizzera*, cit., 69.

94 Una soluzione diversa potrebbe valere per il procedimento amministrativo "punitivo", ossia "penale" nell'ottica della giurisprudenza di Strasburgo. Qui la facoltà di tacere si porrebbe come eccezione alla regola, altrimenti generale, di cooperazione con autorità amministrative indipendenti, comportando perciò un effettivo innalzamento di tutela.

95 MANGIARACINA, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, cit., 737.

96 *Ibid.*

97 RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, cit., 889.

volta, nell'ottica dell'imputato, a conseguire vantaggi (o ad evitare mali) e, nell'ottica dell'organo dell'indagine, a prevenire diseconomie processuali.
In primo luogo, l'interesse perseguito dal soggetto passivo dell'accertamento penale potrebbe essere quello di evitare il rischio di alterazione dei dati contenuti nel dispositivo – non escludibile a priori in caso di accesso *bruteforce* –, o, ancora, il desiderio di conseguire una pronta restituzione del bene oggetto di sequestro[98]. È facile perciò immaginare come i codici di accesso potrebbero venir rivelati, o lo sblocco del *device* venir eseguito, proprio al fine di favorire i predetti esiti.
Questo stato di cose sembra trovare una implicita conferma nella giurisprudenza di legittimità, la quale, pur riconducendo la mancata collaborazione dell'indagato nel rilascio dei codici di accesso all'esercizio di una facoltà difensiva – ossia, al "diritto al silenzio" –, ha già avuto modo di specificare che «si tratta [...] di comportamento che influisce sulla valutazione della legittimità della protrazione del vincolo, che trova giustificazione nella accresciuta difficoltà di accesso ai dati di interesse investigativo»[99]. In altre parole, se è vero che nell'ambito del sequestro probatorio di dispositivi informatici – prodromico ad identificare ed estrarre i dati rilevanti per le indagini – la finalizzazione dell'ablazione alla successiva analisi implica che la protrazione del vincolo (nel rispetto dei principi di proporzionalità e di adeguatezza) debba essere limitata al tempo necessario all'espletamento delle operazioni tecniche, la ragionevolezza della durata dovrà esser valutata in rapporto alle difficoltà tecniche di apprensione dei dati, le quali debbono ritenersi aumentate ove l'indagato non cooperi fornendo le chiavi di accesso alle banche dati contenute nei supporti sequestrati[100].
Non meno insidioso pare poi l'effetto che, *a latere* o prima del giudizio di cognizione, può avere l'inerzia dell'imputato nel rivelare le proprie *passwords*. Il procedimento cautelare rappresenta infatti uno snodo delicato per ciò che concerne la tutela del *nemo tenetur*, essendo facilmente impiegabile da parte del pubblico ministero per sollecitare la collaborazione materiale o la confessione del prevenuto, "scambiandole" con una domanda di revoca o di attenuazione della misura[101].
Proprio al fine di scongiurare tali pratiche, la legge esclude testualmente che

---

98 ZAMPINI, intervento alla conferenza *Dimensione giudiziaria e dimensione mediatica della presunzione d'innocenza*, cit.
99 Cass. pen., Sez. II, 23 marzo 2023, n. 17604, Rv. 284393 – 01. Più di recente, nello stesso senso, si veda Cass. pen., Sez. III, 4 luglio 2024, n. 36776, Rv. 286923 – 01.
100 *Ibid.*
101 Cfr. es. ILLUMINATI, *Carcere e custodia cautelare*, in *Cass. pen.*, 2012, 7-8, 2373.

il silenzio e la mancata ammissione degli addebiti possano rientrare nel novero delle situazioni da cui dedurre l'esistenza di un pericolo per l'acquisizione e la genuinità della prova (*ex* art. 274, co. 1, lett. a), c.p.p.)[102]. Eppure, in senso contrario si è in anni recenti pronunciata la Suprema corte, arrivando a desumere tale rischio di inquinamento proprio dal rifiuto dell'indagato di fornire le chiavi di accesso ai dispositivi informatici a lui sequestrati[103]. Il pericolo ravvisato è stato evidentemente quello di una cancellazione a distanza dei dati da parte del prevenuto non ristretto; seguendo quest'esegesi, un esito favorevole della vicenda cautelare ben potrebbe rappresentare il "premio" offerto a colui che rivela le *passwords* dei sistemi controllati. La soluzione appare tuttavia censurabile, perché il diritto a tacere, anche nella sua appendice elettronica, non dovrebbe costituire di per sé un elemento idoneo a giustificare la compressione della libertà individuale, pena l'elusione dello specifico divieto posto dal legislatore[104].

In quest'ottica, un approccio incoraggiante si rinviene in tema di riparazione per la ingiusta detenzione subita dall'imputato, ove si è escluso che la mancata indicazione alla polizia giudiziaria dei codici di accesso al cellulare possa risultare ostativa al rimedio (art. 314, co. 1 c.p.p., così come modificato dal d.lgs. n. 188 del 2021), stante la riconducibilità di tale comportamento, in senso lato, all'alveo del diritto al silenzio[105].

In ultimo, non può tacersi il rischio che il sindacato sul contegno non collaborativo possa penetrare anche sul piano decisionale. Come tradizionalmente sottolineato, il comportamento meramente passivo rappresenta di per sé un dato neutro sul piano probatorio[106]; tuttavia, scorrendo il diritto vivente ci si accorge che la possibilità di trarre inferenze negative o positive – rispettivamente dall'esercizio o dal mancato esercizio dello *ius tacendi* – fatica a scomparire.

---

[102] La scelta di limitare tale divieto ad uno solo dei *pericula libertatis* è stata peraltro oggetto di critiche in dottrina poiché, letta al contrario, tale clausola rischia di legittimare l'inferenza censurata in relazione alle altre esigenze cautelari. Cfr. es. GIOSTRA, *Per una migliore disciplina della custodia cautelare*, in *Dir. pen. proc.*, 1995, 3, 305.

[103] Cass. pen., Sez. II, 26 febbraio 2021, n. 7568, in *Diritto di internet*, 12 marzo 2021, con nota di PITTIRUTI, *Rifiuto di fornire i codici di sblocco della strumentazione informatica in sequestro e pericolo di inquinamento probatorio: addio al* nemo tenetur se detegere*?*.

[104] PITTIRUTI, *Rifiuto di fornire i codici di sblocco della strumentazione informatica in sequestro e pericolo di inquinamento probatorio: addio al* nemo tenetur se detegere*?*, cit., il quale sottolinea che tale pratica risulterebbe evidentemente propedeutica a fungere da pungolo per la collaborazione.

[105] Cass. pen., Sez. IV, 14 marzo 2023, n. 16118, in *DeJure*.

[106] Per tutti si veda CORDERO, *Procedura penale*, 9ª edizione, Milano, 2012, 255.

La mancata cooperazione, infatti, pur non potendo portare ad una inversione dell'onere della prova[107], viene talvolta valorizzata quale "argomento"[108] o "elemento" probatorio[109]: ciò, ad esempio, al fine di corroborare ulteriori evidenze[110], o per decidere tra la concessione o il diniego di circostanze attenuanti (specie generiche)[111], ovvero in sede di applicazione dei "doppi benefici" (sospensione condizionale della pena e non menzione della condanna nel certificato del casellario giudiziale)[112].

In dottrina, nonostante l'opinione contraria di buona parte degli studiosi, secondo cui consentire al giudice di trarre inferenze negative dal silenzio equivarrebbe a sanzionare l'esercizio di un diritto costituzionalmente tutelato[113], vi è chi assume una posizione più blanda, ammettendo quella indiretta valutazione "negativa" del silenzio nel momento in cui il giudice si trova ad escludere ipotesi alternative, attività necessaria per rispettare lo *standard* dell'"oltre ogni ragionevole dubbio"[114], ovvero distinguendo tale ipotesi dalla valutazione positiva della condotta di collaborazione – la quale, si afferma, non entrerebbe in attrito con il *nemo tenetur*[115].

Non constano precedenti specifici in materia per quanto riguarda il sindacato sul diritto al silenzio "digitale" ai fini della decisione di merito: non può tuttavia escludersi che simili ragionamenti possano venir riproposti, *mutatis mutandis*,

---

107 Cfr., *ex multis*, Cass. pen., Sez. III, 19 settembre 2019, n. 43254, in *DeJure*.

108 Cfr., *ex multis*, Cass. pen., Sez. II, 12 febbraio 2020, n. 16036, in *DeJure*.

109 Cfr., *ex multis*, Cass. pen., Sez. IV, 6 novembre 2019, n. 19216, Rv. 279246 – 02; in senso contrario Cass. pen., Sez. VI, 27 gennaio 2015, n. 8958, Rv. 262499 – 01.

110 Cass. pen., Sez. VI, 19 giugno 2019, n. 28008, Rv. 276381 – 01.

111 Cass. pen., Sez. un., 24 maggio 2012, n. 36258, Rv. 253152 – 01. In senso parzialmente contrario, si vedano invece Cass. pen., Sez. V, 24 settembre 2020, n. 32422, Rv. 279778 – 01; Cass. pen., Sez. VI, 17 ottobre 2013, n. 44630, Rv. 256963 – 01.

112 Cass. pen., Sez. VI, 16 febbraio 1984, n. 4933, Rv. 164489 – 01. La giurisprudenza di legittimità sembra però ormai tendere ad allinearsi alla protezione del *nemo tenetur* su questo punto. Cfr. Cass. pen., Sez. III, 25 novembre 2015, n. 4090, Rv. 265713 – 01, per quanto riguarda la sospensione condizionale, e Cass. pen., Sez. V, 14 settembre 2017, n. 57703, in *DeJure*, con riferimento alla non menzione della condanna.

113 In questo senso ad es. PATANÈ, *Il diritto al silenzio dell'imputato*, Torino, 2006, 214 ss.; STANZIONE, *Autoincriminazione e diritto al silenzio. Le esperienze italiana, francese e inglese*, Assago, 2017, 114; NOBILI, *Il principio del libero convincimento del giudice*, Milano, 1974, 346, 352.

114 CARBONI, *La valutazione probatoria del silenzio: critiche e prospettive*, in *Proc. pen. giust.*, 2018, 5, 922 ss.; SOTTANI, voce *Silenzio (diritto al)*, in *Dig. disc. pen.*, VII agg., Torino, 2013, 558-559.

115 BONZANO, *L'interrogatorio investigativo*, Padova, 2012, 31.

anche in tale nuovo ambito applicativo[116].
L'idea di valorizzare negativamente la mancata rivelazione della *password*, o il suo mancato inserimento, non sarebbe tuttavia appropriata, in quanto finirebbe per degradare la situazione giuridica soggettiva in parola da diritto ad onere.
Si potrebbe forse essere più "laici" per quanto riguarda la introduzione di un'ipotesi premiale. Questa potrebbe assumere la forma di una mitigazione della pena, da riconoscere nelle vesti di un'attenuante in caso di condanna dell'imputato che abbia effettivamente favorito l'accertamento del reato mediante lo sblocco del dispositivo sotto il suo controllo – sulla scorta di quanto già avviene in relazione ad altre fattispecie delinquenziali (es. 323-*bis*, co. 2 c.p.)[117]; oppure in via interpretativa, facendo rientrare un simile comportamento nell'ambito delle c.d. attenuanti generiche (art. 62-*bis* c.p.). Tale ipotesi si porrebbe peraltro in linea con quanto previsto dalla Direttiva 343/2016/UE, secondo cui, sebbene «l'esercizio da parte degli indagati e imputati del diritto al silenzio o del diritto di non autoincriminarsi non [possa] essere utilizzato contro di loro» (art. 7, co. 5), sarebbe comunque consentito tenere conto, in sentenza, del loro comportamento collaborativo (art. 7, co. 4).
In realtà, anche questa soluzione, per quanto non incostituzionale e non anti-comunitaria, non va esente da critiche, poiché finisce per dare luogo ad un'ulteriore ipotesi di quella «"soave inquisizione"»[118], da tempo lamentata dalla

---

116 In Cass. pen., Sez. I, 2 novembre 2023, n. 4853, in *DeJure*, il ricorrente ha avuto modo di lamentare, *inter alia*, la violazione di legge e il vizio di motivazione in ordine al trattamento sanzionatorio ricevuto, dal momento che i giudici d'appello avrebbero negato l'applicabilità delle circostanze attenuanti generiche in base al rifiuto di rivelare la *password* del proprio *smartphone* sottoposto a sequestro, valorizzandolo quale comportamento reticente. La Corte di legittimità non ha affrontato direttamente la questione, ritenendo piuttosto che la sentenza impugnata avesse argomentato la mancata concessione delle attenuanti *ex* art. 62-*bis* c.p. considerando sia la gravità delle condotte che l'intensità del dolo, essendo pacifico l'orientamento secondo cui, al fine di ritenere o escludere tali circostanze, il giudice potrebbe limitarsi a prendere in esame, tra gli elementi desumibili dall'art. 133 c. p., solo «quello che ritiene prevalente ed atto a determinare o meno il riconoscimento del beneficio, sicché anche un solo elemento attinente alla personalità del colpevole o all'entità del reato ed alle modalità di esecuzione di esso può risultare a tal fine sufficiente».

117 Art. 323-*bis*, co. 2 c.p.: «[p]er i delitti previsti dagli articoli 318, 319, 319 ter, 319 quater, 320, 321, 322, 322 bis e 346 bis, per chi si sia efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione degli altri responsabili ovvero per il sequestro delle somme o altre utilità trasferite, la pena è diminuita da un terzo a due terzi».

118 PADOVANI, *La soave inquisizione. Osservazioni e rilievi a proposito delle nuove ipotesi di "ravvedimento"*, in *Riv. it. dir. proc. pen.*, 1981, 2, 541.

dottrina penalistica, in cui la collaborazione processuale del prevenuto «risult[a] condizionata, in positivo, dalle blandizie del trattamento di favore, e, in negativo, dall'idea che il silenzio possa venire sanzionato da un'eventuale condanna senza "sconti"»[119].
Insomma, quando si tratta di diritti fondamentali, quale è il *nemo tenetur*, negare un premio assomiglia molto a prospettare una sanzione[120].

8. Cooperazione "fittizia" e attacchi a "forza bruta". Una lettura lineare del *nemo tenetur* dovrebbe quindi orientare la prassi delle indagini verso altre vie, che non implichino la cooperazione diretta o indiretta dell'accusato[121]. Minori perplessità desta in effetti, per ciò che concerne lo *ius tacendi*, un attacco condotto a forza bruta (*bruteforce*) nei confronti dell'apparecchio elettronico o realizzato inoculando captatori informatici (in funzione di *keylogger* o per la perquisizione del dispositivo bersaglio). Queste tecniche possono infatti venir eseguite d'autorità, senza coinvolgere l'individuo soggetto ad indagine penale.
Per vero, qualche dubbio potrebbe sorgere pure in questi frangenti. Si pensi alla "auto-installazione" del captatore informatico, ossia al *download* del *malware* inconsapevolmente ma proattivamente effettuato dall'indagato sul proprio dispositivo elettronico. La questione è stata in effetti posta proprio con riguardo alle captazioni ambientali eseguite tramite un "*trojan horse*": parte della dottrina ha avuto modo di osservare come la cooperazione artificiosa richiesta al destinatario dell'intercettazione, necessaria per permettere al captatore informatico di "infettare" il dispositivo bersaglio e di controllarne il funzionamento (ad esempio, attivando il microfono), paia confliggere con l'art. 188 c.p.p., il quale vieta, anche con il consenso dell'interessato, l'impiego di metodi o tecniche idonei ad influire sulla sua libertà di autodeterminazione – in ciò distinguendosi dalle intercettazioni ordinarie, in cui sono gli inquirenti a

---

119 *Ibid.*

120 Non a caso, tale obiezione è stata sollevata anche in riferimento alla menzionata disciplina eurounitaria (art. 7, co. 4 Direttiva 343/2016/UE), sottolineando come nel lungo termine una costante valutazione favorevole della rinuncia al silenzio possa finire per rappresentare una sanzione indirettamente rivolta a coloro che invece se ne avvalgono. Così CAIANIELLO, *Right To Remain Silent and Not to Incriminate Oneself in the European Union System*, 5 dicembre 2020), 15 del dattiloscritto, https://ssrn.com/abstract=3743329 o http://dx.doi.org/10.2139/ssrn.3743329; NEGRI, *Diritto al silenzio e verità estorte. Regressioni della storia, reticenze dell'Europa, ipocrisie domestiche*, in *Nulla è cambiato? Riflessioni sulla tortura*, a cura di Stortoni - Castronuovo, Bologna, 2019, 165.

121 ZAMPINI, intervento alla conferenza *Dimensione giudiziaria e dimensione mediatica della presunzione d'innocenza*, cit.

dover piazzare materialmente la "cimice"[122]. Per questa via, vi è quindi chi ha affermato che sollecitare in maniera occulta una cooperazione «potenzialmente *contra se*» condurrebbe ad una violazione del *nemo tenetur*, «da intendersi in senso ampio, non solo come diritto a non rendere dichiarazioni autoincriminanti, ma anche come diritto a non compiere azioni» di tal fatta[123].

Tale approccio va però incontro all'obiezione, difficilmente superabile, secondo cui la captazione così realizzata non implicherebbe alcuna «pressione sulla libertà fisica e morale della persona», non mirando il mezzo d'indagine «a manipolare o forzare un apporto dichiarativo» quanto piuttosto, «nei rigorosi limiti in cui sono consentite le intercettazioni», a captare «le comunicazioni tra terze persone, nella loro genuinità e spontaneità»[124]. Pur essendo un atto *contra se*, quindi, la mancanza di un contatto diretto con l'autorità procedente pone il *download* del *virus* al di fuori dello spettro applicativo del *nemo tenetur*, rendendo la collaborazione di certo inconsapevole, ma non coartata[125].

In ciò sta tutta la differenza rispetto alla richiesta della *password*, della produzione o della decrittazione, ove la domanda degli inquirenti attiva quel rapporto di immediatezza idoneo ad ingenerare una soggezione psicologica non compatibile con la libertà che deve essere invece lasciata alle scelte autodifensive.

Ad ogni modo, anche se appare corretto superare i dubbi circa il rispetto del

---

[122] CHELO, *Tutela della libertà morale e captatore informatico: è davvero tutto concesso a soddisfazione delle esigenze investigative?*, in *Dir. pen. proc.*, 2022, 7, 954 ss.; FILIPPI, *Il cavallo di troia e l'ispeperqui-intercettazione*, in *Penale. Diritto e procedura*, 2022, 1, 69.

[123] SIGNORATO, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, cit., 238.

[124] Cass. pen., Sez. V, 30 settembre 2020, n. 31604, con nota di APRATI, *Il* trojan horse *autoinstallato non rientra tra i metodi che ledono la libertà morale dell'indagato*, in *Foro it.*, 6 gennaio 2021.

[125] Si veda ad esempio la posizione scettica di MIRAGLIA, *Il "Trojan (non) di Stato": una disciplina da completare*, in *Proc. pen. giust.*, 2023, 5, 1232, la quale si domanda se la corrispondente attività svolta nel mondo fisico (nell'esempio «l'apertura della porta di casa ad un falso tecnico del gas che installi cimici tradizionali per eseguire intercettazioni») potrebbe mai andare incontro ad una simile qualificazione. Opinione analoga è espressa da CAMON, *Processo e libertà morale: tendenze recenti della giurisprudenza, della dottrina, della legislazione*, in *Proc. pen. giust.*, 2024, 4, 1029, secondo cui neanche chi assume la veste di indagato o di imputato potrebbe andare esente da incursioni nella propria sfera di autodeterminazione, non dovendo necessariamente «essere gradevoli e genuini» gli stimoli ricevuti nel corso del procedimento; a ragionar diversamente, infatti «nessuno potrebbe dirsi titolare d'una libertà morale piena».

La inoperatività del diritto al silenzio al di fuori di una sollecitazione da parte dell'autorità che procede viene peraltro affermata sin dalla storica Corte cost., 6 aprile 1973, n. 34, punto 3 del *Considerato in diritto*, con nota di GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1973, 2, 317 ss.

diritto al silenzio, l'accesso *bruteforce* presenta comunque alcune ineliminabili criticità: innanzi tutto il costo delle tecniche di *hacking* impiegate, non trascurabile ove occorra fare ricorso a competenze o sistemi che non siano nella immediata disponibilità dell'autorità giudiziaria[126]; la possibile dilatazione dei tempi investigativi richiesti al fine di bypassare le chiavi di accesso[127]; nonché, come detto, il rischio di compromissione dell'integrità dei dati conservati nel dispositivo[128].

9. Obbligo di rivelazione della password *e privilegio contro l'autoincriminazione.* Naturalmente, come osservato in dottrina, «il diritto a non collaborare spetta non solo alla persona indagata, ma anche a chi rischia, con il disvelare codici di accesso, di far emergere una sua responsabilità penale (art. 198, co. 2 c.p.p.)»[129].
Questa disciplina, in apparenza chiara, è però imperfetta, dal momento che il potenziale testimone, non attinto da sospetti di un reato pregresso, pare comunque tenuto a giustificare l'opposizione del privilegio: pertanto, egli non può limitarsi a tacere, ma deve indicare, sia pure in maniera sommaria, le ragioni che permettono di ritener ragionevole la sua scelta – insomma, come notato da attenta dottrina, al fine di invocare il *privilege against self-incrimination* il teste pare «costretto a... "incriminarsi un poco"»[130].
Tuttavia, il vero *punctum dolens* che qui interessa è un altro, ossia la natura essenzialmente "comunicativa" della garanzia, che inerisce a una deposizione e non già a una condotta. Tale stato di cose si riverbera sulla inutilizzabilità (relativa) che consegue al rilascio di affermazioni autoindizianti (art. 63, co. 1 c.p.p.), la quale difficilmente, visto il chiaro tenore letterale, potrebbe estendersi agli atti compiuti in seguito all'accesso al dispositivo, ancorché dotati di piena portata incriminante[131]. Inoltre, bisogna considerare che, nella maggior parte dei casi, sarà solo dopo aver esaminato quanto rinvenuto nell'apparecchio che potrà

---

126 ZAMPINI, intervento alla conferenza *Dimensione giudiziaria e dimensione mediatica della presunzione d'innocenza*, cit.
127 *Ibid.*
128 TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico*, in *Cybercrime*, a cura di Cadoppi et al., 2ª ed., Milano, 2023, 1516.
129 LUPÀRIA, Computer crimes *e procedimento penale*, cit., 388.
130 CAMON, *Le prove*, in AA.VV. *Fondamenti di Procedura penale*, cit., 362.
131 RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, cit., 891.

emergere una vera e propria *notitia criminis*, venendo quindi meno quella contestualità tra dichiarazioni e autoincriminazione richiesta dalla norma[132].
Riportando queste considerazioni al caso dei dispositivi elettronici, dunque, la tutela del terzo parrebbe invero piuttosto contenuta: egli potrebbe, invocando il privilegio, rifiutarsi di rivelare la chiave d'accesso; ma il divieto d'impiego processuale potrebbe al limite riguardare la dichiarazione forzosamente rilasciata (ossia il codice), non già gli elementi rinvenuti a seguito della successiva perquisizione del *device*.
Se la tutela dichiarativa pare limitata, ancora più compressa è l'autodifesa del terzo a cui venga imposta una cooperazione di carattere "materiale". Nonostante infatti tra le "persone idonee" (art. 348, co. 4 c.p.p.) e tra i "consulenti" (art. 359, co. 1 c.p.p.) tenuti a prestare la propria opera nel corso di indagini richiedenti specifiche competenze tecniche non possa certo ritenersi incluso il prevenuto[133], lo stesso non può dirsi per colui che non è interessato dal procedimento. La legge processuale non mostra preclusioni: nel caso degli ausiliari di p.g. è la specifica necessità di volta in volta rilevata il parametro che permette di selezionare il soggetto a cui attribuire la servitù di giustizia[134], il quale ben potrà essere così individuato nell'utente del dispositivo; lo stesso dicasi per i consulenti del pubblico ministero, che solo «di regola» dovranno essere iscritti agli albi peritali, mancando qualsivoglia sanzione in caso di scelta difforme (art. 73 disp. att. c.p.p.)[135]. Questi elementi lasciano intendere come una collaborazione non dichiarativa possa potenzialmente venir imposta al soggetto non indagato che utilizzi un dispositivo elettronico, o alla parte terza che abbia comunque conoscenza della modalità di accesso ai dati ricercati – cooperazione non rifiutabile[136], pena l'integrazione delle fattispecie di omissione di atti d'ufficio (art. 328 c.p.) o di rifiuto di uffici legalmente dovuti (art. 366 c.p.p.)[137].
In sostanza, la tutela del privilegio contro l'autoincriminazione sembra, *de iure condito*, piuttosto limitata[138]. Talune garanzie potrebbero però venir delineate

---

132 MALACARNE, Social network *e giustizia penale. Nuovi scenari investigativi e probatori*, cit., 238.
133 TORRE, *Sull'obbligo per il privato di collaborare ad attività di* digital forensics*: il caso "Apple – F.B.I."*, in *Cybercrime*, a cura di Cadoppi et al., 1ª ed., Milano, 2019, 1684.
134 *Ivi*, 1683.
135 *Ivi*, 1684.
136 *Ivi*, 1685.
137 *Ivi*, 1683-1684.
138 Tale conclusione pare confermata in via implicita dal potere dell'autorità giudiziaria di ordinare l'esibizione di atti, documenti, dati, informazioni e programmi informatici, anche tramite copia su

in un'ottica *de iure condendo*.
Innanzi tutto, per evitare che l'accesso al *device* nasconda un intento meramente esplorativo, ed al fine di contenere il pregiudizio per la riservatezza del terzo, si potrebbe riconoscere espressamente l'inutilizzabilità delle prove estranee al procedimento in cui l'accesso sia stato disposto[139]. Inoltre, l'obbligo collaborativo dovrebbe essere non solo legislativamente previsto, ma anche basarsi su un provvedimento motivato dell'autorità giudiziaria e risultare comunque rispettoso del principio di proporzionalità[140].
Se ci si limitasse a questo, però, nel caso della condotta collaborativa puramente materiale – rispetto alla quale, come si è detto, non sembra operare alcuna forma di legittima astensione – si rischierebbe comunque di lasciar scoperto il nucleo centrale del *privilege against self-incrimination*, vale a dire il rischio di far emergere una notizia di reato a proprio carico ottemperando all'ordine ricevuto. Perciò, sempre in una prospettiva de *iure condendo*, non sarebbe irragionevole aggiungere un'eccezione a quest'obbligo, analoga a quella già prevista sul piano dichiarativo: ossia la facoltà di opporre un rifiuto motivato ove le informazioni richieste possano far emergere una responsabilità di tipo penale.

10. Conclusioni. Il rapporto tra dispositivi elettronici e diritto al silenzio può a buon titolo dirsi controverso. La stretta integrazione che l'apparecchio

supporto idoneo (art. 256 c.p.p.): il soggetto destinatario è infatti qui obbligato a consegnare immediatamente quanto richiesto, salvo non dichiari per iscritto che la *res* cercata è coperta dal segreto professionale. Cfr. es. Cass. pen., Sez. II, 18 ottobre 2017, n. 51446, in *DeJure*.

139 RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, cit., 893 ss.

140 Quest'ultimo, in particolare, impone che il protocollo di ricerca venga formulato in modo chiaro e che l'accesso sia limitato a dati adeguatamente identificati dall'autorità richiedente e pertinenti ai fatti oggetto dell'indagine, in ossequio ai canoni di idoneità, adeguatezza e proporzione in senso stretto. Cfr. ORLANDI, *Postulati del processo penale contemporaneo tra principi "naturali" e concezioni normative*, in *Riv. it. dir. proc. pen.*, 2024, 2, 482 ss.
Si può discutere in ordine ai parametri su cui basare questo giudizio di proporzionalità. Secondo RICOTTA, *Obblighi di collaborazione con l'autorità giudiziaria nella decrittazione dei dispositivi informatici e privilegio contro l'autoincriminazione*, cit., 894, quanto più specifico sarà l'oggetto dell'investigazione, tanto più intenso dovrà essere il dovere cooperativo. Al contrario, per MALACARNE, Social network *e giustizia penale. Nuovi scenari investigativi e probatori*, cit., 237-238, l'intensità del dovere di collaborazione dovrebbe dipendere dalla gravità dei reati oggetto d'indagine e dal tipo di dati richiesti, dimodoché l'obbligo di *disclosure* potrebbe tradursi alternativamente nella rivelazione della *password* o di altre chiavi di sicurezza, oppure, ove ciò risultasse sproporzionato, nella ostensione delle prove reali domandate dagli inquirenti.

stabilisce fra individuo e sua dimensione virtuale – icasticamente rappresentata dal sempre più frequente impiego del corpo stesso (dati biometrici) in funzione di *password* – attiva un'aspettativa di difesa e di riservatezza che, in assenza di una disciplina apposita, non può che venir soddisfatta ricorrendo ai principi generali.

La distinzione tra condotta attiva e passiva quale chiave di lettura del *nemo tenetur*, la impossibilità di punire il contegno non collaborativo del prevenuto e gli obblighi di cooperazione imponibili a testimoni e terze parti rappresentano le linee guida che ci si sente di avanzare.

D'altronde, non molto dissimili paiono le soluzioni a tal fine escogitate da altri ordinamenti. Piuttosto pacifica e trasversale sembra essere la distinzione tra tipologie di chiavi di sicurezza, con il codice alfanumerico posto al centro del nucleo dichiarativo del diritto al silenzio e la matrice biometrica invece potenzialmente esposta a coercizione, in quanto indipendente dalla volontà dell'utilizzatore. Tuttavia non mancano spinte e controspinte, volte da un lato a escludere dalla protezione anche le *passwords* tradizionali (es. Belgio, Francia), dall'altro a recuperare qualche margine di tutela al dato biometrico, mediante la valorizzazione della natura "comunicativa" dell'atto di sblocco (es. USA).

Se i ragionamenti fin qui illustrati sono corretti, l'ordinamento italiano pare inserirsi nel novero dei sistemi più garantisti, grazie alla natura non strettamente dichiarativa del principio *nemo tenetur se detegere*. Certo, tutte le conclusioni rassegnate vanno comunque prese con beneficio d'inventario, nella consapevolezza che, di pari passo con gli apparecchi in parola, l'evoluzione tecnologica e la sua crescente capacità di perscrutare l'individuo rischiano di porre anche le cautele processuali, pensate per il "mondo fisico", a rischio di obsolescenza[141].

[141] Si veda ad esempio, a favore del riconoscimento di un'ampia e inedita "libertà di pensiero" in grado di includere anche la facoltà di non autoincriminarsi, FARAHANY, *Difendere il nostro cervello: la libertà di pensiero nell'era delle neurotecnologie* (trad. it. Francesca Pè), Torino, 2024, specie p. 90.