LUISS

Dipartimento
di Giurisprudenza

Dottorato in Diritto e Impresa

Ciclo XXXV

L'investigazione da remoto su dispositivi digitali

Prof. Antonino Gullo

RELATORE

Giulia Cascone

CANDIDATO

Anno Accademico 2021/2022

INDICE

Introduzione.

Il ricorso a mezzi di ricerca della prova che consentono l'acquisizione occulta e da remoto di dati digitali è sempre più agevole dal punto di vista operativo e, per tale ragione, le investigazioni *online* stanno conoscendo una rapida espansione nell'esperienza giudiziaria. Nondimeno, risulta assai difficile fare il punto su quali siano lo stato dell'arte e i possibili sviluppi normativi in questo ambito.

Sotto un profilo squisitamente tecnico, lo strumento adoperato è comunemente conosciuto come "captatore informatico" o "*trojan virus*" e consente agli investigatori di assumere il controllo da remoto di un determinato dispositivo informatico, spesso con l'inconsapevole collaborazione del suo utilizzatore. In conseguenza di ciò, nel procedimento penale possono riversarsi ingentissime quantità di dati della più disparata natura, portando alla luce anche i più reconditi anfratti dell'esistenza di quest'ultimo.

Le potenzialità operative del captatore – una sorta di sistema di spionaggio itinerante e da remoto – e la tendenza dei dispositivi informatici di uso comune a contenere dati e informazioni attinenti agli aspetti più intimi della nostra quotidianità si combinano in un *mix* dirompente e inedito, suscettibile di mettere a repentaglio le più elementari esigenze di riservatezza degli individui.

Comporre questi due contrapposti interessi in un bilanciamento adeguato è un'operazione tutt'altro che banale, come forse testimonia il ritardo del legislatore nell'adottare una disciplina normativa sistematica in materia. Tale ritardo pare difficilmente spiegabile nei termini di una mera inerzia: l'occasione di regolare l'uso investigativo dei cd. *trojan virus* in maniera sistematica vi è stata quando il legislatore si è cimentato nella riforma della disciplina delle intercettazioni di cui al d. lgs. n. 216 del 2017. Si è preferito, invece, limitare l'intervento normativo alla sola regolamentazione dell'impiego del captatore informatico per la realizzazione delle intercettazioni, lasciando così avvolti dal silenzio tutti i suoi ulteriori possibili usi.

La mancanza di una regolamentazione espressa, tuttavia, non sta impedendo ai diversi uffici delle Procure della Repubblica disseminate sul territorio nazionale di avvalersene nel corso delle indagini, mentre ampi settori della giurisprudenza di legittimità stanno opinabilmente avallando tale prassi investigativa, probabilmente a causa di una comprensione solo superficiale delle molteplici implicazioni critiche dell'uso dello strumento in questione.

Tale stato di cose sembra l'inevitabile punto di convergenza, da un lato, di alcune strutturali ambiguità del nostro ordinamento processuale penale in tema di prova atipica incidente sui diritti fondamentali; dall'altro, di una riflessione ancora troppo superficiale sull'individuazione delle prerogative costituzionali incise per il tramite del ricorso a simili mezzi di ricerca della prova.

Ulteriore fattore di complicazione dal punto di vista dogmatico-ricostruttivo è dato dalla difficoltà di replicare nel mondo virtuale soluzioni esegetiche e categorie giuridiche proprie del mondo fisico, in ragione di alcune insuperabili differenze che contrassegnano quest'ultimo rispetto allo spazio digitale. Tali strutturali divergenze determinano mutamenti qualitativi di fenomeni e interazioni che pur costituendo, all'apparenza, meri succedanei virtuali della realtà fisica, acquisiscono, invece, nuove fisionomie per il solo fatto di svolgersi in un ambiente smaterializzato. Ciò impone il ricorso a soluzioni e approcci regolatori differenziati rispetto a quelli elaborati in relazione agli atti d'indagine tradizionali, anch'essi molto intrusivi, ma altresì tangibili e immediatamente percepibili da chi li subisce

Prendendo le mosse da tali preliminari aspetti, il presente lavoro analizza la questione relativa all'uso di tali strumenti investigativi nella duplice prospettiva *de iure condito* e *de iure condendo*.

Sotto il primo punto di vista, viene delineato il trattamento processuale da riservare, dato l'attuale assetto normativo, ai risultati conoscitivi acquisiti all'esito dell'intrusione occulta e da remoto nel dispositivo informatico bersaglio dell'attività di indagine. In tale ricostruzione si è privilegiato un approccio costituzionalmente orientato, fondato sulla preliminare individuazione dei diritti fondamentali incisi dal ricorso a tali tecnologie della prova. Le conclusioni raggiunte in ordine alla necessità di riconoscere l'esistenza di un diritto costituzionale inedito alla riservatezza e all'autodeterminazione nell'uso delle tecnologie informatiche hanno implicato l'analisi di tematiche tradizionalmente appannaggio della dottrina costituzionalistica, come quella relativa alle matrici costituzionali di diritti fondamentali "nuovi". Stante l'apparente silenzio della Carta fondamentale, tale analisi è apparsa imprescindibile al fine di delineare lo statuto di garanzie minime del diritto in questione e ricostruire il trattamento processuale degli atti incidenti sullo stesso eventualmente adottati nel corso del procedimento penale. Essa,

inoltre, ha rappresentato il punto di partenza del successivo tentativo di un approccio *de iure condendo* alla materia.

Senza alcuna pretesa di completezza, si è tentato, nella seconda parte del presente lavoro, di immaginare le direttrici di un intervento legislativo teso a regolare in maniera sistematica le attività di ricerca della prova realizzabili per il tramite dello strumento in questione. Sulla base dei principi di legalità processuale e di proporzionalità, si è delineato il contenuto minimo di un reticolo di garanzie antecedenti, contestuali e successive allo svolgimento dell'atto investigativo, senza perdere di vista le indicazioni derivanti dalle Corti europee.

L'ultimo capitolo è dedicato allo studio delle misure di investigazione tecnologica introdotte dal legislatore spagnolo con la Ley Organica n. 13/2015 del 5 ottobre 2015, tra le quali si rinviene il cosiddetto *registro remoto*, consistente nell'ingresso occulto e da remoto in un dispositivo informatico, generalmente realizzato per il tramite di un *trojan virus*. L'analisi comparatistica ha offerto spunti interessanti: le criticità e i dubbi interpretativi rilevati in quell'ordinamento con riguardo all'istituto hanno condotto ad alcune ulteriori riflessioni sull'effettiva opportunità di introdurre un simile strumento nel nostro ordinamento, rafforzando le conclusioni già raggiunte in punto di necessaria eccezionalità del ricorso alla sorveglianza occulta dei cittadini ad opera dello Stato, quand'anche sia giustificata dall'esigenza, pur costituzionalmente rilevante, di accertamento dei reati.

Capitolo I

LEGGE E TECNOLOGIA:
LE INVESTIGAZIONI *ONLINE* E IL PROBLEMA DELLA RELATIVA REGOLAMENTAZIONE

Sommario: 1. Diritto e tecnologia: eccezionalismo *vs* non eccezionalismo; 1.1. Importanza (ma insufficienza) del ragionamento analogico; 1.2. Spazio reale e spazio virtuale; 2. L'attività d'indagine *online*: *online search* e *online surveillance*; 2.1. Lo strumento tecnologico: il *trojan virus* e le sue applicazioni; 2.2. Lo strumento normativo: assenza di una regolamentazione *ad hoc*; 3. Diritti costituzionali e investigazioni *online*: l'importanza della definizione della base costituzionale; 3.1. L'individuazione dei diritti costituzionali coinvolti (libertà morale, libertà e segretezza delle comunicazioni, inviolabilità del domicilio, libertà di circolazione, riservatezza); 3.2. "Vecchi" e "nuovi" diritti: il dibattito sull'enucleazione dei nuovi diritti fondamentali; 3.3. Realtà virtuale e "nuovi" diritti costituzionali. La lettura evolutiva del domicilio informatico e il diritto alla riservatezza e all'autodeterminazione nell'uso delle tecnologie informatiche.

1. Diritto e tecnologia: eccezionalismo *vs* non eccezionalismo.

L'assenza di un assetto regolatorio sistematico in materia di investigazioni *online* pone l'interprete dinanzi a due fondamentali questioni: la prima, in una prospettiva *de iure condito*, riguarda la riconducibilità di mezzi di ricerca della prova emergenti dalle nuove tecnologie a categorie giuridiche già esistenti, in modo da rendere esperibili determinati strumenti di indagine e spendibili i loro risultati nel procedimento penale. La seconda, in una prospettiva *de iure condendo*, concerne l'approccio regolatorio da seguire al fine di dare alla materia una sistemazione normativa adeguata, che consenta di bilanciare tutti gli interessi in campo secondo criteri di ragionevolezza e proporzionalità.

La soluzione a entrambe le questioni non può prescindere da una preliminare analisi da svolgersi su un piano generale in ordine al rapporto tra diritto e tecnologia informatica ed agli eventuali elementi di "eccezionalità" di tale relazione rispetto a quelle già esplorate fra l'esperienza giuridica e gli altri campi del sapere scientifico. Ciò si rende necessario in quanto le peculiarità dell'evoluzione tecnologica in atto sono tali da farla

interagire con la legge in modi nuovi e inaspettati[1]. Di conseguenza, al fine di analizzare il fenomeno tecnologico in entrambe le prospettive, *de lege lata* e *de lege ferenda*, appare imprescindibile interrogarsi sulla necessità o meno di ricorrere a nuove istituzioni o a nuove categorie giuridiche, apparendo alcune di quelle tradizionali obsolete e, comunque, inadeguate[2].

Peraltro, non è apparsa del tutto scontata agli studiosi della materia l'effettiva capacità della legge di regolare il fenomeno tecnologico. Tale questione si agita al centro del dibattito su quello che viene comunemente definito l'"eccezionalismo" della rete, alla cui base sta l'idea che le persone, i luoghi, gli oggetti o i concetti, trasposti o rappresentati sulla rete, siano qualitativamente differenti dai loro corrispondenti nel mondo fisico[3].

Quanti sostengono l'"eccezionalismo" della rete ne individuano la scaturigine, anzitutto, nell'assenza di confini geografici del sistema, che avrebbe dirompenti conseguenze, oltre che sull'effettività del potere e sulla legittimazione dei governi locali nell'imporre una regolamentazione tesa a controllare i comportamenti tenuti dai vari agenti che interagiscono al suo interno, anche sugli effetti delle azioni realizzate *online* dagli individui e sulla percezione, non immediata, delle regole applicabili[4]. In altre parole, secondo tale visuale, la rete costituirebbe un luogo distinto dal reale, sottoposto a una sovranità sua propria e sostanzialmente autoregolato da norme che tengono conto delle sue caratteristiche particolari: una sorta di regno autonomo che nessun sistema legale sarebbe in grado di governare.

Un approccio, quello appena delineato, che nel prospettare quale unica via percorribile quella dell'aprioristica rinuncia a qualsivoglia tentativo di normazione dei fenomeni che si verificano sulla rete appare, oltre che del tutto inadeguato a fronteggiare le crescenti esigenze di regolamentazione del sistema, anche fondato sull'opinabile conclusione che la società reale e quella virtuale siano completamente indipendenti tra loro, sicché la prima muterebbe indipendentemente dalla seconda.

---

[1] CALO, *Robotics and the Lessons of Cyberlaw*, in *California Law Review*, 2015, vol. 103, n. 3, 532.

[2] DI PAOLO, *Judicial investigations and gathering of evidence in a digital online context*, in *Revue internationale de droit pénal*, 2009/1-2, vol. 80, 202.

[3] CALO, *Robotics and the Lessons of Cyberlaw*, cit., 550.

[4] JOHNSON E POST, *Law and borders – The rise of law in cyberspace*, in *Stanford Law Review*, 1996, 1367 ss.

Al contrario, è stato argutamente osservato come la tecnologia non possa che evolvere all'interno del contesto sociale e culturale di riferimento, con la conseguente necessaria integrazione di elementi culturali, istituzionali e strutturali di quel medesimo contesto[5]. Sicché, se è possibile comprendere e regolare il contesto di riferimento nel quale il fenomeno tecnologico si inserisce, ne deriva che anche quest'ultimo sia parimenti analizzabile e regolabile per il tramite di un'operazione che, partendo dai principi generali del sistema[6], tenga conto delle peculiarità del medesimo[7]. Questo differente approccio, pur negando l'eccezionalismo *tout court* della rete e criticando l'aprioristica rinuncia a qualsivoglia tentativo di normazione dei fenomeni che ivi si verificano, ha il merito di portare alla luce alcune ambiguità già esistenti, ma poco visibili, nella legge deputata alla regolamentazione del corrispondente fenomeno nel mondo fisico[8].

---

[5] MEG LETA JONES, *Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw*, in *Journal of Law, Technology & Policy*, Georgetown University, 2018, 250 ss.

[6] EASTERBROOK, *Cyberspace and the Law of the Horse*, in *Chicago Unbound*, 1996, 207.

[7] Si veda TIM WU, *Is Internet Exceptionalism Dead?, The next digital decade: essays on the future of the internet*, Berin Szoka & Adam Marcus, eds., Techfreedom, 2010 (2011), 184, su https://scholarship.law.columbia.edu/faculty_scholarship/1676, il quale si oppone all'idea della non regolabilità del sistema dall'esterno, sostenuta da Johnson e Post, ma riconosce che internet ha caratteristiche particolari, tra cui, ad esempio, quella di essere una "Republic of Users".

[8] Un esempio paradigmatico di ciò può ravvisarsi nel contrasto interpretativo riguardante la sussistenza dell'interesse a impugnare il decreto di sequestro di dati informatici a seguito dell'effettuazione, ai sensi dell'articolo 258 c.p.p., di copia dei dati acquisiti con conseguente restituzione degli originali. La soluzione all'annosa questione è dovuta passare per la trattazione di complesse problematiche interpretative, attinenti, anzitutto, alla definizione dei confini dell'interesse a impugnare il decreto di sequestro probatorio e, in secondo luogo, di cosa debba intendersi per sequestro informatico. Sotto il primo profilo, si è trattato di capire se l'interesse a impugnare il decreto di sequestro probatorio fosse riconducibile esclusivamente alla reintegrazione dei pieni diritti proprietari sul bene sottoposto a vincolo ovvero se l'impugnazione potesse mirare ad altri fini (come, ad esempio, quello di impedire che quanto illegittimamente reperito tramite la misura ablativa confluisca nella piattaforma probatoria a disposizione del giudice della cognizione), non intaccati dalla previa restituzione del bene. Sotto il secondo profilo, invece, occorreva comprendere se e a quali condizioni la realizzazione di copie del materiale informatico sottoposto a sequestro potesse atteggiarsi alla stregua di un vero e proprio provvedimento di sequestro, in quanto tale suscettibile di riesame (per una ricostruzione più approfondita, vedi cap. 3, par. 1.1). È evidente come le problematiche sopra delineate non siano il precipitato di caratteristiche proprie dei dati informatici, ben potendo le stesse riguardare qualsiasi tipo di bene sottoposto a vincolo di indisponibilità. Nondimeno, c'è una specifica ragione se tali questioni, pur astrattamente riguardanti qualunque tipologia di sequestro, sono state compiutamente affrontate per ben due volte dalle Sezioni unite proprio in tema di sequestro informatico (cfr. Sez. un., 24 aprile 2008, n. 18253, Tchmil, in *Cass. pen.*, 2008, 4031, con osservazioni di Aprile; Sez. un., 20 luglio 2017, n. 40963, Andreucci, in *Cass. pen.*, 2018, 1, 131, con nota di RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio del materiale informatico*, e tale ragione è da rinvenirsi nel fatto che lo stesso presenta alcune marcate peculiarità rispetto al suo corrispondente fisico, da ravvisarsi, anzitutto, nell'intensità della compressione dei diritti incisi dalla misura che è sistematicamente più elevata di quella che contrassegna un sequestro tradizionale. Per una esaustiva ricostruzione delle complesse problematiche interpretative sottese alla materia si veda, per tutti, CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. e proc.*, 2009, 4, 469.

Per dirla altrimenti, quest'ultima prospettiva, invece che ritenere separati il mondo reale e quello virtuale, coglie l'intimo *continuum* che c'è nelle problematiche giuridiche concernenti i due ambiti, evidenziando come queste ultime si manifestino, però, secondo una differente intensità nell'uno e nell'altro contesto, posto che nel mondo reale talune tensioni risultano "attenuate" rispetto alle più dirompenti manifestazioni che le caratterizzano nel mondo virtuale. Da questo angolo visuale, quindi, può dirsi che studiare e regolare il mondo virtuale consente di risolvere tensioni di cui generalmente non si era riconosciuta l'esistenza. Alla stregua di questo approccio, l'unico fattore di eccezionalità di *internet* è ravvisabile, semmai, nel fatto che esso richieda talvolta «cambiamenti sistematici nella legge o nelle istituzioni legali al fine di riprodurre o modificare i bilanciamenti di valori esistenti»[9].

Ciò, ovviamente, significa che le categorie giuridiche tradizionali potrebbero essere inadeguate all'inquadramento dei vari aspetti di un fenomeno che, come detto, presenta indubbie peculiarità, tanto da rendere, talora, del tutto inappropriato il ricorso al ragionamento analogico e da richiedere uno sforzo critico di gran lunga maggiore, nel tentativo di fornire una classificazione di strumenti tecnologici solo apparentemente assimilabili a dei corrispondenti nel mondo fisico.

1.1. Importanza (ma insufficienza) del ragionamento analogico.

Se e in che misura una determinata attività svolta nel mondo digitale sia inquadrabile in una categoria già definita e regolata nel mondo fisico è la domanda che lo studioso, ivi incluso quello del diritto, deve porsi dinanzi a nuove tecnologie suscettibili di introdurre in qualsivoglia sistema giuridico concetti inediti, che «si collocano lungo i confini semantici degli istituti "tradizionali" e ne forzano il senso»[10]. È evidente, infatti, che comprendere se un certo fenomeno o strumento tecnologico si ponga al di fuori dell'ideale confine che delimita, sul piano concettuale, una categoria già esistente e regolata nel mondo fisico è operazione preliminare rispetto all'individuazione dello specifico trattamento che, sul piano regolatorio, va riservato a quel fenomeno o strumento. In altri termini, non è detto che le tradizionali categorie, anche giuridiche, che regolano e sistematizzano il mondo fisico non siano applicabili a quello virtuale. In

[9] CALO, *Robotics and the Lessons of Cyberlaw*, cit., 552.
[10] CESARI, *Editorial: The Impact of New Technologies on Criminal Justice: An Horizon with Unknown Implications*, in *Rev. bras. dir. proc. pen*., vol. 5, n. 3, 2019, 1180.

alcuni casi, tuttavia, il ragionamento analogico può condurre a vere e proprie disfunzioni sistematiche, stravolgendo il senso proprio e i meccanismi, per così dire, fisiologici di alcuni istituti. Ciò, come si è detto, è diretta conseguenza di alcune specifiche peculiarità delle nuove tecnologie virtuali che vanno necessariamente tenute presenti nel condurre lo sforzo analitico che lo studio delle interazioni tra la legge e le nuove tecnologie informatiche richiede all'interprete[11]. Proprio nella ideale mappatura delle principali similarità e differenze concettuali e funzionali tra il mondo fisico e quello virtuale risiede la chiave per comprendere se un determinato strumento o un certo istituto si atteggino nel primo differentemente da quanto accade nel secondo.

1.2. Spazio reale e spazio virtuale.

Come è stato acutamente osservato, la capacità e l'attitudine regolatoria della legge nel disciplinare un certo fenomeno dipende da una serie di variabili, tra le quali va annoverata, anzitutto, l'architettura medesima del sistema[12]. Vale a dire, cioè, che le stesse caratteristiche strutturali del sistema possono determinare una maggiore o minore efficienza regolatoria di una certa disciplina.

Se così stanno le cose, non v'è dubbio che proprio il carattere virtuale di alcune nuove tecnologie, tra le quali le *online technologies*, rappresenti un fondamentale elemento di valutazione dell'efficienza regolatoria di una norma che disciplina un istituto o uno strumento proprio del mondo fisico nel mondo virtuale.

Proprio la sua peculiare struttura virtuale, infatti, assicura alla rete una serie di caratteristiche che non si riscontrano – o, quantomeno, non in maniera sistematica – nel mondo fisico. Il riferimento è, anzitutto, all'attitudine della rete a esprimersi attraverso un continuo flusso di dati, che consente di mettere in connessione spazi e oggetti virtuali in maniera tendenzialmente illimitata. Tanto anche grazie al costo relativamente basso della conservazione delle informazioni, che se trova alcune invalicabili barriere proprio nella struttura del mondo fisico e nella naturale limitatezza dei suoi spazi, non incontra

[11] Sul punto, si vedano le compiute riflessioni di FLOR, *Le indagini ad alto contenuto tecnologico fra esigenze di accertamento e repressione dei reati e tutela penale di tradizionali e nuovi beni giuridici nell'era digitale*, in Flor e Marcolini, *La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Giappichelli, 2022, 139 ss.

[12] LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, vol. 113, n. 2, 1999, 504.

invece limiti di sorta nel mondo virtuale, suscettibile di contenere in minuscoli spazi quantitativi elevatissimi di informazioni.

Altra strutturale caratteristica delle nuove tecnologie, soprattutto di quelle fondate sull'uso della rete, è la loro polifunzionalità: gli strumenti tecnologici di ultima generazione di uso comune sono ideati e realizzati per svolgere non una singola, precisa attività, ma un numero più o meno variabile di funzioni[13]. Basti pensare agli *smartphone* che, senza alcuna pretesa di esaustività, consentono, oltre che di comunicare, vocalmente e per iscritto, in maniera pressoché istantanea, di avere accesso a contenuti multimediali, di controllare altri dispositivi mobili con loro connessi, di tracciare costantemente gli spostamenti dell'utilizzatore del sistema, di accedere alle piattaforme di compravendita più disparate.

La polifunzionalità di tali tecnologie, per come appena descritta, ha indubbie ripercussioni sulla natura e sulla quantità dei beni giuridici che possono essere lesi per il tramite della violazione della riservatezza dei sistemi informatici in questione. Vale a dire, cioè, che mentre fino a qualche anno fa la lesione dell'aspettativa di riservatezza dell'utilizzatore di un telefono fisso o mobile di vecchia generazione si realizzava per lo più tramite la predisposizione di un'attività di intercettazione che, di per sé, incideva esclusivamente o comunque in via principale sulla libertà e segretezza delle comunicazioni, oggi l'acquisizione del controllo su un dispositivo mobile di ultima generazione consente, anche contemporaneamente, la lesione di più beni giuridici[14], in dipendenza del fatto che siamo sempre più abituati ad espletare attraverso l'uso di tali tecnologie i più disparati bisogni individuali e relazionali[15].

---

[13] SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, 5. Nello stesso senso, BETZU, *Regolare internet. Le libertà di informazione e di comunicazione nell'era digitale,* Giappichelli, 2012, 115.

[14] Già su un piano prettamente intuitivo, può facilmente comprendersi come assuma un certo rilievo l'intera gamma dei diritti di libertà tutelati dagli artt. 13 ss. Cost. Come si vedrà in seguito, proprio l'individuazione dei beni giuridici incisi dai mezzi di ricerca della prova *online* rappresenta una delle più complesse problematiche della materia. Si veda, sul punto, anche CESARI, *Editorial: The Impact of New Technologies on Criminal Justice*, cit., 1178, che evidenzia come i nuovi mezzi tecnologici comportino tipologie di aggressioni a beni giuridici che poco hanno a che vedere con le tradizionali, perché spesso immateriali e non avvertibili.

[15] Non è lontano dalla realtà quanto acutamente osservato da CALO, *Robotics and the Lessons of Cyberlaw*, cit., 521, in merito al fatto che, più che limitarsi a mettere in connessione contesti diversi, le tecnologie della rete creano un autonomo senso dello spazio nel quale «*we found ourselves commonly mediated*». Caratteristica, questa, che, come si vedrà, chiama direttamente in causa la crescente esigenza di tutela della personalità di ciascuno di noi, che, oltre ad esplicarsi nelle modalità tradizionali, oggigiorno si esprime senz'altro anche attraverso l'uso delle tecnologie.

Su questo quadro, poi, incide ulteriormente la sostanziale promiscuità dei dati digitali[16] racchiusi negli spazi virtuali, che, per quanto concerne il piano oggetto di interesse in questa sede, ha quale considerevole conseguenza che nella ricerca di elementi utili per l'accertamento del reato ci si imbatta inevitabilmente in elementi conoscitivi attinenti alla vita privata degli individui del tutto irrilevanti rispetto all'accertamento stesso, ma che finiscono per essere travolti dall'attività di investigazione. Ciò, peraltro, accade molto spesso senza lasciare alcun segno visibile: l'intangibilità del mondo virtuale comporta, al tempo stesso, la sua semplice e tendenzialmente immediata modificabilità e la scarsa tracciabilità della modifica stessa. Sicché, mentre l'intervento umano nel mondo fisico si accompagna, essendone controbilanciato, alle possibilità di controllo derivanti dalla sua immediata percepibilità, un intervento nel mondo virtuale è molto più difficile da percepire e, conseguentemente, da sottoporre a controllo.

Proprio in ciò va ravvisata un'ulteriore causa della strutturale differenza tra un'attività di ricerca della prova nel mondo reale e in quello virtuale. Il ricorso alle tecnologie della rete consente, infatti, di oltrepassare sistematicamente le barriere fisiche preordinate a tutelare la *privacy* degli individui che una tradizionale attività investigativa generalmente incontra, rendendo del tutto ovvio che l'intrusione fisica non è più essenziale per comprimere le prerogative costituzionali[17], essendo ormai state sdoganate forme di osservazione e controllo non palesi, molto spesso non solo non efficientemente esperibili, ma neppure immaginabili *offline*. Tanto limita sistematicamente la capacità degli individui di reazione rispetto a certe forme di aggressione di loro beni giuridici, generando un'asimmetria informativa che solo un adeguato intervento regolatorio pare suscettibile di colmare al fine di ristabilire un equilibrio accettabile tra i contrapposti interessi in campo, evitando compressioni eccessive delle prerogative dei singoli[18].

---

[16] DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, 2, 288, che parla di promiscuità delle prove digitali, che «possono trovarsi collocate in spazi virtuali enormi e pieni di dati di ogni tipo. Non è raro che siano mescolate ad informazioni irrilevanti rispetto al reato, e magari attinenti alla vita privata dell'indagato o di altre persone». Si veda anche DI PAOLO, *Judicial investigations and gathering of evidence*, cit., 205, che, parlando di "liberalizzazione delle tecnologie", evidenzia come le stesse tendano ad aggregare quantità incredibili di dati, così facilitando incredibilmente il ricorso ad attività profilazione degli utenti.

[17] DI PAOLO, *Judicial investigations and gathering of evidence*, cit., 243.

[18] In termini, BALSAMO, *Le intercettazioni mediante* virus *informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 2016, 5, 2274, che osserva come «le tecnologie si innestano su istituti processuali tradizionali e ne modificano il volto e le potenzialità, al punto che dobbiamo ripensare il sistema delle garanzie consolidato in giurisprudenza».

È la stessa architettura del sistema, in definitiva, a dover indirizzare le scelte regolatorie del legislatore che intenda intervenire sulla materia e a influenzare qualsiasi tentativo di fornire un inquadramento sistematico della stessa da parte dell'interprete. Ciò in quanto, come avviene nel caso di specie, alcuni beni giuridici che nella dimensione fisica necessitano di forme di tutela più blande, nel mondo virtuale appaiono maggiormente vulnerabili e reclamano forme di protezione più intense.

2. L'attività di indagine *online*: *online search* e *online surveillance*.

Se, tradizionalmente, i mezzi di ricerca della prova hanno avuto quale bersaglio spazi e oggetti fisici facilmente individuabili[19], l'avvento delle nuove tecnologie ha profondamente mutato tale scenario: sempre più spesso accade che elementi probatori rilevanti per l'accertamento siano custoditi, anziché in supporti fisici, in spazi virtuali, in conseguenza della già segnalata tendenza degli individui a riversare nei dispositivi tecnologici di uso comune le più disparate informazioni sul loro agire quotidiano. Proprio in ragione di ciò, peraltro, a differenza di quanto potrebbe pensarsi di primo acchito, tale fenomeno riguarda non solo l'accertamento dei reati informatici ma anche dei reati comuni[20].

Ne è seguita una vera e propria «metamorfosi investigativa»[21] stante il sempre più cospicuo ricorso a tecniche di indagine inedite, basate sull'uso delle tecnologie informatiche, che stanno modificando profondamente i connotati dell'indagine penale e che appaiono talvolta difficilmente riconducibili, sul piano concettuale, agli istituti già noti al codice di rito[22].

Un simile cambiamento di paradigma rappresenta l'inevitabile conseguenza di alcune peculiari caratteristiche della tecnologia informatica, sulle quali anche la dottrina processualpenalistica riflette ormai da svariati anni, da ravvisarsi, anzitutto, nella

[19] DANIELE, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen e giust*. 2018, 5, 831.
[20] Così, DANIELE, *La prova digitale nel processo penale*, cit., 283.
[21] L'espressione è ripresa da SIGNORATO, *Le indagini digitali*, cit., 2018.
[22] Secondo FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. e giust*., 2016, 5, 121, «la scienza imprime al processo un'accelerazione eccezionale che cagiona un mutamento delle coordinate concettuali di alcuni istituti i quali vengono adattati a recepire nuovi contenuti». In alcuni casi, tuttavia, tale opera di adattamento non è possibile, se non al costo di opinabili forzature concettuali.

dematerializzazione dei dati contenuti nei supporti digitali[23], che ha comportato una serie di non trascurabili conseguenze.

Tra queste, merita di essere annoverata la scomparsa della tradizionale distinzione tra originale e copia, determinata dal fatto che il dato digitale è null'altro che una serie ordinata di *bit*, dunque di impulsi elettromagnetici infinitamente riproducibili, senza che tra l'originaria serie di partenza e quella generata dalla copia possa riscontrarsi differenza alcuna. Allo stesso tempo, la volatilità dei dati digitali, ovvero la loro instabilità e alterabilità, comporta l'esigenza di apprestare adeguate garanzie a tutela della loro integrità nel corso dell'estrazione e della successiva conservazione dei medesimi in ulteriori supporti digitali a disposizione degli investigatori.

Con le complesse problematiche connesse alla materia – invero ben più numerose di quelle solo sommariamente appena esemplificate[24] – si interfaccia costantemente la tecnica d'indagine ormai comunemente nota come *digital forensics*, il cui oggetto principale consiste nell'individuazione delle modalità più appropriate per procedere alla identificazione, estrazione e memorizzazione di elementi probatori aventi natura digitale per il tramite del ricorso a specifici strumenti informatici e con l'osservanza delle *best practices* elaborate e costantemente aggiornate dagli esperti in materia[25].

Negli anni, la dottrina ha avuto modo di individuare e affrontare i molteplici risvolti critici e le ripercussioni sistematiche di questa rivoluzione investigativa sugli assetti tradizionali dell'accertamento penale. Si è, così, messa in luce la tendenza delle indagini e della prova digitale a riproporre, esacerbandole, le problematiche tradizionalmente legate alla prova scientifica, alla sua presunta infallibilità e alle ripercussioni della medesima sulla cognizione del giudice, tentando di fornire chiavi di lettura adeguate al problema dell'elevato rischio di appiattimento del suo percorso decisionale sui risultati della stessa, normalmente veicolati nel processo grazie alla figura dell'esperto. Si è altresì posto in evidenzia il pericolo, meno immediatamente percepibile ma più

---

[23] PITTIRUTI, Digital evidence *e processo penale*, Giappichelli, 2017 4, che evidenzia come «le informazioni rilevanti ai fini investigativi sono, nel caso della *computer forensics*, conservate e trasmesse in un linguaggio diverso, ovverosia quello digitale. Seppure i dati digitali, nel loro contenuto informativo, possono essere immediatamente percepiti da colui che viene in contatto con essi, ciò non significa che siano dotati di una materialità immediatamente percepibile. Essi vivono, piuttosto, quali frammenti di elettricità veicolati attraverso contenitori, dai quali il dato può essere estratto mediante complesse operazioni tecniche».

[24] Per un'analisi esaustiva, si veda, per tutti, SIGNORATO, *Le indagini digitali*, cit., 1 ss.

[25] DI TARANTO, *Nuove tecniche d'investigazione nell'era digitale: il "malware" di Stato,* in *Ciberspazio e diritto*, 2017, Vol. 18, n. 57, 113 e 169.

dirompente per i suoi effetti strutturali, di un'alterazione sistematica degli equilibri tra indagini preliminari e dibattimento penale, conseguente al sempre maggiore ricorso, nella fase delle indagini, a mezzi di ricerca della prova altamente tecnologici caratterizzati dall'irripetibilità e dunque dalla fisiologica tendenza dei risultati probatori raggiunti a sconfinare nel dibattimento. Ancora, si è evidenziato come solo l'ossequio rigoroso ai protocolli e alle linee guida adottati nella fase dell'estrazione e della successiva conservazione dei dati sia suscettibile di confinare il rischio di una scarsa attendibilità della prova digitale all'interno di soglie ragionevolmente accettabili e si è ampiamente affrontata la complessa questione delle ripercussioni, sul piano processuale, di una violazione di siffatti protocolli[26].

È in questo complesso scenario che si inserisce il tema delle investigazioni *online*, che rispetto alle indagini digitali si pongono, per così dire, in un rapporto di specie a genere, sicché le prime sono contenute nelle seconde e ripropongono tutte le criticità appena segnalate, ma a queste se ne aggiungono altre la cui analisi rappresenta il principale proposito delle pagine che seguono.

Con il termine investigazioni *online* ci si riferisce, dunque, a quella porzione della più grande categoria delle indagini digitali nella quale si inseriscono le tecniche informatiche più evolute, che permettono l'acquisizione di dati rilevanti per l'accertamento penale sfruttando la rete *internet* e, dunque, consentendo agli investigatori di svolgere l'intera procedura di acquisizione dei dati da remoto, senza alcuna esigenza di un intervento propriamente fisico sui sistemi informatici bersaglio dell'attività, che, invece, continua a caratterizzare altri strumenti informatici di acquisizione della prova già regolati dalla legge[27].

---

[26] Per una rassegna delle complesse problematiche in questione, da ultimo, PAOLOZZI, *Relazione introduttiva*, in AA.VV., *Dimensione tecnologica e prova penale*, a cura di Luparia, Marafioti e Paolozzi, Giappichelli, 2019, 9 ss. Sulle molteplici questioni relative alla prova scientifica nel processo penale la letteratura è, ormai, sconfinata. Senza pretesa di esaustività, si vedano AA.VV., *Prova scientifica e processo penale*, Parti I e II, Cedam, 2022, 3 ss.; AA.VV., *Prova scientifica, ragionamento probatorio e decisione giudiziale*, a cura di Bertolino e Ubertis, Jovene, 2015; CONTI, *La prova scientifica*, in AA.VV., *La prova penale*, a cura di Ferrua, Marzaduri, Spangher e Rivello, Giappichelli, 2013, 87 ss.; DOMINIONI, *La prova penale scientifica*, Giuffré, 2005, *passim*; DOMINIONI, voce *Prova scientifica* (diritto processuale penale), in *Enc. dir., Annali*, vol. II, tomo I, Giuffrè, 2008, 976 ss.; FIANDACA, *Il giudice di fronte alle controversie tecnico-scientifiche. Il diritto e il processo penale*, in *Diritto e questioni pubbliche*, 2005; RIVELLO, *La prova scientifica*, Giuffrè, 2014, *passim*;

[27] Il riferimento è, ovviamente, agli istituti e alle modifiche del codice di rito introdotti a seguito dell'intervento legislativo scaturito dall'approvazione della l. 18 marzo 2008, n. 148, Legge di "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno". Con specifico riguardo alla

Vengono, in tal modo, assicurati il completo anonimato delle operazioni investigative, la loro segretezza e la possibilità di svolgere un controllo occulto e continuativo[28], acquisendo enormi quantitativi di dati e informazioni. Tutte caratteristiche, queste ultime, che se per un verso sono suscettibili di impattare su alcune fondamentali prerogative costituzionali in maniera molto più intensa di quanto non accada in conseguenza del ricorso agli ordinari mezzi, anche informatici, di ricerca della prova, per altro verso contribuiscono a rendere ancora più problematico l'inquadramento degli strumenti in questione nelle consuete categorie giuridiche e negli istituti propri delle indagini penali. Detto altrimenti, i nuovi strumenti di ricerca della prova da remoto non sembrano limitarsi a offrire agli inquirenti nuove modalità, più avanzate e intrusive, di attuazione di istituti processuali tradizionali, ma paiono rappresentare nuovi casi e modi di aggressione a beni giuridici costituzionalmente tutelati[29]. Tanto, com'è intuibile, con la conseguenza che diviene cruciale, per l'analisi della materia, l'istituto della prova atipica e della sua incidenza sulle prerogative costituzionali, che pure sarà oggetto di specifico approfondimento[30].

Quando si fa riferimento alle indagini svolte da remoto, si distinguono tradizionalmente due tipologie di attività: l'*online search* e *l'online surveillance*. Nella prima categoria si

---

materia processualpenalistica, le disposizioni previste dalla Convenzione imponevano alle Parti l'adozione e la definizione di procedure adeguate all'accertamento dei reati commessi per il tramite delle tecnologie informatiche, che consentissero di bilanciare l'interesse all'azione repressiva con la tutela dei diritti fondamentali. Oltre a introdurre alcune fattispecie penali relative a fatti commessi per il tramite delle tecnologie informatiche (per una panoramica delle modifiche apportate in materia di diritto penale sostanziale si veda PICOTTI, *Ratifica della convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. int.*, 2008, 5, 437), la legge in questione ha, infatti, modificato svariate norme del codice di rito, innestando nella disciplina concernente alcuni tradizionali mezzi di ricerca della prova (perquisizioni, ispezioni e sequestri) disposizioni specificamente volte a regolamentare la ricerca e l'apprensione dei dati informatici. Le modifiche più rilevanti al codice di procedura penale hanno riguardato le disposizioni in materia di ispezioni (art. 244, comma 2 c.p.p.), perquisizioni (art. 247, comma 1 *bis* e art. 352 c.p.p.) e sequestri (artt. 254, 254 *bis*, 256, 259, 260 c.p.p.) nonché l'attribuzione, agli ufficiali di polizia giudiziaria, di particolari poteri relativi all'assicurazione delle fonti di prova digitale nei casi di urgenza derivante dal rischio di dispersione o di alterazione dei dati (artt. 353 e 354 c.p.p.).

[28] Locuzione mutuata da NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Un tentativo di sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Cedam, 2020.

[29] NOCERINO, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in *Dir. pen. e proc*., 2021, 8, 1018. Si pensi, per meglio comprendere le capacità intrusive di simili strumenti, alla possibilità di procedere, grazie al ricorso agli stessi, a una vera e propria profilazione degli individui e, conseguentemente, a indagini a tappeto sulla personalità dell'imputato o dell'indagato, suscettibili di alterare gli esiti dell'accertamento penale, come rilevato, fin dagli anni '70, da VASSALLI, *I metodi di ricerca della verità e la loro incidenza sulla integrità della persona*, in *Riv. pen*., 1972, 1, 396 ss.

[30] Cfr. cap. 2. In termini, con riferimento, in generale, alla prova digitale, TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. pen. e proc.*, 2014, 6, 761.

fanno rientrare le attività investigative finalizzate alla ricerca e all'acquisizione, tramite l'intrusione nei sistemi informatici bersaglio degli investigatori, di dati e flussi informativi già archiviati negli stessi al momento dell'intervento sul sistema. Nella seconda categoria, invece, convergono le attività di acquisizione di dati e flussi informativi in tempo reale, cioè contestualmente alla loro formazione nel sistema informatico bersaglio[31]. In entrambi i casi, le informazioni acquisite vengono trasmesse via internet agli organi inquirenti.

A pensare, tuttavia, che la distinzione appena prospettata sia sempre così netta si commetterebbe un errore: le specifiche modalità tecniche di esecuzione delle operazioni, infatti, rendono non sempre agevole distinguere tra un'attività di ricerca e acquisizione di dati già archiviati nel sistema (*search*) e una di vera e propria *surveillance* continuativa, che, apparentemente, parrebbe essere quella maggiormente intrusiva. È evidente, infatti, come la distinzione tra le due attività tenda a sfumare sensibilmente ogniqualvolta la ricerca e acquisizione da remoto di dati già memorizzati nel sistema informatico venga attuata a intervalli ravvicinati e per considerevoli periodi di tempo. Tanto, ovviamente, farebbe trasfigurare l'attività comunemente definita come *search* in una vera e proprio sorveglianza occulta[32].

Peraltro, a ben vedere, anche l'effettiva corrispondenza al vero della conclusione relativa alla maggiore intrusività di un'attività di *surveillance* rispetto a una di *search* è questione controversa. Si è osservato, infatti, che se è vero che una sorveglianza continuativa consente l'apprensione in tempo reale di dati, comunicativi e non comunicativi, anche altamente riservati, è altrettanto vero che le capacità di memoria dei dispositivi informatici di uso quotidiano sono tali da mettere a disposizione degli

---

[31] BALSAMO, *Le intercettazioni mediante virus informatico*, cit., 2275. Nello stesso senso, BRIGHI, *Funzionamento e potenzialità investigative del* malware, in AA.VV., *Nuove norme in tema di intercettazioni: tutela della riservatezza, garanzie difensive e nuove tecnologie*, a cura di Giostra e Orlandi, Giappichelli, 2018, 222. Nello stesso senso, si vedano FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., 124 e TORRE, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. e proc.*, 2015, 9, 1163.

[32] Specularmente, si è evidenziato che una rigida classificazione è impedita anche dal fatto che le risultanze dell'*online surveillance* di solito non sono apprese in modo immediato, ma confluiscono in una serie di copie "salvate" nella memoria del sistema e trasmesse agli inquirenti ad intervalli di tempo ravvicinati, PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. e giust*., 2020, 2, 293. Sul tema si tornerà *funditus* nei capitoli 3 e 4.

inquirenti una quantità smisurata di dati sulle abitudini di vita presenti e passate dell'utilizzatore del sistema[33] e sui suoi rapporti personali e famigliari.

La linea di demarcazione appena prospettata, nondimeno, si rivela certamente utile su un piano metodologico nella misura in cui consente di impostare in maniera più chiara e lineare l'analisi della materia sia in una prospettiva *de iure condito* che in una prospettiva *de iure condendo*. Come si vedrà, infatti, mantenendo ferma questa distinzione appare più semplice verificare, di volta in volta, la riconducibilità di certi nuovi mezzi di ricerca della prova a categorie e istituti già esistenti, pur non essendo affatto scontato l'esito positivo della ricognizione. Allo stesso tempo, sotto il profilo della regolazione futura della materia, la distinzione appena prospettata sembra un utile punto di partenza per tracciare i confini di due categorie probatorie distinte sia sotto il piano operativo e "fenomenologico" dell'attività investigativa realizzata, sia sotto il piano dei diritti incisi[34].

Prima di entrare *in medias res*, però, occorre precisare che la presente analisi tralascerà volutamente l'approfondimento dell'attività di intercettazione eseguita tramite gli strumenti di ultima generazione che consentono lo svolgimento da remoto dell'atto.

La ragione di questa scelta va individuata nel fatto che tale tema, al centro del dibattito dottrinale degli ultimi anni sul tema delle prove, è stato già ampiamente esplorato.

A seguito di una importante pronuncia a Sezioni unite della Suprema corte[35], nella quale si è affermata l'ammissibilità della captazione ambientale disposta per il tramite del cosiddetto captatore informatico[36], il legislatore è intervenuto a regolare la materia. È stata introdotta una disciplina specifica, tarata su quella delle intercettazioni, che avrebbe dovuto essere in grado di far fronte alle criticità, anche operative, derivanti

---

[33] PARLATO, *Problemi insoluti: le perquisizioni on-line*, in AA.VV., *Nuove norme in tema di intercettazioni*, a cura di Giostra e Orlandi, Giappichelli, 2018, 314, rileva acutamente come «le attività "atipiche", nel contesto delle perquisizioni online, sono principalmente coincidenti con la *on-line search* e volte a ottenere copia, in tutto o in parte, della documentazione archiviata all'interno di un dispositivo. Stupisce come questo ambito di attività, più "periferico" rispetto al "mondo delle intercettazioni", abbia destato sinora minore interesse rispetto alla c.d. *on-line surveillance*, nonostante si tratti di operazioni particolarmente invasive 83. Per il loro tramite si riesce, infatti, a risalire a un'ingente massa di dati, formati anche in tempi di gran lunga antecedenti al provvedimento autorizzativo dell'autorità giudiziaria, senza alcuna previa selezione del materiale utile all'indagine».

[34] Cfr. capp. 3 e 4.

[35] Sez. un., 28 aprile 2016, n. 26889, Scurato, in *Arch. nuova proc. pen.*, 2017, 76 e ss. con nota di CAMON, *Cavalli di troia in Cassazione* e in *Cass. pen*. 2016, 2274, con nota di BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*.

[36] Come si vedrà, si tratta dello strumento tecnologico che, allo stato di avanzamento attuale della tecnica, consente effettivamente lo svolgimento di investigazioni da remoto tramite la rete internet (cfr. *infra*).

dalle peculiarità dello strumento informatico in questione, la cui caratteristica principale è, come noto, quella di consentire un'intercettazione ambientale itinerante tramite l'inoculazione di un *virus* informatico nel dispositivo portatile del bersaglio dell'attività di ricerca della prova e la conseguente acquisizione del controllo del microfono del dispositivo stesso[37].

Molteplici critiche sono state rivolte dalla dottrina alla pronuncia delle Sezioni unite prima e alla disciplina normativa introdotta dal legislatore poi, reputate entrambe insuscettibili di cogliere le peculiarità dello strumento informatico in questione e la maggiore lesione dei beni costituzionali connaturata al suo utilizzo rispetto a quanto non accada in un'intercettazione "tradizionale[38].

Pur essendosi protestata a gran voce l'esigenza di apprestare più intense garanzie, la riconduzione dell'attività d'indagine in questione alla categoria delle intercettazioni, quanto meno laddove ad essere captati siano contenuti di carattere comunicativo, è per

---

[37] Sulla specifica materia, si vedano le ampie riflessioni di BALSAMO, *Le intercettazioni mediante virus informatico*, cit., 2276 ss.; BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 2018, 4; BARROCU, *Il captatore informatico: un virus per tutte le stagioni*, in *Dir. pen. e proc*., 2017, 3, 379; BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* in *Riv. it. scienze giur*., 2017, 8 332 ss.; CAJANI, *Odissea del captatore informatico*, in *Cass. pen*. 2016, 11, 4140; CAMON, *Cavalli di troia in Cassazione*, in *Arch. n. proc. pen*., 2017, 1, 91 ss.; CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. bras. dir. proc. pen*., 2017, vol. 3, n. 2, 497 ss.; DANIELE, *L'illusione di domare il captatore informatico*, in *Leg. pen*., 2020, 2, 49 ss.; FOTI, *La nuova disciplina del captatore informatico. Un disfunzionale equilibrio?*, in *Proc. pen. e giust.*, 2021, 1, 202-214; GRIFFO, *Il captatore, tra luoghi e tempo*, in *Proc. pen. e giust.*, 2021, 3, 658-668; ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. e proc. pen.*, 2018, 2, 544 ss.; RIVELLO, *Le intercettazioni mediante captatore informatico*, in AA.VV., *Le nuove intercettazioni*, a cura di Mazza, Giappichelli, 2018; SIGNORATO, *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra e Orlandi, Giappichelli, 2018, 263 ss.; TESTAGUZZA, *I sistemi di controllo remoto*, cit., 760 ss.; TESTAGUZZA, Exitus acta probat "*Trojan" di Stato: la composizione di un conflitto*, in *Nuovo arch. pen*., 2016, 2.

[38] Si vedano, sul punto, le considerazioni di PARLATO, *Problemi insoluti: le perquisizioni on-line*, cit., 308, che evidenzia come l'ancoraggio alla disciplina delle intercettazioni sia insoddisfacente in quanto l'intrusione è in questo caso più intensa, trattandosi di strumento itinerante che, peraltro, consente di captare anche elementi non comunicativi, come suoni e rumori; sullo stesso piano le considerazioni di PINELLI, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di stato",* in *Dir. pen. cont*., 2017, 4, 79. Per una critica specifica alla pronuncia delle Sezioni unite, si vedano le considerazioni di FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen*., 2016, 2, 349, il quale evidenzia come la circostanza che, nel caso di captazione disposta tramite il *virus*, il giudice non possa previamente conoscere il domicilio intercettato, essendo lo strumento itinerante ed essendo imprevedibili gli spostamenti del soggetto che lo utilizza, comporta che si sia dinanzi a un mezzo di ricerca della prova non previsto dalla legge e non sottoponibile al previo controllo giurisdizionale quanto agli sconosciuti domicili che potranno essere violati, con la conseguente violazione della riserva di legge e di giurisdizione, imposta dagli artt. 14 e 15 Cost., oltre che dall'art. 8 C.e.d.u.

lo più incontroversa[39]. Tanto giustifica il mancato approfondimento della questione in questa sede, con l'avvertenza, però, che anche in questo caso occorre guardarsi da semplificazioni eccessive.

Volendo adottare lo schema interpretativo ormai consolidato nella giurisprudenza di legittimità a partire dalla pronuncia a Sezioni unite del 28 maggio 2003, n. 6747, Torcasio[40], non è, infatti, sempre semplice operare una netta distinzione tra le attività che rientrano nel perimetro concettuale delle intercettazioni e quelle che si pongono al di fuori di questa categoria. Tanto più quando si tratti di strumenti che consentono l'acquisizione da remoto della prova tramite il controllo, anche per lunghi periodi di tempo, del dispositivo informatico. Valga su tutti l'esempio dell'acquisizione, protratta e ripetuta a intervalli ravvicinati nel tempo, delle *e-email* già inviate e ricevute dalla casella di posta elettronica[41]. Trattasi di un'attività che, attenendosi rigorosamente alle coordinate ermeneutiche fornite dalla giurisprudenza della Suprema corte, dovrebbe collocarsi al di fuori del perimetro delle intercettazioni. Ma una simile lettura appare eccessivamente formalistica, atteso che non v'è dubbio che nel caso in considerazione la lesione della libertà e segretezza delle comunicazioni tutelata dall'art. 15 Cost. sembra in tutto e per tutto assimilabile, qualitativamente e quantitativamente, a quella conseguente a un'attività di intercettazione in senso stretto, sicché differenze di disciplina tra le due attività rischiano di apparire del tutto irragionevoli[42].

---

[39] Esprime convincentemente perplessità rispetto a questo assetto, tuttavia, CAPRIOLI, *Il "captatore informatico" come strumento di ricerca*, cit., 49, che evidenzia che anche quando l'attività svolta tramite il captatore è inquadrabile nella categoria delle intercettazioni di conversazioni, la relativa disciplina è insoddisfacente in quanto traspone sul piano normativo un bilanciamento di interessi che non è più attuale essendo il nuovo strumento del captatore molto più intrusivo.

[40] Secondo la pronuncia, l'intercettazione consiste nella captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere altri e con modalità oggettivamente idonee allo scopo. Ulteriore connotato è che essa sia attuata da soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato.

[41] Il tema sarà oggetto di successiva analisi nel cap. 4.

[42] Sul punto, si veda anche PARLATO, *Libertà della persona nell'uso delle tecnologie digitali*, cit., 292 ss., che evidenzia come «in relazione all'uso di dispositivi elettronici, ad esempio, non è semplice discernere ciò che può essere considerato "comunicazione" da quanto, invece, sia estraneo a tale categoria. Ne derivano interrogativi circa la possibilità di ricondurre, o meno, specifiche fattispecie alla disciplina prevista per le intercettazioni. […] Il principale punto di contatto con la fattispecie delle intercettazioni riguarda la captazione di messaggi inoltrati via mail, via chat e tramite programmi come *whatsapp*, nonché la possibilità di conoscere "eventi" acustici o visivi, grazie all'attivazione del microfono e della telecamera in dotazione nel dispositivo».

2.1. Lo strumento tecnologico: il *trojan virus* e le sue applicazioni.

Il *trojan virus*[43], noto anche come captatore informatico, è uno strumento di vigilanza da remoto che, inoculato in un dispositivo informatico, consente di acquisirne il pressoché totale controllo. Si tratta, dunque, di un vero e proprio *maleware*, ovvero di un *software* appartenente alla categoria dei *virus* informatici, con la quale condivide la caratteristica, particolarmente subdola, di poter essere installato nel sistema bersaglio e di operare al suo interno in maniera furtiva, senza cioè che l'utilizzatore del dispositivo sappia alcunché in ordine alla sua presenza[44].

L'inserimento del dispositivo nel sistema bersaglio può avvenire tramite due distinte modalità. È possibile, anzitutto, procedere a un'installazione del *virus* per il tramite di un intervento fisico sul dispositivo, ma trattasi di una soluzione normalmente non praticata dagli investigatori in quanto comporta maggiori rischi che l'attività investigativa sia scoperta dal soggetto sottoposto all'indagine o, comunque, dall'utilizzatore del dispositivo. Ragione per cui, generalmente, si procede all'installazione del *maleware* da remoto, essendo tale soluzione tecnicamente esperibile in maniera piuttosto semplice sfruttando la connessione a internet del dispositivo. In questo caso, il *virus* viene, letteralmente, camuffato in un aggiornamento del sistema operativo o in altra operazione informatica che l'utilizzatore del dispositivo percepisce alla stregua di una usuale attività di modifica o adeguamento dello stesso. In tal caso, dunque, l'installazione avviene per il tramite della collaborazione, naturalmente inconsapevole, dello stesso utilizzatore del dispositivo[45].

---

[43] Occorre premettere che l'analisi che segue si concentra su questo peculiare strumento informatico in quanto è quello attualmente reso disponibile dallo stato di avanzamento della tecnica informatica. Naturalmente, però, le considerazioni che seguono devono intendersi riferite anche a qualsivoglia altro strumento, anche futuro, che consenta di svolgere attività di investigazione da remoto del tipo di quelle descritte nelle pagine seguenti.

[44] Per una ricognizione delle caratteristiche tecniche del captatore si veda, per tutti, BRIGHI, *Funzionamento e potenzialità investigative del* malware, cit., 219, il quale specifica, sul piano tecnico, che «i captatori informatici sono dunque composti da due moduli principali: il programma *server* che infetta il dispositivo oggetto di indagine e il programma client, necessario per il controllo da remoto del dispositivo stesso; si differenziano dalla categoria generale dei sistemi di controllo remoto, tuttavia, perché l'installazione della componente server avviene di nascosto, senza che la "vittima" si accorga del captatore attivo sul suo dispositivo».

[45] Sul punto, si veda, ancora una volta BRIGHI, *Funzionamento e potenzialità investigative del* malware, cit., 219, nonché BARROCU, *Il captatore informatico*, cit., 379.

Tali *maleware*, poi, sono generalmente dotati di infrastrutture informatiche tali da consentire di aggirare qualsivoglia contromisura in grado di ostacolarli[46] e di eliminare ogni traccia della loro presenza nel sistema informativo di riferimento[47].

Acquisito il controllo del sistema informatico, il captatore è in grado di operare sullo stesso alla stessa stregua di un soggetto che ne avesse la disponibilità fisica. Può, infatti, agire su qualunque periferica di *input* o di *output*[48] e sui *software* nello stesso installati, alla stregua di un invisibile osservatore di tutto quanto avviene non solo al suo interno, ma anche intorno allo stesso.

È possibile attivare la videocamera, captando occultamente video e foto; accedere, estraendone copia, a tutto quanto memorizzato nel dispositivo (a mero titolo di esempio, i contatti in rubrica, l'agenda, la lista delle chiamate in entrata e in uscita, i *files* multimediali, i messaggi inviati e ricevuti e così via); tracciare gli spostamenti dell'utilizzatore del dispositivo sfruttando i sistemi di localizzazione presenti sullo stesso; effettuare attività di *keylogging*, monitorando tutto quanto viene visualizzato digitato sulla tastiera del dispositivo e consentendo, in tal modo, anche di acquisire le *passwords* e le chiavi di sicurezza di qualunque applicazione di servizi – si pensi a quelli bancari o assicurativi – ai quali l'utente accede tramite il dispositivo; intervenire su qualunque tipo di *file* presente nello stesso, modificandolo, alterandolo o eliminandolo; specularmente, è possibile installare sul dispositivo nuovi contenuti digitali[49].

Uno dei principali vantaggi – e, al contempo, delle più evidenti attrattive – del ricorso al *virus*, peraltro, è quello di consentire di eludere completamente qualunque sistema di criptatura cui le più comuni applicazioni di messaggistica (come *Whatsapp, Blackberry, Telegram, Skype*) fanno ricorso per tutelare la segretezza delle comunicazioni dei loro clienti, frapponendo un significativo ostacolo allo svolgimento di un'attività di intercettazione "tradizionale". Al contempo, viene del tutto aggirato il problema

---

[46] TESTAGUZZA, *I Sistemi di controllo remoto*, cit., 759.

[47] BRIGHI, *Funzionamento e potenzialità investigative del* malware, cit., 222.

[48] Si tratta delle componenti *hardware* del dispositivo, come la tastiera, il *touchpad*, il microfono, la *webcam*, gli altoparlanti e così via.

[49] Si vedano BRIGHI, *Funzionamento e potenzialità investigative del* malware, cit., 221; BRONZO, *L'impiego del* trojan horse *informatico*, cit., 346; CAPRIOLI, *Il "captatore informatico" come strumento di ricerca*, cit., 484; in termini, MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, in AA.VV., *Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura*, a cura di Giarda, Giunta e Varraso, Cedam, 2018, 195-196; MANCUSO, *La perquisizione* on line, in *Jusonline*, 2017, 3, 415; BALSAMO, *Le intercettazioni mediante* virus *informatico*, cit., 2275.

dell'acquisizione dei dati presenti sul *cloud*[50], rendendo superfluo il ricorso alla rogatoria[51].

La massa di dati che può, in tal modo, entrare nella disponibilità degli inquirenti è smisurata e non paragonabile, né su un piano quantitativo né su quello qualitativo, alle notizie acquisibili tramite gli ordinari mezzi di ricerca della prova. La tecnologia in argomento consente di operare una vera e propria "pesca a strascico" di informazioni attinenti ai più disparati aspetti della vita dell'utilizzatore del sistema, ivi inclusi quelli che non avrebbero rilevanza alcuna rispetto all'oggetto delle investigazioni. Si è lucidamente parlato, non a caso, di una sorta di «chip inserito sotto pelle che consente di controllare la totalità delle azioni, delle comunicazioni e anche dei pensieri di un individuo, senza possibilità alcuna di scindere ciò che può essere utile, o meglio utilizzabile, nel processo penale, con aspetti che sono e devono rimanere necessariamente privati»[52]. Nulla impedirebbe, dunque, di procedere a un vero e proprio *profiling* del soggetto sottoposto all'indagine, ricostruendone i gusti, le abitudini, gli orientamenti politici, sessuali e religiosi[53].

Il controllo sugli aspetti più privati della persona umana diviene, in tal modo, incredibilmente penetrante.

2.2. Lo strumento normativo: assenza di una regolamentazione *ad hoc*.

Nonostante il carattere particolarmente intrusivo delle attività di indagine che il captatore consente di esperire, l'intervento legislativo in materia si è limitato, come visto, alla sola disciplina relativa all'uso del *trojan virus* per le intercettazioni tra presenti[54], mentre alcun tipo di regolamentazione si ravvisa, allo stato, con riferimento a tutte le altre attività investigative che, come visto, è possibile esperire tramite l'uso della formidabile tecnologia informatica di cui si discorre[55].

Ciò pone, quanto meno, due ordini di questioni.

---

[50] Il riferimento è alla tecnologia informatica grazie alla quale è possibile conservare i dati non già sul dispositivo informatico in possesso dell'utilizzatore, ma direttamente sulla rete, generalmente sfruttando dei *server* situati all'estero. Si veda, per un approfondimento sul funzionamento di tale tecnologia e sulle problematiche connesse alla stessa, SIGNORATO, *Le indagini digitali*, cit., 55 ss.

[51] CAMON, *Cavalli di troia in Cassazione*, cit., 91.

[52] BARROCU, *Il captatore informatico*, cit., 390.

[53] BRONZO, *L'impiego del* trojan horse *informatico*, cit., 7, 350. In termini, FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., 121.

[54] BRONZO, *L'impiego del* trojan horse *informatico*, cit., 330.

[55] Parla, a questo proposito, di un colpevole disinteresse del legislatore DANIELE, *La vocazione espansiva delle indagini informatiche*, cit., 834.

La prima, che si muove in una prospettiva *de iure condito*, attiene al se e in che misura le attività esperibili tramite l'uso del captatore non espressamente disciplinate dalla legge siano riconducibili a istituti a categorie giuridiche già esistenti e possano, dunque, trattarsi alla stregua di strumenti di ricerca della prova "tradizionali", rispetto ai quali il carattere di novità attiene esclusivamente allo strumento tecnico utilizzato. Tanto con la conseguenza che simili atti di indagine sarebbero perfettamente legittimi e i loro esiti pienamente utilizzabili.

La seconda, che invece si muove in una prospettiva *de iure condendo*, è relativa all'approccio regolatorio da seguire nel caso in cui il legislatore dovesse intervenire per delineare una disciplina complessiva della materia.

Muovendo da un piano squisitamente concettuale, occorre segnalare che entrambi i quesiti dipendono dalla soluzione di una questione preliminare in ordine alla quale non v'è, in dottrina, unanimità di vedute. Il riferimento è, in particolare, all'opportunità di procedere a una scomposizione delle singole potenzialità investigative del captatore informatico, tante quante sono le attività di indagine cui risultano assimilabili[56], ovvero di fornire un inquadramento unitario delle tecniche in questione, sul presupposto che "spacchettare" le singole attività esperibili equivarrebbe a una forzatura concettuale[57].

Si tratta, però, di un falso problema. L'adozione dell'uno o dell'altro paradigma finisce, inevitabilmente, per dipendere da quale delle due prospettive sopra segnalate è oggetto di analisi. Detto altrimenti, in un'ottica *de iure condito* non vi sono molte alternative a una scomposizione delle singole attività esperibili tramite il captatore al fine di verificare se le stesse siano riconducibili ai mezzi di ricerca della prova già noti al codice di rito e, dunque, se i loro esiti conoscitivi abbiano o meno diritto di cittadinanza nel procedimento penale. In una prospettiva *de iure condendo*, al contrario, sarebbe probabilmente preferibile una regolazione complessiva ed unitaria dello strumento in questione, che meglio consentirebbe di coglierne appieno l'efficacia intrusiva e, conseguentemente, di mettere a punto una trama di garanzie che consenta di bilanciare

[56] In questo senso, FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento* penale, cit., 123, secondo la quale «ogni singola cadenza di tale procedimento deve essere inquadrata giuridicamente e disciplinata»; MANCUSO, *La perquisizione* on line, cit., 424, che evidenzia come, anche in ragione della diversità dei beni giuridici che possono essere incisi dalle attività captative in argomento, sia difficoltoso ricondurre le tecniche in questione a un unico *nomen iuris*.

[57] Di questo tenore le considerazioni di BARROCU, *Il captatore informatico*, cit., 386 e di IOVENE, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont*., 2014, 3-4, 330, secondo la quale le perquisizioni *online* finiscono per assommare diversi strumenti di indagine.

adeguatamente l'interesse alla riservatezza dei singoli con quello alla repressione dei reati[58]. È evidente, infatti, che il principale limite di una ricostruzione che pretenda di scindere in tante singole monadi le specifiche attività intrusive esperibili tramite la tecnologia in argomento sia da ravvisarsi nel fatto che essa che non permetta di afferrarne appieno l'efficacia intrusiva quando le singole attività investigative non vengano compiute isolatamente ma si cumulino tra loro[59].

L'assenza di qualsivoglia indicazione normativa in merito agli ulteriori usi del captatore informatico ha, come si diceva, rimesso all'interprete la soluzione della questione dell'ammissibilità di tali ulteriori impieghi dello strumento[60]. Tanto in quanto, come pressoché unanimemente evidenziato dalla dottrina processualpenalistica, l'ammissibilità degli impieghi del captatore per lo svolgimento di attività diverse dalle intercettazioni telefoniche dovrebbe essere limitata al caso in cui si tratti esclusivamente del ricorso a una metodologia particolare per compiere attività investigative già regolamentate[61] ovvero attività investigative non riconducibili a istituti già normati ma non incidenti su diritti fondamentali.

La mancanza di una specifica regolamentazione della materia non implica, dunque, in maniera pressoché automatica che simili attività debbano ritenersi vietate e i loro esiti inutilizzabili. Il tema si intreccia inesorabilmente con quello della prova atipica e incostituzionale[62].

In alcuni casi, infatti, le attività in questione parrebbero riconducibili a strumenti di ricerca della prova già disciplinati dalla legge. È, ad esempio, quanto si è riscontrato in materia di intercettazioni ambientali ancora prima dell'intervento legislativo sull'uso del *trojan* per la loro esecuzione. In altri casi, invece, tali strumenti non sembrano riconducibili alle categorie giuridiche e agli istituti già esistenti. Nondimeno, i relativi

---

[58] Per tale soluzione, si veda anche NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 61.

[59] Sul punto si tornerà *funditus* nel cap. 4.

[60] BRONZO, *L'impiego del* trojan horse *informatico*, cit., 350, che evidenzia come oggi sia rimessa alla sola giurisprudenza la scelta se ricondurre queste attività a categorie esistenti o meno. Nello stesso senso, CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. e proc*., 2018, 9, 1579, che stigmatizza apertamente il fatto «che il giudice sia stato chiamato ad una attività di "creazione" della disciplina in applicazione del principio di proporzionalità». In termini, MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, cit., 194.

[61] BRONZO, *L'impiego del* trojan horse *informatico*, cit., 346.

[62] Vedi cap. 2.

risultati probatori potrebbero essere considerati alla stregua di prove non disciplinate dalla legge, ai sensi dell'art. 189 c.p.p.[63].

Tale conclusione, però, come si vedrà, va recisamente esclusa tutte le volte in cui si sia al cospetto di una prova che incida su diritti fondamentali degli individui costituzionalmente presidiati tramite riserva di legge e di giurisdizione: in caso di prova atipica, infatti, per definizione, manca la predeterminazione legale dei casi e dei modi della restrizione che, invece, è necessaria per non violare la riserva assoluta di legge imposta dalla Costituzione per gli atti che si risolvono nella intrusione in un diritto qualificato come inviolabile.

Quando gli istituti processuali impattano sui diritti che la Costituzione definisce inviolabili, è necessario che la legge fornisca una disciplina chiara, in ossequio al principio di legalità[64], suscettibile di comporre in un bilanciamento adeguato i contrapposti interessi in gioco[65]. I diritti fondamentali rappresentano, anzitutto, dei limiti all'azione della pubblica autorità, con la conseguenza che qualsivoglia attività della medesima che comporti la restrizione di quel diritto trova la sua legittimazione esclusivamente nella predisposizione di regole legali che assoggettino l'intrusione ad appositi limiti e controlli, volti a verificare l'effettiva osservanza delle garanzie imposte dalla legge da parte dei pubblici poteri[66].

Peraltro, i nuovi strumenti tecnologici, e tra questi il captatore, consentono lo svolgimento di attività di ricerca che sembrano impattare su aspettative di tutela inedite, non integralmente riconducibili ai tradizionali diritti di libertà tutelati dalla Carta costituzionale. Si tratta di un altro campo in cui le caratteristiche peculiari della

---

[63] CAPRIOLI, *Il "captatore informatico" come strumento di ricerca*, cit., 485 ss. In termini, BONTEMPELLI, *Il captatore informatico in attesa della riforma*, cit., 2; si veda, altresì, BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in AA.VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra e Orlandi, Giappichelli, 2018, 237-238, che pure distingue tra impieghi ammissibili del captatore («nelle ipotesi in cui l'inoculazione del virus costituisca solo una particolare metodica di attività investigative già conosciute e regolamentate») e altri inammissibili, ammonendo, però, in ordine al fatto che l'inammissibilità si estenda anche ai casi in cui i meccanismi "assomiglino" solamente, ma non siano completamente sovrapponibili, «a quelli propri di mezzi investigativi consentiti: ad esempio, le cosiddette perquisizioni on-line (on-line search) o l'accesso, con facoltà di copia, ai dati memorizzati nei dispositivi o in cloud».

[64] CONTI, *Prova informatica e diritti fondamentali*, cit., 1210.

[65] FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., 122.

[66] GAITO e FÙRFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen.*, 2016, 2, 313.

tecnologia sembrano incidere profondamente, rendendo obsolete le attuali categorie giuridiche e non più rinviabile l'esigenza di aggiornarne il catalogo[67].

3. Diritti costituzionali e investigazioni *online*: l'importanza della definizione della base costituzionale.

È ravvisabile un nesso di diretta proporzione tra la potenza euristica dello strumento tecnologico che consente lo svolgimento di investigazioni da remoto e il *vulnus* alle aspettative individuali di tutela incise da simili misure[68]. Ne deriva un accrescimento delle esigenze di garanzia, per far fronte al quale si è parlato, efficacemente, di un bisogno di protezione progressiva dei diritti fondamentali degli individui in un duplice senso[69]. Per un verso, occorre adeguare e implementare le garanzie esistenti e riconoscerne di nuove, prendendo atto del fatto che gli strumenti tecnologici di ultima generazione incidono su posizioni soggettive in qualche misura inedite. Essi, infatti, non si limitano a rendere possibili nuove forme di aggressione a beni giuridici già noti, ma si spingono a colpire prerogative la cui emersione è relativamente recente e rappresenta il precipitato della massiva digitalizzazione della vita delle persone che contrassegna l'epoca contemporanea. Per altro verso, e in conseguenza di ciò, occorre ridisegnare gli equilibri del bilanciamento tra la tutela dei diritti fondamentali e l'esigenza di repressione dei reati, la cui attuale traduzione sul piano normativo rappresenta il portato di scelte di politica criminale che, se potevano apparire ragionevoli dinanzi a un differente organigramma dei diritti incisi dalle investigazioni penali, risultano oggi anacronistiche a fronte delle rinnovate potenzialità intrusive dei nuovi strumenti tecnologici.

La questione al fondo del dibattito che, su queste tematiche, agita da tempo la dottrina può essere così riassunta: se i nuovi mezzi tecnologici di ricerca della prova incidano su diritti fondamentali espressamente sanciti dalla Costituzione e, in caso positivo, su quali; ovvero se incidano su diritti, in qualche misura "nuovi" e, in quest'ultimo caso, quale debba essere lo statuto per la loro migliore salvaguardia.

---

[67] In tal senso, con specifico riferimento ai diritti fondamentali tutelati dalla Costituzione, si veda KOSTORIS, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in AA.VV., *Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, a cura di Ruggieri e Picotti, Giappichelli, 2011, 179.

[68] CONTI, *Sicurezza e riservatezza*, in *Dir. pen. e proc*., 2019, 11, 157.

[69] ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. e proc. pen*., 2014, 57, 3, 1151.

La definizione di una base costituzionale delle prerogative incise da simili misure è, infatti, questione tutt'altro che teorica. Dalla sua soluzione discendono conseguenze pratiche di estremo rilievo sul duplice piano dell'assetto attuale dei nuovi mezzi di ricerca della prova e delle scelte future del legislatore in materia.

Sotto il primo profilo, anche alla luce di quanto si è già accennato nelle pagine precedenti in tema di prova atipica e incostituzionale, è evidente che ricondurre l'efficacia lesiva delle nuove misure a prerogative costituzionali presidiate dalla doppia riserva di legge e giurisdizione (si pensi agli artt. 13 ss. Cost.) comporta precise conseguenze – da ravvisarsi, come si vedrà, nell'inammissibilità di simili strumenti e nell'inutilizzabilità dei relativi esiti probatori[70] – nel caso in cui dovesse concludersi per la mancanza di una base legale alla luce dell'impossibilità di inquadrare tali strumenti investigativi in istituti già regolati dalla legge. Conseguenze, quelle appena delineate, che invece non si produrrebbero ove si reputasse che l'impatto di simili misure sia limitato a prerogative (si pensi all'art. 2 Cost., da cui generalmente si fa discendere[71] il diritto alla *privacy*) la cui restrizione è sottoposta a uno statuto di tutela più blando. Tanto, peraltro, senza considerare che l'individuazione dei diritti incisi dalla misura finisce per influenzare lo stesso inquadramento giuridico delle attività investigative rese possibili dagli strumenti di cui si discorre[72].

Lo scenario è, poi, ulteriormente complicato da quanto si è già avuto modo di anticipare in ordine all'accresciuta consapevolezza della difficoltà di ricondurre le prerogative incise da tali strumenti a garanzie costituzionali già espresse, atteso che il loro contenuto sembra non essere perfettamente convergente con quello proprio di queste ultime[73]. Sicché, ove si reputasse di essere dinanzi a diritti fondamentali "nuovi", si porrebbe altresì il problema di individuarne il preciso statuto di tutela.

Anche in una prospettiva *de iure condendo* la previa individuazione delle garanzie connesse alla restrizione dei diritti implicati nell'utilizzo di dispositivi digitali

[70] Cfr. cap. 2.

[71] Come si vedrà nelle pagine seguenti, non senza qualche forzatura.

[72] Esemplare, ancora una volta, la questione relativa all'assimilabilità della apprensione delle *e-mail* già spedite e ricevute all'attività di intercettazione delle comunicazioni, la cui soluzione finisce per essere influenzata dall'individuazione della prerogativa costituzionale incisa nel caso di specie. Nel caso in cui si reputasse l'incidenza dell'investigativa in questione sulla libertà e segretezza delle comunicazioni, infatti, un inquadramento della stessa alla stregua di una mera acquisizione documentale o di tipologie investigative similari sarebbe senz'altro riduttiva. In termini, PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. e giust.*, 2020, 2, 296.

[73] Sul punto, si veda il paragrafo seguente.

costituisce l'insopprimibile premessa di qualsivoglia discussione. Infatti, solo ove si riconosca che i più intrusivi strumenti di ricerca della prova messi a disposizione dalle nuove tecnologie incidono su diritti fondamentali potrebbe concludersi nel senso che il legislatore sia tenuto a mettere a punto non già una disciplina normativa quale che sia, ma una legge che abbia determinate caratteristiche in punto di proporzione[74]. E ciò anche in ossequio agli ultimi moniti della giurisprudenza europea in materia di misure tecnologiche restrittive dell'aspettativa di riservatezza degli individui, che hanno contribuito a delineare il contenuto – o meglio, i contenuti minimi – di una disciplina normativa che possa dirsi rispettosa del principio di legalità della misura.

Sulla scorta delle ultime indicazioni in materia[75], deve considerarsi ormai un dato acquisito che proporzionalità e legalità delle misure restrittive delle prerogative individuali siano inestricabilmente legate, in quanto il principio di necessaria proporzione implica, anche in ossequio al disposto dell'art. 52 della Carta di Nizza, la trasposizione sul piano legislativo del bilanciamento dei contrapposti interessi rilevanti nel caso di specie, tramite l'individuazione dei presupposti sostanziali e procedurali per l'adozione della misura, di modo che i soggetti incisi dalla stessa possano prevedere le conseguenze delle loro azioni ed essere dotati di adeguati strumenti di reazione alle ingerenze dell'autorità pubblica[76].

---

[74] GAITO e FÙRFARO, *Le nuove intercettazioni "ambulanti"*, cit., 313 ss.

[75] Contenute, da ultimo, nella sentenza della Corte di Giustizia dell'Unione Europea del 2 marzo 2021 (c-746/18) nel caso H.K., in materia di tabulati telefonici. Vedi anche Corte Giust. 16 dicembre 2021 (c-24/19), con commento di DANIELE, *Il controllo giurisdizionale sull'emissione dell'ordine europeo di indagine: la necessaria simmetria con la disciplina nazionale nei casi interni analoghi*, in *Sistema penale*, 31 marzo 2022. Per una disamina dei principi espressi dalla giurisprudenza europea sul punto, tanto con riguardo alla Corte di Giustizia, quanto con riferimento alla Corte europea dei diritti dell'uomo, si veda il par. 4.1.2. del capitolo 3.

[76] La Corte, infatti, al par. 48 della decisione del 2 marzo 2021, parla espressamente di «regole chiare e precise che disciplinano la portata e l'applicazione della misura in questione e fissino dei requisiti minimi, di modo che le persone i cui dati personali vengono in discussione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abusi. Tale normativa deve essere legalmente vincolante nell'ordinamento interno e precisare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di dati del genere, in modo da garantire che l'ingerenza sia limitata allo stretto necessario». Tanto, peraltro, similmente alle sollecitazioni della dottrina che, negli ultimi anni, si è specificamente occupata del tema della proporzionalità delle misure adottate nel processo penale impattanti sui diritti di riservatezza, anche informatica e telematica, degli individui. Si è, infatti, evidenziato come l'elaborazione di una disciplina legislativa in materia, in grado di cogliere le peculiarità della stessa e di individuare in maniera più stringente i limiti dell'ingerenza dell'autorità pubblica nelle prerogative individuali è necessaria perché il vaglio di proporzionalità possa essere adeguatamente effettuato nella sede processuale, risultando, altrimenti, sbrigliato da qualsivoglia criterio direttivo ed esponendo i diritti fondamentali dei singoli al rischio di abusi. In tal senso, NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. e proc. pen.*, 2020, 1, 32; NEGRI, *Splendori e miserie della legalità*

3.1. L'individuazione dei diritti costituzionali coinvolti (riservatezza, libertà e segretezza delle comunicazioni, inviolabilità del domicilio, libertà morale).

L'accresciuta attitudine intrusiva dei nuovi strumenti tecnologici di ricerca della prova induce l'interprete a interrogarsi sulla congruità del riferimento ai tradizionali diritti di libertà nella ricerca della copertura costituzionale delle prerogative individuali incise da questi ultimi[77].

È evidente, ad esempio, l'inadeguatezza del richiamo alla sola libertà e segretezza delle comunicazioni presidiata dall'art. 15 Cost., atteso che il ricorso alle tecnologie in argomento consente l'apprensione non solo di dati comunicativi ma anche di altra natura[78], la qual cosa induce inevitabilmente ad ampliare lo spettro dell'indagine a possibili ulteriori parametri di tutela.

Tra questi, appare intuitivo il riferimento al diritto alla riservatezza, tradizionalmente ricondotto all'art. 2 Cost. che, operando alla stregua di una fattispecie aperta, consentirebbe l'enucleazione di nuovi diritti fondamentali non espressamente sanciti dalla Carta[79]. Tale aggancio costituzionale, tuttavia, risulta insoddisfacente e inadeguato ad apprestare un reticolo di garanzie la cui intensità sia effettivamente parametrata alle gravi intrusioni realizzabili per il tramite del ricorso alle tecnologie oggetto di analisi. La norma in questione, contrariamente agli artt. 13 ss. Cost., non individua con il dovuto rigore i presupposti della legittimità di una limitazione dei diritti inviolabili ivi

---

processuale. Genealogie culturali, "èthos" delle fonti, dialettica tra le Corti, in *Arch. pen*., 2017, 2, 454, che evidenzia come, in vista di un recupero del primigenio significato del principio di legalità, «la battaglia meritevole d'essere combattuta dalla dogmatica e dal ceto forense consiste nel munire la legalità processuale di uno statuto metodologico completo, accrescendo la qualità del canone costituzionale così da assoggettare il momento applicativo sia al criterio della massima fedeltà al testo scritto, sia al divieto per il singolo interprete di aprire lo schema formale della fattispecie al bilanciamento con valori, principi e interessi estranei alla medesima o di riconfigurare la proporzione tra le diverse esigenze in gioco rispetto alle calibrature prefissate dal legislatore». Nel senso che il principio di legalità impone la definizione previa, ad opera del legislatore, delle regole processuali applicabili, anche in materia di restrizione dei diritti fondamentali dei singoli, e che non siano concepibili soluzioni tese ad affidare al giudice il compito di realizzare il bilanciamento degli interessi in campo, MAZZA, *Legge e potere: l'irruzione delle Corti internazionali*, in AA.VV., *Legge e potere nel processo penale. Atti del Convegno. Bologna, 4 e 5 novembre 2016*, Cedam, 2017, 190 ss. In generale, si veda il volume da ultimo citato sul tema progressivo indebolimento del principio di legalità ad opera della giurisprudenza interna, anche su impulso delle linee interpretative adottate dalle Corti europee. Vedi anche cap. 3, par. 4.1.2.

[77] FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., 126.

[78] PARLATO, *Problemi insoluti: le perquisizioni on-line,* cit., 301 ss.

[79] In tal senso, ad esempio, IOVENE, *Le c.d. perquisizioni online*, cit., 336.

sanciti ad opera dei pubblici poteri[80], non essendo espressamente presidiata né da riserva di legge, né da riserva di giurisdizione.

È per tale ragione che una parte della dottrina[81] ha proposto di integrare il richiamo alla norma tramite l'ancoraggio alle garanzie sancite a livello sovranazionale e, segnatamente, all'art. 8 della Convenzione europea dei diritti dell'uomo che, come noto, tutela il diritto al rispetto della vita privata. Risultato, quest'ultimo, che si raggiungerebbe valorizzando i principi da tempo affermati dalla giurisprudenza costituzionale[82] in tema di rapporti tra l'ordinamento interno e quello sovranazionale, alla stregua dei quali le norme C.e.d.u. a salvaguardia dei diritti fondamentali costituiscono norme interposte del giudizio di costituzionalità delle leggi, stante il disposto dell'art. 117, comma 1, Cost. L'ancoraggio alla disposizione di cui all'art. 8 della Convenzione consentirebbe di colmare, infatti, la mancata individuazione, ad opera dell'art. 2 Cost., delle precise condizioni alle quali può reputarsi legittima la compressione delle prerogative di riservatezza dei singoli in funzione dell'accertamento e del perseguimento dei reati tramite il richiamo alla necessaria previsione, ad opera della legge, dei presupposti dell'ingerenza e della proporzionalità della stessa, che dovrebbe assumere i contorni di «una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la sicurezza pubblica, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, per la protezione dei diritti e delle libertà degli altri»[83].

L'argomento, però, prova troppo. Che il richiamo all'art. 8 della Convenzione sia davvero sufficiente a soddisfare pienamente le esigenze di tutela della riservatezza dei

---

[80] Così, ad esempio, CAMON, *Cavalli di troia in Cassazione*, cit., 94; MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, cit., 198

[81] In questo senso, ad esempio, IOVENE, *Le c.d. perquisizioni online*, cit., 336 e MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, cit., 198.

[82] Il riferimento è, ovviamente, alle cosiddette "sentenze gemelle": Corte Cost., 24 ottobre 2007, n. 348, in *Giur. cost.*, 2007, 3475 ss., con nota di PINELLI, *Sul trattamento giurisdizionale della CEDU e delle leggi con essa confliggenti*; Corte cost., 24 ottobre 2007, n. 349, *ivi*, 2007, 3535 ss., con nota di CARTABIA, *Le sentenze "gemelle": diritti fondamentali, fonti, giudici*, confermate negli anni successivi da una granitica giurisprudenza costituzionale; si vedano, *ex multis*, Corte Cost., 27 febbraio 2008, n. 39; Corte Cost., 26 novembre 2009, n. 311; Corte Cost., 4 dicembre 2009, n. 317; Corte Cost., 14 aprile 2010, n. 138; Corte Cost., 28 maggio 2010, n. 187; Corte Cost., 4 giugno 2010, n. 196; Corte Cost., 11 marzo 2001, n. 80; Corte Cost., 7 aprile 2011, n. 113; Corte Cost., 23 luglio 2015, n. 184; Corte Cost., 13 dicembre 2017, n. 263; Corte Cost., 2 marzo 2018, n. 43; Corte Cost., 29 maggio 2020, n. 102.

[83] Insistono sul richiamo all'art. 8 della Convenzione anche FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., 125 ss., e LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *Dir. pen. cont.*, 7 ottobre 2016, 15 ss.

singoli di fronte al ricorso massiccio alle più intrusive tecnologie investigative a disposizione delle procure è conclusione di cui è legittimo dubitare almeno per due ragioni.

Anzitutto, è noto che il significato della "previa previsione di legge" richiesta dalla Convenzione per l'adozione di misure restrittive dei diritti ivi sanciti assume nel sistema convenzionale contorni molto più sfocati rispetto al concetto di riserva di legge tipico di un ordinamento, come quello italiano, di *civil law*. Secondo la granitica interpretazione della Corte europea dei diritti dell'uomo – e non potrebbe essere altrimenti viste la molteplicità e le fisiologiche differenze degli ordinamenti giuridici che aderiscono alla Convenzione – per previsione di legge deve intendersi un fondamento normativo certo, conoscibile e prevedibile che non necessariamente si identifica nella legge formale[84], potendo coincidere anche con il diritto non scritto, ivi incluso quello giurisprudenziale[85]. Si sarebbe, dunque, dinanzi a una garanzia molto più attenuata di quella sancita dagli artt. 13 ss. Cost.[86]

In secondo luogo, e soprattutto, non possono non condividersi i rilievi critici di quanti hanno evidenziato come i meccanismi decisori sottesi alle pronunce della Corte europea dei diritti dell'uomo aventi a oggetto la violazione dei diritti sanciti dalla Convenzione siano sempre più improntati a logiche "sfocate e polivalenti"[87], alla stregua delle quali anche una marchiana violazione dei diritti sanciti dalla Convenzione viene giudicata sostanzialmente irrilevante sol che, sulla scorta di un'operazione fortemente

---

[84] Come è stato osservato, possono, addirittura, venire in considerazione disposizioni contenute in atti di rango sub-legislativo, così come anche le disposizioni contenute in accordi internazionali applicabili nell'ordinamento interno (Corte e.d.u., 28 marzo 1990, app. n. 10890/84, Groppera Radio AG e a. vs Svizzera, parr. 65-68), MORI, *Il principio di legalità e il ruolo del giudice comune tra Corte costituzionale e Corti europee*, in *Dir. un. eur*., 2018, 1, 100.

[85] Corte e.d.u., 26 aprile 1979, app. n. 6538/74, Sunday Times vs Regno Unito, par. 49; Corte e.d.u., 13 luglio 1995, app. n. 18139/91, Tolstoy Miloslavsky vs Regno Unito, par. 37.

[86] Paradigmatica un'importante pronuncia della Corte europea dei diritti dell'uomo, relativa proprio alle forme di sorveglianza occulta, nella quale, con riferimento al requisito della prevedibilità della restrizione delle prerogative tutelate dalla Carta, si legge che «As regards the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out exhaustively, by name, the specific offences which may give rise to interception. However, sufficient detail should be provided on the nature of the offences in question […] The Court has previously found that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance», Corte e.d.u., 4 dicembre 2015, app. n. 47143/06, Zakharov vs. Russia, parr. 244 e 247.

[87] CAPRIOLI, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, in AA.VV., *Dimensione tecnologica e prova penale*, Giappichelli, a cura di Luparia, Marafioti e Paolozzi, 2019, 47.

discrezionale, la Corte ritenga integrato il vago requisito della "complessiva equità del processo"[88].

Alla luce di ciò, ancorché, come si vedrà[89], i principi elaborati dai giudici di Strasburgo in materia di limiti alla compressione del diritto alla vita privata rappresentino un'utile guida nella prospettiva della futura regolazione della materia, affidare la definizione delle garanzie interne esclusivamente alle mutevoli prospettive ermeneutiche consolidatesi in relazione ai diritti sanciti nella relativa Convenzione appare sconsigliabile.

È, infatti, sul piano della normativa interna che una parte cospicua della dottrina si è particolarmente soffermata al fine di rinvenire una matrice costituzionale appropriata alla tutela delle prerogative emergenti dal ricorso ormai sistematico ai mezzi tecnologici in funzione di ricerca della prova, propugnando un'interpretazione evolutiva dell'art. 14 Cost. che, sancendo l'inviolabilità del domicilio, parrebbe prestarsi a una lettura che estenda l'area del costituzionalmente tutelato anche a proiezioni "virtuali" dello stesso. In questo senso, si è sostenuto che si può «ben dire che esista ormai anche una proiezione informatica dell'individuo, destinata ad allargare i confini del diritto all'intimità della vita privata e al rispetto della dignità personale: un nuovo ed ulteriore spazio virtuale al cui interno – esattamente come nel domicilio e nei circuiti comunicativi riservati – ciascuno deve essere in grado di manifestare e sviluppare liberamente la propria personalità, al riparo da occhi e orecchi indiscreti»[90].

---

[88] Per tutti, si veda MAZZA, *Legge e potere*, cit., 10, che parla, con riferimento alle garanzie processuali di cui all'art. 6 della Convenzione, di una logica *fuzzy*, «che non distingue più nettamente fra bianco e nero, ma si muove su un terreno fatto di grigi, di concetti sfumati che si prestano a giustificare qualsiasi decisione dettata dall'opportunità politica del caso. Pur in presenza di un regolamento scritto di diritti perfetti contenuto nell'art. 6 CEDU, la giurisprudenza di Strasburgo giunge così a enucleare una serie di diritti imperfetti che scolorano nell'unico vero diritto, dai contorni tuttavia indistinti, quello all'equità complessiva del processo».

[89] Cfr. cap. 3, par. 4.1.2.

[90] CAPRIOLI, *Il "captatore informatico" come strumento di ricerca*, cit., 489-490, il quale evidenzia altresì come la correttezza di tale conclusione sia comprovata dall'inserimento, nel codice penale, delle fattispecie di reati informatici nella sezione quarta del libro secondo del codice, dedicata ai delitti contro l'inviolabilità del domicilio. Per la stessa conclusione, si vedano ALONZI, *L'escalation dei mezzi di intrusione nella sfera privata: ripartire dalla Costituzione,* in *Rev. bras. dir. proc. pen*., 2019, 5, 1436, CAMON, *Cavalli di troia in Cassazione*, cit., 95; SIGNORATO, *Le indagini digitali*, cit., 49 ss.; TROGU, *Le indagini svolte con l'uso di programmi spia (trojan horses),* in AA.VV., *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di Internet*, a cura di Flor, Falcinelli e Marcolini, ed. DipLap, 2015, 68, il quale, però, evidenzia come in caso di sorveglianza penetrante per il tramite del captatore a venire in rilievo è anche un altro bene giuridico, rappresentato dalla riservatezza informatica, che avrebbe senz'altro rango costituzionale (sul punto, vedi anche *infra*). Da ultimo, in merito alla necessità di riconoscere l'esistenza di nuovi beni giuridici meritevoli di tutela, si vedano gli interessanti rilievi di FLOR, *Le indagini ad alto contenuto tecnologico*, cit., 147 ss., che evidenzia come la

Una simile lettura è, tuttavia, tutt'altro che incontroversa. Non è mancato, infatti, chi ha rilevato come il riferimento al domicilio sia riduttivo se non, addirittura, fuorviante in quanto mentre il concetto di domicilio richiama l'esistenza di uno spazio che è esso stesso oggetto di tutela, l'interesse all'uso riservato dei sistemi informatici prescinde dal luogo nel quale il dato si trova e dallo strumento di comunicazione prescelto dal fruitore del sistema[91].

Allo stesso modo, si è evidenziato come non sia percorribile neppure una distinzione tra dati riservati e non riservati ai fini dell'individuazione di una copertura costituzionale: gli strumenti digitali di uso comune, infatti, contengono una pluralità di dati e informazioni di varia natura, rispetto ai quali non è sempre realizzabile un accesso selettivo. Ne deriva che anche l'acquisizione di dati non strettamente riservati e, dunque, apparentemente meritevoli di forme più blande di tutela può, in realtà, comportare una grave lesione delle prerogative individuali, soprattutto laddove si tenga conto della possibilità di mettere i dati acquisiti in collegamento tra loro e tracciare, così, una panoramica complessiva della personalità del loro titolare[92].

In definitiva, non avrebbe più senso distinguere, in un sistema informatico, tra dati e informazioni riservate e non. L'aspettativa di riservatezza si estenderebbe al sistema nel suo insieme, da intendersi però non già come spazio, sia pure "virtuale", dotato di confini propri, ma come complesso di dati e informazioni in ordine al quale l'individuo ha un'aspettativa di riservatezza, a prescindere dal luogo nel quale si trovano, nella misura in cui gli stessi assurgono a strumento di manifestazione della sua personalità e, dunque, del diritto all'autodeterminazione dell'individuo.

---

tutela dei sistemi informatici di uso comune stia passando da una dimensione privata a una dimensione collettiva, con la conseguenza esigenza di riconoscere, quale nuova oggettività giuridica, anche quella della cosiddetta "*cybersecurity*", di cui l'autore delinea i contenuti.

[91] In tal senso, si vedano FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., 123; IOVENE, *Le c.d. perquisizioni on line*, cit., 335; PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in AA.VV., *Il diritto penale dell'informatica nell'epoca di Internet*, a cura di Picotti, Cedam, 2004, 80, secondo il quale «il parallelismo con il domicilio, bene eminentemente privato e personale, coglie solo parzialmente il contenuto dell'interesse all'esclusione di terzi da determinate "sfere di disponibilità e rispetto", create e rese fruibili dalla tecnologia informatica». Nello stesso senso, ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Arch. pen. web*, 25 luglio 2016, per il quale «le perquisizioni *on-line* non minacciano né il domicilio (non c'è intrusione fisica), né la libertà e segretezza delle comunicazioni (spiare fra i documenti contenuti sull'hard disk di un pc è cosa diversa dal controllare il flusso di corrispondenza o attentare alla segretezza di una comunicazione in atto)».

[92] IOVENE, *Le c.d. perquisizioni on line*, cit., 334.

Tale ricostruzione coglie un aspetto particolare della questione che occupa, creando un collegamento ideale tra il diritto del quale si cerca di definire la base costituzionale e il diritto all'autodeterminazione tutelato dall'art. 13 Cost.[93], che viene in risalto in quanto i nuovi strumenti informatici sono suscettibili di assumere i contorni di una vera e propria «propaggine dell'io»[94], se solo si considera che attraverso gli stessi è possibile ricostruire i più reconditi moti interiori dell'individuo[95], acquisendo finanche informazioni che egli ha deciso di non rivelare a terzi[96].

Occorrerebbe, dunque, prendere atto dell'esistenza di un nuovo bene giuridico, meritevole di protezione costituzionale e consistente in una sorta di nuova ramificazione del diritto alla riservatezza, che non potrebbe dirsi, in questo specifico ambito, limitato all'originario e restrittivo concetto di *right to be let alone*, ma acquisirebbe i contorni di un diritto al controllo dei dati, slegato dall'individuazione di qualsivoglia limite spaziale o relativo alla natura dei dati medesimi[97]. Tanto anche sulla scorta di quanto già sperimentato in altri ordinamenti giuridici[98].

---

[93] Come noto, benché l'articolo 13, comma 4, Cost. menzioni la libertà personale e non morale dell'individuo, tuttavia è anche a quest'ultima che la norma accorda tutela. La condizione di limitazione della libertà personale è semplice presupposto della tutela approntata dalla disposizione (VASSALLI, *Il diritto alla libertà morale (contributo alla teoria dei diritti della personalità)*, in AA.VV., *Studi giuridici in memoria di Filippo Vassalli*, Utet, 1960, 1641). Sul punto, si veda anche TAORMINA, *Narcoanalisi*, in *Enc. dir.*, vol. XXVII, 1977, secondo il quale ancorché la Costituzione non la menzioni mai espressamente, tuttavia «la libertà morale è un valore che aleggia in tutta la normativa costituzionale sulle libertà ed è vero che queste la rafforzano […] perché (essa) costituisce il presupposto dal quale tutte le altre si dipartono e sono sovrastate». Più recentemente, FANUELE, *La libertà personale*, in AA.VV., *Processo penale e Costituzione*, a cura di Dinacci, Giuffrè, 2010, 213 ss.

[94] CONTI, *Sicurezza e riservatezza*, cit., 1574

[95] D'altronde, la Corte Costituzionale, in un caso, ha ricondotto alla prerogativa della libertà personale addirittura la tutela degli oggetti ed agli accessori che gli individui portano abitualmente con loro, come borse o portafogli, considerandoli alla stregua di appendici della persona (Corte Cost., 31 marzo 1987, n. 88.)

[96] Si pensi, ad esempio, a un messaggio che viene digitato sullo schermo di un telefono cellulare ma successivamente cancellato prima dell'invio. O ancora, alle note e agli appunti che possono essere salvati sul medesimo. Sullo stesso piano, le considerazioni di DANIELE, *La prova digitale nel processo penale,* cit., 288. Si vedano anche le considerazioni di PARLATO, *Libertà della persona nell'uso delle tecnologie digitali*, cit., 292, che parla, efficacemente, della «necessità di "essere" tramite la rete».

[97] TROGU, *Le indagini svolte con l'uso di programmi spia (trojan horses),* cit., 68; si veda anche IOVENE, *Le c.d. perquisizioni on line*, cit., 334. Secondo DANIELE, *La prova digitale nel processo penale,* cit., 288, «quale che sia la veste formale individuata, ciò che conta è la sostanza delle cose: si configura inequivocamente un bene giuridico dotato di un rango quanto meno equiparato a quello dell'inviolabilità del domicilio e della segretezza delle comunicazioni, se non addirittura superiore, ove si ritenga di attribuire ad esso lo statuto di un vero e proprio bene-presupposto per il godimento degli altri. E il cuore pulsante dell'istanza individuale in oggetto è la somma, inaccessibile – e vorremmo aggiungere indisponibile – intimità dell'Io. Il fatto che ci si trovi dinanzi ad un bene giuridico le cui esigenze di tutela sono emerse "dopo", in ragione dell'idoneità aggressiva della tecnologia, non incide - sotto un profilo assiologico - sul rango primario e sulla assolutezza di sapore giusnaturalistico di tale istanza».

[98] Nel febbraio 2008, ad esempio, il Tribunale Costituzionale federale tedesco (*Bundesverfassungsgericht*), BVerfG, NJW 2008, 822, ha espressamente riconosciuto l'esistenza di un

Volendo riassumere e tentando di semplificare, secondo le tesi appena riportate i diritti fondamentali già sanciti dalla Costituzione e sopra richiamati, espandendosi ed evolvendo conformemente ai profondi mutamenti tecnologici e sociali occorsi negli ultimi anni, sarebbero suscettibili di configurare un nuovo diritto alla riservatezza informatica. Una simile prerogativa, tuttavia, se per un verso non è sancita espressamente dalla nostra Costituzione, per altro verso non sembra neppure semplicemente riducibile ai diritti costituzionali espressamente previsti singolarmente considerati (artt. 2, 13, 14,15 e 16[99] Cost.), in quanto ciò equivarrebbe a scinderla in una serie di componenti differenziate insuscettibili di rendere conto della consistenza, tutto sommato unitaria, di tale "nuovo" bene giuridico. Tanto, quanto meno, laddove l'intrusione nella sfera intima del singolo avvenga tramite il ricorso a metodiche di indagine che consentono un controllo "a tappeto" sulle attività, sugli spostamenti, sulle comunicazioni e, in generale, su tutti gli aspetti della quotidianità dell'individuo. Dinanzi a intrusioni di tale intensità, l'estensione dei diritti fondamentali in considerazione dovrebbe convergere verso la creazione di un diritto nuovo, che non rappresenta una semplice sommatoria delle prerogative individuali tradizionali ma che assume un significato e una portata inediti.

Una simile conclusione, però, presuppone una rigorosa riflessione su quale debba essere il rango di un simile diritto e, conseguentemente, su quali siano le guarentigie costituzionali a tutela della sua integrità. È una questione, quella appena delineata, che non pare possa risolversi, in maniera del tutto assertiva, facendo perno sull'ovvia percezione che un simile diritto meriti le più ampie tutele accordate dalla Costituzione ai diritti sanciti dagli artt. 13 ss., da rinvenirsi nella riserva di legge e di giurisdizione. Occorre, invece, domandarsi se, sostenendo che tale diritto promani da prerogative

---

nuovo diritto fondamentale alla integrità e riservatezza dei sistemi tecnologici d'informazione quale nuovo diritto della personalità e ha, di conseguenza, individuato i requisiti minimi per una sua compressione. La pronuncia ha segnato l'ultima, importante tappa di un percorso avviato già negli anni '80, quando, con una decisione del 15 dicembre 1983, il medesimo Tribunale Costituzionale aveva riconosciuto l'esistenza, tra i diritti fondamentali dell'uomo, di un diritto alla libera disponibilità dei dati personali. Allo stesso modo, la Corte Suprema dell'Oregon, nel caso State vs. Campbell, 759 P.2d 1040, 1998, ha affermato l'esistenza di un diritto costituzionale alla libertà dallo scrutinio degli strumenti tecnologicamente avanzati nella vita privata degli individui.

[99] Che viene senz'altro in rilievo, quanto meno, in relazione all'attività di pedinamento realizzabile tramite i nuovi strumenti tecnologici in argomento. Si è, infatti, persuasivamente sostenuto che la consapevolezza del rischio di essere sottoposti a un monitoraggio sistematico degli spostamenti potrebbe avere l'effetto di limitare in concreto l'esercizio del diritto tutelato dalla norma costituzionale, CAMON, *L'acquisizione dei dati sul traffico di comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, 2, 634.

costituzionali per le quali è prevista la riserva di legge e di giurisdizione, si ottenga l'effetto di estendere allo stesso tali guarentigie, ovvero se, trattandosi, comunque, di un diritto nuovo e non tipizzato dalla Costituzione, lo stesso confluirebbe nell'ambito applicativo dell'art. 2 Cost., essendo così assoggettato a una disciplina più blanda in termini di tutela. La soluzione al quesito non può prescindere da un'analisi, sia pur succinta, della tematica relativa all'emergere di nuovi diritti fondamentali, da tempo al centro di un acceso e interessante dibattito tra gli studiosi del diritto costituzionale.

3.2. "Vecchi" e "nuovi" diritti: il dibattito sull'enucleazione dei nuovi diritti fondamentali.

Il dibattito sulla enucleazione di nuovi diritti fondamentali è risalente ed è stato caratterizzato dall'emergere, nella dottrina costituzionalistica italiana, di una pluralità di posizioni rispetto alle quali, come si vedrà, la Corte costituzionale non sembra aver raggiunto alcun approdo definitivo.

Escludendo una revisione costituzionale e ragionando *de iure condito*, le possibili alternative[100] rispetto all'emersione di nuovi diritti costituzionali, non espressamente sanciti dalla Carta, sono le seguenti: una interpretazione evolutiva dei diritti esistenti; l'aggancio all'art. 2 Cost., quale fonte aperta suscettibile di generare nuovi diritti; la valorizzazione di norme sovraordinate di matrice europea, come quelle della Convenzione europea dei diritti dell'uomo e della Carta di Nizza[101].

Con specifico riguardo al diritto europeo, è stato osservato come esso abbia rappresentato, soprattutto negli ultimi anni, un non trascurabile fattore di tensione verso un catalogo "aperto" dei diritti fondamentali, in ragione delle pressioni che le fonti sovraordinate esercitano sugli ordinamenti interni per il riconoscimento delle prerogative individuali dei singoli[102]. Nonostante ciò, pare più opportuno impostare l'analisi della complessa questione in esame partendo dal piano interno. Ciò, quanto

---

[100] Per una ricostruzione più dettagliata della questione e delle alternative ermeneutiche emerse nel corso del tempo si veda, per tutti, vedi PACE, *Problematica delle libertà costituzionali, Parte generale*, Cedam, 1990, 20 ss.

[101] ORLANDI, *Usi investigativi dei cosiddetti captatori informatici*, cit., 542.

[102] CARTABIA, *I "nuovi" diritti*, in www.statoechiese.it, 2011, 3, che evidenzia come sia «dalle frontiere europee che provengono le maggiori pressioni sull'ordinamento costituzionale italiano in tema di diritti individuali. E come per la circolazione dei cittadini europei, anche per i diritti individuali le frontiere nazionali sono state gradualmente smantellate, cosicché possiamo dire – con qualche approssimazione, ma senza deformare il quadro nel suo complesso – che oggi qualunque decisione riguardante individuali assunta nelle sedi europee fa stato anche nell'ordinamento nazionale».

meno, per due ragioni, una di ordine metodologico, l'altra di ordine concettuale. Sotto il primo profilo, nel caso in cui si reputasse possibile giustificare l'emersione di nuovi diritti fondamentali facendo leva sugli strumenti giuridici rinvenibili nel diritto interno il richiamo al diritto europeo potrebbe avere l'effetto, semmai, di rafforzare le conclusioni raggiunte ma non risulterebbe pregiudiziale rispetto alla soluzione della questione[103]. Sotto il secondo profilo, si è già visto come la tutela dei diritti fondamentali apprestata dalle fonti europee risulti tendenzialmente edificata su guarentigie formali e procedurali meno solide di quelle apprestate sul piano interno[104].

Torna utile, pertanto, partire dall'analisi delle due principali posizioni sostenute dalla dottrina italiana quanto a enucleazione dei nuovi diritti fondamentali, che paiono così riassumersi: mentre secondo alcuni autori i nuovi diritti fondamentali troverebbero la loro matrice nell'art. 2 Cost., altri escludono tale conclusione e propugnano, piuttosto, una lettura evolutiva dei diritti esistenti quale unica via per il riconoscimento di quelli non espressamente sanciti dalla Carta.

Secondo il primo dei due orientamenti[105], l'art. 2 Cost. accrediterebbe la conclusione che la Carta Costituzionale rappresenti non già un sistema completo e non integrabile di diritti ma, piuttosto, un catalogo aperto. La norma, infatti, per la sua peculiare e ampia formulazione, consentirebbe di recepire le nuove istanze di tutela legate all'evoluzione sociale.

A tale ricostruzione si è storicamente contrapposta quella di chi[106] sostiene, invece, che l'art. 2 Cost. non rappresenti affatto il fondamento teorico di nuovi diritti costituzionali operando, piuttosto, alla stregua di un principio espansivo in relazione a nuovi diritti

[103] Tanto è quanto, d'altronde, finiscono per riconoscere gli stessi sostenitori della necessità di guardare ai diritti sanciti dalle fonti sovraordinate per integrare il quadro interno delle garanzie in materia riconoscono. Si veda, ad esempio, MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, cit., 199, il quale, a proposito dell'art. 8 della Convenzione europea dei diritti dell'uomo, specifica che «così declinato, il parametro convenzionale – fonte interposta della lettura costituzionale – arricchisce di contenuto l'art. 14 Cost., consentendo di avvalorare l'idea di una doppia riserva, di legge e di giurisdizione, in riferimento ai casi e alle modalità di compressione del diritto alla riservatezza informatica».

[104] Cfr. par. precedente.

[105] In dottrina autorevolmente sostenuto da BARBERA, *Commento all'art. 2 della Costituzione*, in *Commentario della Costituzione*, a cura di Branca, Zanichelli, 1975, 65 ss.

[106] BALDASSARRE, *Diritti inviolabili (1989)*, ora in *Diritti della persona e valori costituzionali*, Giappichelli, 1997, 61. Sulla stessa posizione BARILE, *Diritti dell'uomo e libertà fondamentali*, Il Mulino, 1984, 56.

fondamentali la cui matrice, però, deve essere rinvenuta nei diritti già enumerati dalla Carta[107].

Dal canto suo, la Corte costituzionale non ha mai espresso una soluzione univoca[108].

In alcune prime pronunce, la Consulta pare aver mostrato adesione alla tesi non estensiva dell'art. 2 Cost. dichiarando l'inesistenza dei diritti non espressamente sanciti dalla Carta di volta in volta invocati alla stregua di parametri di costituzionalità nelle ordinanze di rimessione[109].

Al contrario, in altre decisioni, la Corte sembra aver riconosciuto nell'art. 2 Cost. una matrice di tutela di diritti "nuovi", pur senza, tuttavia, aderire completamente alla tesi della fattispecie "aperta" della disposizione in argomento. Tant'è, ad esempio, quanto sembra emergere dalla lettura della sentenza del 14 aprile 2010, n. 138, in tema di equiparazione dell'unione omosessuale a quella eterosessuale. Nella pronuncia, infatti, la Corte sembra implicitamente riconoscere la possibilità di interpretare l'art. 2 Cost. alla stregua di una matrice di nuovi diritti costituzionali nella materia oggetto della decisione nella misura in cui tutela le "formazioni sociali" tra cui rientrerebbero unioni omosessuali, evidenziando la necessità di interpretare norme costituzionali tenendo conto delle trasformazioni dell'ordinamento e dell'evoluzione della società e dei costumi. È la stessa Corte, tuttavia, a specificare immediatamente dopo che una simile conclusione non può avere l'effetto d'incidere sul nucleo delle norme costituzionali, modificandole al punto che includano fenomeni e problematiche e non erano stati considerati in alcun modo al momento dell'adozione della Carta[110].

---

[107] Per una posizione critica nei confronti di entrambe le teorie, per come formulate, si veda PACE, *Problematica delle libertà costituzionali,* cit., 20 ss., il quale avversa tanto la tesi della fattispecie "aperta" dell'art. 2 Cost. che quella opposta, che conclude nel senso la norma in questione non rappresenti un fattore di apertura del catalogo costituzionale dei diritti fondamentali.

[108] Per una ricognizione degli orientamenti in materia, si veda CAVALIERE, *Questioni attuali in tema di "nuovi diritti",* in www.dirittifondamentali.it, 2015, 7.

[109] Si vedano, ad esempio, le prime pronunce sull'identità sessuale (Corte Cost., 1° agosto 1979, n. 98, in cui si afferma che «infatti, nella costante interpretazione della Corte, l'invocato art. 2 della Costituzione, nel riconoscere i diritti inviolabili dell'uomo, che costituiscono patrimonio irretrattabile della sua personalità, deve essere ricollegato alle norme costituzionali concernenti singoli diritti e garanzie fondamentali […] quanto meno nel senso che non esistono altri diritti fondamentali inviolabili che non siano necessariamente conseguenti a quelli costituzionalmente previsti»), e sul diritto all'abitazione (Corte Cost., 22 febbraio 1983, n. 252).

[110] «Si deve escludere, tuttavia, che l'aspirazione a tale riconoscimento – che necessariamente postula una disciplina di carattere generale, finalizzata a regolare diritti e doveri dei componenti della coppia – possa essere realizzata soltanto attraverso una equiparazione delle unioni omosessuali al matrimonio. È sufficiente l'esame, anche non esaustivo, delle legislazioni dei Paesi che finora hanno riconosciuto le unioni suddette per verificare la diversità delle scelte operate. Ne deriva, dunque, che, nell'ambito applicativo dell'art. 2 Cost., spetta al Parlamento, nell'esercizio della sua piena discrezionalità,

Talvolta, invece, i Giudici delle Leggi hanno desunto l'esistenza di nuovi diritti fondamentali da diritti già espressamente garantiti nella Costituzione. Ciò, significativamente, è avvenuto proprio in materia di diritto alla riservatezza, con l'importante sentenza del 12 aprile 1973, n. 38, nella quale si afferma che tra i diritti inviolabili dell'uomo rientra senz'altro «quello del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza, intimità e reputazione», il cui riconoscimento viene collegato all'art. 2 Cost. e alla realizzazione delle finalità che lo stesso esprime, ma è altresì direttamente desunto dagli artt. 3 e 13 Cost.

La scelta, sistematicamente operata dalla Corte costituzionale, di non agganciare mai l'emersione di nuovi diritti fondamentali esclusivamente all'art. 2 Cost. ben si spiega alla luce di quello che parrebbe essere il principale inconveniente di una simile impostazione, da ravvisarsi nel fatto che la stessa Consulta sarebbe onerata, in conseguenza della stessa, di un compito complesso e caratterizzato da ampi margini di discrezionalità, consistente nell'individuazione dello statuto di tutela del nuovo diritto. Compito che, a ben vedere, dovrebbe essere appannaggio del legislatore, previa effettuazione dei bilanciamenti opportuni. È stato, d'altronde, autorevolmente evidenziato come l'art. 2 Cost. rappresenti, evidentemente, una norma di principio, priva di specifica disciplina inerente alle garanzie e i limiti connessi al rispetto di quanto nella stessa sancito[111].

Al contempo, neppure soddisfa l'idea di un catalogo "chiuso" dei diritti costituzionali. Infatti, gli stessi detrattori dell'opinione secondo cui l'art. 2 Cost. potrebbe costituire la matrice di nuovi diritti individuali finiscono col convenire sul fatto che occorra pur sempre una lettura aggiornata dei diritti esistenti, generandosi, altrimenti, l'effetto di un'inaccettabile "pietrificazione"[112].

Sembra, allora, da condividere la soluzione di quanti hanno ritenuto che la struttura e la formulazione delle norme costituzionali siano tanto ampie da consentire senz'altro un graduale adattamento della Carta al fisiologico mutamento delle condizioni sociali, in

---

individuare le forme di garanzia e di riconoscimento per le unioni suddette, restando riservata alla Corte costituzionale la possibilità d'intervenire a tutela di specifiche situazioni (come è avvenuto per le convivenze more uxorio: sentenze n. 559 del 1989 e n. 404 del 1988)».

[111] PACE, *Problematica delle libertà costituzionali,* cit., 20 ss. L'autore evidenzia altresì come l'enucleazione di nuovi diritti fondamentali a partire dall'art. 2 Cost. potrebbe avere l'effetto di creare delle antinomie, in quanto all'affermazione di un diritto talora segue l'imposizione di un obbligo a carico di altro soggetto privato, titolare anch'esso di diritti costituzionali.

[112] Lo evidenzia, altresì, PACE, *Problematica delle libertà costituzionali,* cit., 20 ss. MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, Giappichelli, 1995, 2 ss.

modo da apprestare le necessarie tutele per far fronte al rischio di eventuali nuove aggressioni a beni di rilievo costituzionale, non esplicitamente ricompresi nella sua originaria formulazione del 1948[113]. Occorre, dunque, distinguere tra diritti e loro dimensioni di tutela, ben potendo la norma costituzionale, stante la sua struttura, generare nuove forme di tutela dei diritti dalla stessa sanciti, in dipendenza del mutare delle tipologie di aggressione che i medesimi possono subire[114]. Tanto, peraltro, ben può essere l'effetto di quella che è stata efficacemente definita la «composizione in sistema di due o più diritti esplicitamente tutelati dalla Costituzione, con esito "generativo" di un diritto "nuovo"»[115] che, di conseguenza, verrebbe a mutuare lo statuto di tutela di quello dal quale promana.

3.3. Realtà virtuale e "nuovi" diritti costituzionali. La lettura evolutiva del domicilio informatico e il diritto alla riservatezza e all'autodeterminazione nell'uso delle tecnologie informatiche.

Alla luce di quanto appena osservato, appare corretto concludere nel senso che, nella materia che occupa, la tesi dell'esistenza di un diritto fondamentale "nuovo" (nel senso, sopra specificato, di diritto generato dal convergere di altri diritti costituzionali espressamente sanciti, nella loro interpretazione evolutiva) sia tutt'altro che peregrina.

Tentando di individuare i suoi contenuti essenziali e, al tempo stesso, le sue specifiche matrici, non v'è dubbio che un primo fondamentale referente sia costituito proprio dal diritto alla riservatezza, viepiù se si tiene conto della nuova accezione che lo stesso sta assumendo negli ultimi anni per effetto dei mutamenti sociali e tecnologici intervenuti.

È stato autorevolmente osservato[116] che, in conseguenza dell'emergere della nuova dimensione tecnologica, due tradizionali componenti del diritto alla riservatezza – la *privacy* e la protezione dei dati personali – vanno emancipandosi dalla originaria matrice incentrata sulla mera esigenza di tutela dell'intimità per assumere i contorni di una garanzia più complessa, consistente nella necessità di protezione delle informazioni personali e di controllo sui dati che riguardano l'individuo. Per effetto di tale fenomeno,

---

[113] In termini, NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 50.

[114] SILVESTRI, *L'individuazione dei diritti della persona*, in *Dir. pen. cont.*, 27 ottobre 2018, 2, che specifica altresì come, dunque, il carattere di "novità" del diritto fondamentale sia solo apparente.

[115] Ancora, SILVESTRI, *L'individuazione dei diritti della persona*, cit., 6.

[116] RODOTÀ, voce *Riservatezza*, in *Enc. Treccani online*, consultabile sul sito https://www.treccani.it/enciclopedia/riservatezza_res-9e2b210a-9bc7-11e2-9d1b-00271042e8d9_%28Enciclopedia-Italiana%29/.

il termine *privacy* perde la sua originaria accezione di "diritto ad essere lasciato solo"[117] per implicare l'insieme di libertà connesse al trattamento dei dati personali in un contesto socio-culturale caratterizzato dalla tendenza a tradurre in dati suscettibili di trattamento informatico pressoché ogni aspetto dell'esistenza umana[118]. Perde, così, qualsivoglia rilievo, ai fini della minore o maggiore intensità dell'intrusione nell'interesse individuale a mantenere il riserbo sulla propria vita privata, oltre all'ubicazione dei dati, qualsivoglia distinzione tra natura riservata o non riservata di questi ultimi, assumendo carattere preliminare la protezione da accordare alla persona stessa nel suo esprimersi attraverso la tecnologia. In questo senso, si è osservato che tale nuova espressione della "privatezza" non appare *sic et simpliciter* riconducibile alla tutela statica delle comunicazioni e del domicilio, per come tradizionalmente intese[119], venendo piuttosto in rilievo la volontà dell'individuo di escludere gli altri da ciò che gli accade.

Trattasi di osservazioni senz'altro condivisibili. Tuttavia, il diritto alla riservatezza nei termini appena compendiati non pare da solo sufficiente a giustificare la messa a punto di un sistema di garanzie improntato al massimo rigore. Si vuole dire, cioè, che l'atteggiarsi dei poteri di intervento dell'autorità pubblica nella repressione dei reati non può dipendere dalla mera individuazione, da parte del soggetto, di ciò che desidera rimanga privato.

A dispetto di quanto sostenuto da una parte della dottrina, allora, far leva sull'inviolabilità del domicilio informatico pare utile proprio per cogliere appieno l'estensione e il contenuto del diritto di cui si tenta di tracciare i confini: la sua "legittimazione" a essere destinatario di uno statuto di garanzie estremamente rigoroso deriva, invero, proprio dal fatto che l'aspettativa di riservatezza verte su oggetti, cioè dati informatici, tendenzialmente collocati in un "luogo" peculiare, che ben può individuarsi nel domicilio informatico quale "luogo virtuale" di espressione della personalità del singolo. Con ciò non si vuole ipotizzare la necessità di una limitazione della tutela dei dati in dipendenza del luogo nel quale sono inseriti, ma solo evidenziare che ritenere che il domicilio, nella sua accezione di domicilio informatico, sia un "luogo" caratterizzato da precisi confini fissi, sia pur virtuali – e, per l'effetto, escludere

[117] Così come teorizzato da WARREN e BRANDEIS, *The right to privacy*, in *Harvard law review*, 1890.
[118] IOVENE, *Le c.d. perquisizioni online*, cit., 338.
[119] GAITO e FÙRFARO, *Le nuove intercettazioni "ambulanti"*, cit., 313 ss.

che possa farsi leva sullo statuto dell'art. 14 Cost. a tutela delle prerogative di cui si discorre – rappresenta un equivoco fondato su un'impropria sovrapposizione fra il concetto di domicilio informatico e quello di sistema informatico[120], da intendersi alla stregua del complesso di elementi fisici (*hardware*) e virtuali (*software*) che compongono un apparato di elaborazione dati. Fin da tempi risalenti, infatti, la giurisprudenza[121] definisce il sistema informatico alla stregua di una pluralità di apparecchiature deputate a compiere funzioni utili all'uomo tramite il ricorso a tecnologie informatiche. Trattasi, quindi, di un "luogo" rispetto ai quali sono individuabili concreti limiti, tanto reali quanto virtuali.

È ben possibile, invece, interpretare il concetto di domicilio informatico alla stregua di un luogo dai confini "variabili", la cui estensione – e, conseguentemente, quella del diritto dell'individuo che ne è titolare a escludere gli altri – dipende dal mutevole atteggiarsi e moltiplicarsi dei dati[122], concernenti la vita privata del singolo, che sono in esso contenuti. In questo senso, può certamente sostenersi che il concetto di domicilio informatico venga in risalto ogni qual volta si verifichi una intrusione, da parte dell'Autorità Pubblica, in quel "luogo" virtuale contenente una massa indistinta di dati nella titolarità dell'utilizzatore del dispositivo informatico bersaglio dell'attività investigativa.

Deve, nondimeno, convenirsi sul fatto che anche una simile prerogativa – quella del domicilio informatico – non pare idonea a cogliere appieno la natura e l'intensità dell'intrusione nella sfera di riservatezza dei singoli che si trovino a subire non già una intrusione di carattere "istantaneo" nel loro domicilio informatico, ma un assoggettamento a un'attività costante di sorveglianza occulta. Una simile attività, infatti, finisce necessariamente per impattare su aspettative di tutela che trascendono la mera rilevanza del domicilio – sia pur informatico – per attentare alle sfere più intime della personalità.

---

[120] Da intendersi alla stregua del complesso di elementi fisici (*hardware*) e virtuali (*software*) che compongono un apparato di elaborazione dati. La giurisprudenza (fin da tempi risalenti, cfr. Sez. VI, 4 ottobre 1999, n. 3067) definisce il sistema informatico alla stregua di una pluralità di apparecchiature deputate a compiere funzioni utili all'uomo tramite il ricorso a tecnologie informatiche. Trattasi, quindi, di un "luogo" rispetto ai quali sono individuabili concreti limiti, tanto reali quanto virtuali.

[121] Cfr. Sez. VI, 4 ottobre 1999, n. 3067, in *CED Cass*., n. 214946.

[122] In tal senso, anche MANCUSO, *La perquisizione on line*, cit., 421, che evidenzia la «natura mobile, mutevole e mai statica dello stesso domicilio, in ragione dell'estrema portabilità di tecnologie di accesso alla casella postale e agli account di archiviazione dei messaggi ricevuti o inviati e di qualsiasi altro documento o contenitore di informazioni e dati sensibili».

Se così è, rispetto a simili attività non pare peregrino ipotizzare la percorribilità di una lettura evolutiva dello stesso concetto di domicilio informatico, in combinato disposto con la tutela della libertà personale di cui all'art. 13 Cost. È stato, d'altronde, autorevolmente sostenuto che nel panorama dei diritti fondamentali, il diritto all'inviolabilità del domicilio rappresenta la situazione giuridica più connessa alla libertà personale di cui all'art. 13 Cost. in quanto nel domicilio si concretizzano i presupposti per l'estrinsecazione della personalità umana[123].

A sostenere l'esigenza di operare tale lettura estensiva, poi, è proprio il legame privilegiato, già in parte lumeggiato nelle pagine precedenti, tra il domicilio informatico quale proiezione spirituale della persona e il diritto all'autodeterminazione tutelato dall'art. 13 Cost.[124], che non può che estendersi a ogni proiezione, ivi inclusa quella virtuale, della persona umana. Il concetto di libertà personale che la Costituzione definisce inviolabile, d'altronde, è un concetto storicamente e socialmente mutevole, i cui confini sono suscettibili di rimodularsi in ragione, quanto meno, di due fattori: per un verso, l'emergere di nuove modalità di espressione del diritto inviolabile, ulteriori rispetto a quelle che il legislatore Costituente ha espressamente considerato. Per altro verso, e in conseguenza di ciò, l'insorgenza di nuove forme di aggressione al contenuto del diritto inviolabile che implicano, quale corollario della necessità di assicurare una tutela effettiva del medesimo, una reazione uguale e contraria dell'ordinamento, che deve ergersi a tutela di quel diritto quale che sia il suo concreto atteggiarsi in un dato periodo storico o in un dato contesto sociale e tecnologico.

L'uso dei dispositivi digitali è, ormai, tanto radicato nella quotidianità degli individui che ben può dirsi che anche attraverso tali strumenti essi esprimano la loro personalità e tale espressione di libertà deve essere, in via di principio, libera da intrusioni esterne. Da ciò consegue che ogni aggressione segreta ed *ex auctoritate* alla relazione fra individuo e dispositivi informatici è suscettibile di incidere sulla libertà personale del singolo.

---

[123] BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in AA.VV., *Il diritto alla riservatezza e la sua tutela penale, Atti del terzo simposio di studi di diritto e procedura penali*, Giuffrè, 1970, 103.

[124] Si vedano, sul punto, le efficaci considerazioni di PARLATO, *Libertà della persona nell'uso delle tecnologie digitali*, cit., 294, che evidenzia come «frequentemente, ciascuno viene "conosciuto" da altri soggetti, sia pubblici che privati, proprio per mezzo dei dati che lo riguardano. E, se la persona si pone quasi come una "entità disincarnata", sorge l'esigenza di proteggerne il "corpo elettronico", sentendosi il bisogno di una sorta di habeas corpus, nella forma di un habeas data, da considerare come l'evoluzione del nucleo dal quale storicamente si è sviluppata la libertà personale».

Tanto si sostiene non solo in relazione al foro puramente interno, ma altresì in un'ottica relazionale.

Come si è visto precedentemente, la dottrina non ha mancato di evidenziare come la vigilanza indiscriminata della "vita digitale" degli individui possa assumere i contorni di una invasione nella psiche della persona. Con tale conclusione non può che convenirsi per tutto quanto finora argomentato. Alla stessa deve, però, aggiungersi che anche la proiezione, per così dire, esterna della libertà in questione rischia di essere fortemente intaccata: il riconoscimento di un diritto inviolabile, infatti, non ha solo una rilevanza meramente interna, ma presenta sempre anche un rilievo esterno nella misura in cui risulta funzionale a consentire all'individuo quell'appartenenza dinamica e attiva al tessuto sociale che l'art. 2 Cost. mira a presidiare[125]. L'intrusione dell'autorità statale nei dispositivi informatici quotidianamente adoperati dagli individui impatta senz'altro sulle dinamiche relazionali dei medesimi se è vero – e difficilmente può negarsi – che buona parte delle relazioni sociali oggi si svolge sui – o per mezzo dei – dispositivi informatici di uso comune.

In questo senso, le garanzie costituzionali sopra richiamate, nella loro interpretazione evolutiva, convergono verso la creazione di un diritto alla riservatezza e all'autodeterminazione nell'uso delle tecnologie informatiche che, trovando la sua principale matrice negli artt. 13 e 14 della Costituzione, deve reputarsi senz'altro presidiato dalla riserva di legge e di giurisdizione prevista dagli stessi. Tale diritto è certamente suscettibile di venire in considerazione in tutti quei casi in cui l'intrusione dell'Autorità nella sfera di riservatezza del singolo assuma, per il suo carattere perdurante, i contorni di una vera e propria sorveglianza occulta.

[125] TAORMINA, *Narcoanalisi*, cit., 494.

Capitolo II

L'ATTIVITÀ D'INDAGINE ATIPICA

Sommario: 1. La prova atipica; 2. Le condizioni di ammissibilità della prova atipica; 3. Prova atipica e diritti inviolabili: 3.1. Il quadro delineato dalla giurisprudenza costituzionale e di legittimità; 4. Attività d'investigazione atipica incidente sui diritti fondamentali e applicazione dell'art. 189 c.p.p. nella fase delle indagini preliminari; 5. L'intrinseca inadeguatezza dello stato dell'arte in tema di prova atipica con riferimento alle investigazioni *online*.

1. La prova atipica.

Il tema relativo all'impiego, nelle investigazioni penali, di mezzi tecnologici altamente intrusivi della sfera di intimità degli individui risulta inesorabilmente collegato a quello della prova atipica, stante la mancanza di un'apposita disciplina legislativa. Tale vuoto normativo, per un verso, impone di verificare di volta in volta la riconducibilità dei singoli strumenti di indagine ai tipi legali[126]; per altro verso, rende necessario – in caso di esito negativo della verifica testé menzionata – l'attenta disamina delle regole che, nell'attuale sistema processuale penale, presiedono all'impiego, in funzione di accertamento del fatto, di mezzi di prova e di ricerca della prova non disciplinati dalla legge.

È evidente, infatti, che l'operazione esegetica di riconduzione di un dato strumento investigativo alle categorie legali espressamente disciplinate piuttosto che al novero delle prove atipiche implichi non solo che siano esattamente individuati i contorni dell'"atipicità" probatoria – che, nel nostro sistema processuale penale, trova il suo fondamentale referente nell'art. 189 c.p.p. – ma altresì che si verifichi l'effettiva applicabilità di tale ultima disposizione nella fase delle indagini. Tale norma, infatti, regola espressamente l'acquisizione, nel dibattimento, di quelle fonti del convincimento giudiziale non previste dalla legge e rese possibili dall'evoluzione scientifica e tecnologica[127].

[126] Questione che sarà oggetto di precipua analisi nei prossimi capitoli.

[127] ORLANDI, *Atti e informazioni dell'autorità amministrativa nel processo penale*, Giuffrè, 1992, 23, il quale evidenzia come la mancata previsione di tali mezzi di prova sia da ricondurre all'imprevedibilità della loro comparsa sulla scena processuale.

Vigente il codice di procedura penale abrogato e in vista dell'approvazione del nuovo codice, era tema assai discusso se il novero dei mezzi di prova da impiegare nel processo penale dovesse classificarsi come tassativo o se, al contrario, dovesse reputarsi consentito l'impiego di nuovi mezzi di prova che, non prevedibili al momento dell'approvazione del codice di procedura penale, fossero in seguito divenuti esperibili in virtù del processo di costante innovazione che connota ogni campo del sapere scientifico[128].

Al fondo della questione stava, e sta, uno dei nodi nevralgici di qualunque sistema processuale penale, ovvero quello relativo all'individuazione dei modi di formazione del sapere giudiziale in vista dell'accertamento dei fatti, dunque alla stessa funzione cognitiva connaturata al processo penale quale strumento di conoscenza in grado di legittimare la risposta sanzionatoria e l'esercizio del potere allo stesso connaturato[129].

Proprio la preoccupazione che il ricorso alla categoria dell'atipicità potesse rappresentare il viatico per aggirare surrettiziamente i limiti di ammissibilità e le regole di formazione della prova[130] aveva indotto il legislatore, nel progetto di codice di procedura penale del 1978, a sancire il principio di tassatività dei mezzi di prova, in netta discontinuità con l'opzione, poi prevalsa nel codice attualmente vigente, per un sistema, per così dire, intermedio, nel quale la scelta se consentire l'ingresso nella

---

[128] Per la ricostruzione del dibattito relativo all'esistenza di un principio di atipicità probatoria nel precedente sistema processuale, stante l'assenza di una norma parificabile all'attuale art. 189 c.p.p., si veda BOZIO, *La prova atipica*, in AA.VV., *La prova penale*, a cura di Ferrua, Marzaduri e Spangher, Giappichelli, 2013, 58 ss.

[129] BOZIO, *La prova atipica*, cit., 61 ss.; BUZZELLI, *Le letture dibattimentali*, Giuffrè, 2000, 27; DI CHIARA, *Atipicità e sistemi probatori: linee per una fenomenologia generale*, in AA.VV., *Sicurezza e nuove frontiere tecnologiche*, a cura di Militello e Spena, Giappichelli, 2018, 371 ss.; DI BITONTO, *La regola di giudizio nei singoli riti speciali: il ragionamento probatorio*, in *Cass. pen.*, 2022, 3, 1249; FERRUA, *Il giudizio di diritto nel processo penale*, in *Cass. pen.*, 2000, 6, 1829; FERRUA, *Contraddittorio e verità nel processo penale*, in *Studi sul processo penale*, in *Studi sul processo penale, vol. II, Anamorfosi del processo accusatorio*, Giappichelli, 1992, 47 ss.; ZAPPALÀ, *Le garanzie giurisdizionali in tema di libertà personale e di ricerca della prova*, in AA.VV., *Libertà e ricerca della prova nell'attuale assetto delle indagini preliminari*. *Atti del Convegno dell'Associazione tra gli studiosi del processo penale*, Giuffrè, 1995, 53; Sul conoscere giudiziale come esercizio di un potere, per tutti, FERRAJOLI, *Diritto e ragione. Teoria del garantismo penale*, 11a ed., Editori Laterza, 2009, 17 ss. e NOBILI, *La nuova procedura penale*. *Lezioni agli studenti*, Clueb, 1989, 114.

[130] Osserva MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont., Riv. Trim.*, 2013, 3, 6, che «da sempre l'atipicità della prova rappresenta un concetto eversivo della legalità processuale al pari della libertà della prova, del libero convincimento del giudice, inteso erroneamente come possibilità di valutare qualsivoglia elemento conoscitivo a prescindere dal relativo metodo di formazione, o del perseguimento della ricerca della verità, fine superiore che giustifica qualunque mezzo». Sul tema, si vedano anche le considerazioni di NUVOLONE, *Le prove vietate nei paesi di diritto latino,* in *Riv. dir. proc*., 1966, 447, che evidenzia come «l'abbandono del sistema delle prove legali corrisponde a un'esigenza di razionalità, ma il principio del libero convincimento può schiudere la porta all'arbitrio, e quindi all'illegalità».

piattaforma probatoria di risultati di conoscenza ottenuti con mezzi di prova diversi da quelli legalmente previsti è rimessa al giudice[131] che la effettua, però, sulla scorta di parametri legalmente predeterminati. L'art. 189 c.p.p., infatti, dispone che «quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea all'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova».

In tal modo, la scelta di apertura del sistema processuale[132] a strumenti cognitivi inediti è temperata dalla necessità di verificare di volta in volta e in contraddittorio la loro effettiva valenza gnoseologica. Si tratta, dunque, pur sempre di un sistema improntato al principio di legalità della prova in quanto, pur ammettendo prove non disciplinate dalla legge, prescrive specifiche condizioni di ingresso delle medesime nel processo[133].

2. Le condizioni di ammissibilità della prova atipica.

Secondo una ricostruzione largamente condivisa, nell'ambito applicativo dell'art. 189 c.p.p. confluiscono, oltre alla prova autenticamente innominata – cioè quella che non presenta alcun punto di contatto con altri strumenti probatori espressamente previsti – anche quella che risulta dalla contaminazione di altri mezzi di prova tipici ovvero dall'innesto di elementi di atipicità in contesti di prova tipica[134].

Vanno, invece, certamente esclusi dal campo di azione dell'art. 189 c.p.p. gli aspetti di atipicità che non riguardano lo strumento probatorio in sé ma più o meno marcate difformità rispetto allo schema legale dei regimi acquisitivi di strumenti della prova tipici[135]. In termini più generali, può dirsi che non è possibile fare ricorso alla disposizione in argomento al fine di aggirare surrettiziamente i limiti normativi previsti

---

[131] GRIFFO, *Perquisizione informatica… e dintorni*, in *Giur. pen. web*, 2019, 5, 2. MARCOLINI, *Prove atipiche (diritto processuale penale),* in *Enc. Dir. Annali*, vol. X, Giuffrè, 2017, 696, parla di un sistema misto, con "tendenziale tipicità dei mezzi di prova" e "tassatività temperata".

[132] FERRUA, *Ammissibilità della prova e divieti probatori,* in *Rev. Bras. Dir. proc. pen*., 2021, 7, 228.

[133] CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, 2007, 158; DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni unite*, in *Cass. pen.*, 2006, 12, 4372 ss. Significativamente, si è osservato che anche quando è innominata la prova non nasce mai a forma libera, RAFARACI, *Ricognizione informale dell'imputato e (pretesa) fungibilità delle forme probatorie,* in *Cass. pen*, 1998, 6, 1742. In termini, SANTORIELLO, *La legalità della prova*, in AA.VV., *Processo penale e Costituzione*, (a cura di) Dinacci, Giuffrè, 2010, 434.

[134] Si vedano, in questo senso, DOMINIONI, *La prova penale scientifica*, Giuffré, 2005, 93 ss; MARCOLINI, *Prove atipiche (diritto processuale penale)*, cit., 699.

[135] RICCI, *Le prove atipiche*, Giuffrè, 1999, 529.

in materia di prova. Il riferimento, quindi, è non solo alla determinazione delle specifiche modalità di assunzione della prova – restando precluso il ricorso all'art. 189 c.p.p. per procedere all'assunzione di prove tipiche con modalità diverse da quelle previste dalla legge[136] – ma altresì all'esistenza di eventuali divieti probatori.

Su questo crinale si situa la questione interpretativa più delicata posta dalla disposizione in argomento. Com'è evidente, la tenuta del sistema nel suo complesso viene a dipendere dall'individuazione di criteri sufficientemente rigorosi per operare una duplice distinzione: quella tra una prova solo apparentemente atipica e una tipica (ma acquisibile solo secondo le regole già previste dalla legge) e quella tra una prova solo apparentemente atipica ma in realtà vietata (e, dunque, non acquisibile *tout court*). Non sempre questa distinzione appare netta e, anzi, proprio i nuovi mezzi tecnologici di ricerca della prova tendono a situarsi, quasi sistematicamente, su quel crinale.

Diviene, quindi, cruciale l'individuazione di quei criteri distintivi[137] di cui si è appena detto: dinanzi a un dubbio in ordine alla tipicità o atipicità di un mezzo di prova, è necessario, anzitutto, verificare l'esistenza di tratti comuni ad altri istituti già regolati dalla legge. Si tratta di un'operazione simile a quella che presiede all'individuazione della *ratio legis* in caso di interpretazione analogica o alla formulazione di massime di esperienza quando si prendono in considerazione casi simili[138]. Detto altrimenti, deve riscontrarsi una coincidenza ontologica tra lo strumento investigativo la cui tipicità è oggetto di accertamento e quello nominato, in modo che «la disciplina esistente sia idonea a supportare la nuova tecnologia: quest'ultima non deve, cioè, comportarne una deformazione tale da determinare un mutamento qualitativo dell'attività cui le norme fanno riferimento»[139].

Ove, poi, tale valutazione conducesse a un risultato negativo, tale, cioè, da escludere la riconducibilità della prova a una categoria giuridica nota, dovrebbe ulteriormente verificarsi che non si sia dinanzi ad una prova vietata, non potendo, in questo caso, procedersi alla sua acquisizione. In questo senso, si è parlato dell'esistenza, nel nostro

---

[136] GRIFFO, *Perquisizione informatica… e dintorni*, cit., 2.

[137] Sulla necessità di interpretare rigorosamente il disposto dell'art. 189 c.p.p., MARCOLINI, *Prove atipiche (diritto processuale penale)*, cit., 697, secondo il quale tale esigenza è da mettere in diretta correlazione con il principio di legalità che impronta il nostro ordinamento processuale.

[138] CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. e proc*., 2018, 9, 1215.

[139] CONTI, *Sicurezza e riservatezza*, in *Dir. pen. e proc*., 2019, 11, 1585.

sistema, quale corollario del principio di legalità, di un principio di non sostituibilità[140], secondo il quale deve reputarsi vietato l'impiego di una prova, tipica o atipica che sia, finalizzato ad aggirare i limiti e le guarentigie previste dal legislatore in relazione a istituti tipici.

Ancora, però, questo non basta per distinguere, nei casi dubbi, un'attività tipica da una atipica. È evidente, infatti, che per verificare il ricorrere di quel mutamento "qualitativo" di cui si è detto poc'anzi occorre intendersi su quali siano – e come individuarli – gli aspetti "ontologici" di una certa attività istruttoria, al mutamento dei quali segue l'impossibilità di qualificare come tipica quella oggetto del vaglio. Tale attività, peraltro, risulta particolarmente complessa a fronte di misure che, apparentemente, incidono sul medesimo bene giuridico.

Tra le molteplici variabili che possono caratterizzare un certo istituto processuale, così come un determinato mezzo di prova, tre sembrano senz'altro suscettibili di comporre il nucleo "ontologico" di cui sopra: in primo luogo, l'oggetto sul quale l'attività processuale viene a cadere (rispetto al quale non può non cogliersi la stretta correlazione al bene giuridico impattato dall'esecuzione della misura); in secondo luogo, il tipo di attività compiuta sull'oggetto in questione; in terzo luogo, le garanzie apprestate dalla legge a tutela dei diritti incisi dalla misura. In altre parole, l'identificazione di tali variabili consente, anche a parità di bene giuridico inciso da una certa misura processuale, di distinguere i singoli istituti tramite i quali tale restrizione avviene. Così, ad esempio, nel corso del processo penale molteplici sono le attività processuali che, potenzialmente, potrebbero incidere sul diritto di un individuo alla libertà e segretezza delle sue comunicazioni, sancito dall'art. 15 Cost. (si pensi, banalmente, alla distinzione tra un sequestro di corrispondenza e un'attività, ben più intrusiva, di intercettazione), ma ciò che consente di distinguere – su un piano fenomenico e, conseguentemente, su quello giuridico che del primo costituisce necessaria trasposizione – un'attività dall'altra è proprio la combinazione tra queste tre componenti: per un verso, l'oggetto su cui cade l'attività (nel qual caso, restando sull'esempio della distinzione tra sequestro di corrispondenza e intercettazione, è il medesimo, ovvero il dato di natura comunicativa); in secondo luogo, il tipo di attività svolta (che nel caso delle intercettazioni, a differenza

[140] TORRE, *Il captatore informatico, tra riforma Orlando e sistema processuale,* in *Giur. ita*., 2018, 7, 1781; FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma,* in *Proc. pen. e giust.*, 2016, 5, 1215.

del sequestro di corrispondenza, si caratterizza per essere contestuale, segreta e continuativa, sicché l'incidenza sulla prerogativa costituzionale coinvolta è di maggiore intensità ed è, al contempo, più complicato per il soggetto che subisce la misura apprestare forme di reazione alla restrizione dei suoi diritti costituzionali); infine, le garanzie poste dalla legge a tutela del diritto inciso (ben maggiori nel caso dell'intercettazione in conseguenza proprio del differente impatto sulla prerogativa costituzionale coinvolta).

Tenendo presenti tali coordinate, è possibile verificare la riconducibilità di una data attività probatoria rispetto a un certo schema legale tipico. Il tema sarà ripreso nel successivo capitolo, che avrà ad oggetto proprio la riconducibilità dei nuovi strumenti tecnologici di acquisizione della prova da remoto alle categorie legali esistenti. Come si vedrà, ad esempio, la possibilità che certe garanzie previste per gli strumenti tipici possano efficacemente operare anche in relazione alle attività altamente intrusive prese in considerazione è uno di quegli elementi di valutazione imprescindibili per verificare la tipicità o meno dello strumento.

Rinviando, per il momento, alle pagine a seguire per una più approfondita analisi della questione e tornando alla disciplina prevista dall'art. 189 c.p.p., una volta stabilita l'atipicità dello strumento probatorio, il giudice, oltre a valutare, ai fini dell'ammissibilità della prova, la sussistenza degli ordinari requisiti di cui all'art. 190 c.p.p., deve vagliare altresì il ricorrere di due condizioni ulteriori, da ravvisarsi nella mancata incidenza della prova sulla libertà morale delle persone e nella idoneità della stessa all'accertamento del fatto. Al ricorrere di tali presupposti, si può procedere all'ammissione della prova innominata, non prima, però, di aver sentito le parti sulle modalità di acquisizione della medesima.

Tale ultimo adempimento procedurale ha una valenza, quanto meno, duplice[141]: si tratta non solo di apprestare, in ideale continuità con il principio dispositivo, una garanzia di

[141] In termini, si veda FALATO, *Sulla categoria dei mezzi atipici di ricerca della prova e le cd. intercettazioni Gps,* in *Giur. it.,* 2010, 11, 2420, secondo la quale «in termini di legalità del modus operandi scelto dalla parte, da un lato garantisce l'altra parte (quella cioè non richiedente) dai rischi di una procedura non regolata dalla legge — si è detto — consentendo allo stesso giudice di utilizzare, in sede di deliberazione, la prova atipica (art. 526, comma 1, c.p.p.); dall'altra evita che possano essere ammessi mezzi di prova con la procedura dell'art. 189 c.p.p. quando il modello legale è di per sé sufficiente a perseguire il risultato voluto, oppure che la prova atipica possa diventare uno strumento per rendere utilizzabili prove illegittimamente acquisite. Seguendo questa linea di ragionamento, l'organo della giurisdizione rimane il garante della legalità del metodo acquisitivo del mezzo di prova atipico tipizzato dalla parte richiedente».

partecipazione delle parti processuali, ma altresì di assicurare che, proprio grazie allo svolgimento del contraddittorio, si possa vagliare la valenza gnoseologica del mezzo di prova e addivenire all'individuazione delle modalità acquisitive più adeguate perché il mezzo innominato esprima il massimo potenziale euristico. Non v'è dubbio, d'altronde, che le modalità di acquisizione di una data prova sono suscettibili di incidere sul risultato conoscitivo della medesima. È questa la ragione per la quale la legge prevede, in relazione ad ogni mezzo tipico di prova, una specifica disciplina acquisitiva. Basti pensare al divieto di domande suggestive previsto in relazione allo svolgimento dell'esame dall'art. 499 c.p.p., evidentemente volto a evitare che la risposta del dichiarante sia influenzata dal modo in cui la domanda viene posta; o, ancora, alle specifiche regole dettate, dall'art. 213 c.p.p., in materia di ricognizione, finalizzate a vagliare la attendibilità del riconoscimento operato.

A differenza, infatti, di quanto accade in relazione ai mezzi di prova tipici – per i quali l'astratta idoneità all'accertamento dei fatti e le modalità di acquisizione della relativa conoscenza sono già positivamente valutati dal legislatore – il mezzo di prova atipico non è assistito da una medesima "presunzione" di valenza conoscitiva. Pertanto, fino al momento processuale nel quale tale valutazione viene compiuta nel contraddittorio tra le parti, esso non dovrebbe essere reputato alla stregua di una fonte di conoscenza suscettibile di avere "cittadinanza" nel processo. In questo senso, può dirsi che la mancata regolamentazione, ad opera della legge, delle caratteristiche dello strumento probatorio e dei singoli passaggi del procedimento probatorio viene compensata proprio dal sinergico contributo dialettico delle parti.

3. Prova atipica e diritti inviolabili.

Una delle questioni più controverse nel nostro ordinamento in tema di prova e, in particolare, di prova atipica, è se sia ammissibile e utilizzabile una prova atipica che impatti su prerogative costituzionalmente tutelate. Tale questione è stata oggetto di attenzione da parte della dottrina processualpenalistica fin dagli anni '60 del secolo scorso, quando la tematica del contemperamento tra i diritti costituzionali dei singoli e le esigenze di accertamento del fatto di reato iniziò a suscitare sempre maggiore interesse. Si deve all'insegnamento di Vittorio Grevi la definizione di prove incostituzionali con riferimento a quelle risultanze probatorie «ottenute attraverso

modalità, metodi e comportamenti realizzati in dispregio dei diritti fondamentali del cittadino garantiti dalla Costituzione»[142]. Definizione che, certamente, è da mettere in diretta relazione con gli approdi di una importante e nota pronuncia della Corte costituzionale del 1973, nella quale si affermò per la prima volta che i risultati di attività compiute in spregio dei diritti fondamentali dei singoli non possono assurgere a fondamento dell'adozione di atti processuali a carico di chi le abbia subite[143].

Nella vigenza del precedente codice di procedura penale, il dubbio interpretativo relativo alla sorte dei risultati probatori ottenuti tramite violazioni dei diritti fondamentali costituzionalmente sanciti derivava dalla mancanza di qualsivoglia disciplina specifica non solo in tema di prova contrastante con la Carta costituzionale ma, altresì, in tema di inutilizzabilità, istituto che avrebbe fatto la sua comparsa sulla scena processuale con il codice del 1988[144].

Mentre veniva autorevolmente sostenuto[145] che la sorte delle prove assunte in spregio dei diritti fondamentali dei singoli non potesse che essere l'espulsione dalla piattaforma probatoria, ad opera dello stesso giudice, altrettanto autorevolmente[146] si ribatteva che «i precetti costituzionali rappresentano altrettanti paradigmi della normazione attuata in sede legislativa; ma s'incorre in un salto logico, quando si postula che la reazione dell'ordinamento giunga al punto di rifiutare, come processualmente irrilevante, ogni dato conoscitivo conseguito con una condotta difforme da quelle direttive […] se tali prove siano o meno ammissibili, è quesito che esige d'essere risolto in base ad un'interpretazione sistematica delle norme processuali, salvo poi verificare se la disciplina di cui si è ricostruito l'assetto, non confligga con i principi della Costituzione». Vale a dire, cioè, che le norme costituzionali opererebbero solo

---

[142] GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche,* in *Giur. cost.,* 1973, 2, 341.

[143] La pronuncia sarà oggetto di studio *infra*.

[144] Nella vigenza del vecchio codice di procedura penale l'istituto era stato, invero, parzialmente sperimentato tramite l'introduzione di regole particolari in relazione a singoli mezzi di prova, ma non era previsto quale categoria generale di sanzione processuale conseguente alla violazione di qualsivoglia divieto probatorio, com'è attualmente. Si veda PISANI, *Le prove. Appunti sul Titolo I, Libro III, del Progetto di un nuovo codice di procedura penale, Testo della relazione scritta presentata al Seminario sul tema: «Prospettive del nuovo processo penale»,* a cura dell'Istituto Superiore Internazionale di Scienze Criminali (Siracusa, 9-14 gennaio 1978), in *Riv. it. dir. proc. pen*., 1978, 202.

[145] Il riferimento è, ancora una volta, a GREVI, *Insegnamenti, moniti e silenzi*, cit., 341; si vedano anche NUVOLONE, *Le prove vietate nei paesi di diritto latino,* cit., 474; VIGORITI, *Prove illecite e Costituzione,* in *Riv. dir. proc.*, 1968, 64 ss.;

[146] CORDERO, *Prove illecite nel processo penale,* in *Jus*, 1961, 73, poi confluito in CORDERO, *Il procedimento probatorio,* in *Tre studi sulle prove penali,* Giuffrè, 1963.

indirettamente, sicché, ravvisato il contrasto tra un mezzo di prova e la norma costituzionale, l'unico modo per addivenire a un'espulsione del risultato conoscitivo dalla piattaforma probatoria sarebbe una declaratoria di incostituzionalità della norma giuridica sulla base della quale quel risultato è stato ottenuto, non potendo il giudice, *sic et simpliciter*, dichiarare l'inutilizzabilità della prova per contrasto con la Carta Costituzionale.

Il tema ha evidenti affinità con quello delle prove illecite, cioè ottenute sulla base della violazione non già di altra norma processuale, ma di una norma penale sostanziale[147]. Come, però, si è osservato[148], sovrapporre le due questioni equivale a commettere un errore concettuale in quanto nel caso della prova incostituzionale non si è dinanzi a un rapporto orizzontale tra fonti (quella processuale e quella sostanziale), ma a un rapporto verticale alla luce della sovraordinazione gerarchica della fonte costituzionale[149].

Nonostante la complessità della questione, giustamente definita al crocevia tra una concezione "liberista" e una "restrittiva" della prova[150], l'opzione del legislatore del 1988 è stata quella di non intervenire con una regolazione espressa della prova incostituzionale.

Nondimeno, l'introduzione nel nuovo codice di procedura penale di una nuova tipologia di invalidità processuale – l'inutilizzabilità di cui all'art. 191 c.p.p. – ha offerto nuovi

---

[147] Sul tema, per la tesi secondo la quale le prove acquisite in violazione di leggi penali sostanziali sarebbero nondimeno utilizzabili, CAPRIOLI, *Colloqui riservati e prova penale*, Giappichelli, 2000, 232; CORDERO, *Prove illecite nel processo penale*, cit., 1961; GALANTINI, voce *Inutilizzabilità*, in *Enc. dir*., Agg. I, Giuffrè, 1997, 700; GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Cedam, 1992, 213; PERONI, *Prova illegittima e prova illecita: una singolare nozione di inutilizzabilità ex art. 191 c.p.p. (nota a Sez. un., 30/10/02, dep. 21/5/03, n.22327, Carnevale)*, in *Cass. pen.*, 2005, 3, 921; *contra*, CISTERNA, *Sull'irrilevanza probatoria dei nastri illeciti una lettura di merito che non convince*, in *Guid. Dir*., 2006, 38, 73 ss.; MELCHIONDA, *Prove illegali e prove illecite nel futuro del processo penale*, in *Riv. pen*., 1977, 129 ss.; NOBILI, sub *art. 191*, in *Commento al nuovo codice di procedura penale*, a cura di Chiavario, vol. II, Utet, 1990, 413; UBERTIS, *Riflessioni sulle "prove vietate"*, in *Riv. pen*., 1975, 705 ss.; si veda, altresì, NUVOLONE, *Le prove vietate*, cit., 474, il quale, criticando la tesi di Cordero, osserva come l'ordinamento giuridico non sia fatto di compartimenti stagni, sicché gli istituti processuali trovano una loro qualificazione anche in altri rami dell'ordinamento. Per la posizione secondo la quale è possibile rinvenire regole di esclusione direttamente nelle norme costituzionali, che opererebbero direttamente, si veda, più recentemente, MARCOLINI, *Regole di esclusione e nuove tecnologie*, in *Criminalia*, 2006, 1, 419.

[148] CAMON, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove incostituzionali*, in *Cass. pen*., 1999, 4, 1206, fa notare come Cordero impostasse e risolvesse entrambe le questioni (cioè quella della prova illecita e quella della prova incostituzionale) partendo dal rapporto di separazione delle fonti del diritto sostanziale e processuale. Il che, se risolve il problema della prova illecita, non risolve anche quello della prova incostituzionale stante la sovraordinazione della norma costituzionale.

[149] CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, 2007, 152.

[150] CAMON, *Le riprese visive come mezzo di indagine*, cit., 1206.

argomenti a quella parte della dottrina[151] che sostiene la tesi della radicale inutilizzabilità – con il conseguente obbligo del giudice di dichiarare l'invalidità processuale in questione senza dover transitare per una questione di legittimità costituzionale – delle prove ottenute in spregio dei diritti fondamentali.

La disposizione, come noto, sancisce l'inutilizzabilità delle prove acquisite in violazione dei «divieti stabiliti dalla legge». Termine, quest'ultimo, la cui genericità ha fatto immediatamente sorgere l'interrogativo se il riferimento fosse alla sola legge processuale oppure se, data l'ampiezza della formulazione, fosse possibile ricomprendere nel termine altra tipologia di legge, come quella penale sostanziale nonché, ovviamente, la legge costituzionale.

Si è, perciò, sostenuto che, alla luce del *novum* normativo, la soluzione della questione relativa alla prova incostituzionale richiedesse un mutamento di paradigma[152], non implicando più l'analisi – complessa e da svolgere anzitutto sul piano della dogmatica costituzionalistica – della diretta operatività o meno delle norme costituzionali, ma risolvendosi nella interpretazione del termine "legge" adoperato nella disposizione, suscettibile, data la sua ampiezza, di ricomprendere la fonte costituzionale[153].

Un'alternativa, sul piano esegetico, suscettibile di giustificare l'esclusione dal materiale probatorio adoperabile per la decisione dei risultati conoscitivi acquisiti tramite la violazione di diritti fondamentali potrebbe passare, poi, per lo stesso art. 189 c.p.p. È stato, cioè, sostenuto che proprio nella disposizione in parola possa rinvenirsi un limite all'ammissione della prova atipica, nel senso che la stessa, non prevedendo i casi e i modi della restrizione della prerogativa costituzionale, sarebbe strutturalmente insuscettibile di fungere da base legale legittimante la restrizione medesima. Detto altrimenti, il divieto di acquisire nel processo risultati conoscitivi di qualsiasi tipo tramite mezzi di prova atipici suscettibili di impattare sui diritti fondamentali dei singoli si dovrebbe rinvenire nella stessa formulazione dell'art. 189 c.p.p. che, non prevedendo – come invece richiederebbe la Carta costituzionale – i casi e i modi della

[151] Cfr. nota 145.

[152] Per tutti, sulla necessità di aggiornare i termini del dibattito in materia di prova illecita in seguito all'introduzione del nuovo art. 191 c.p.p., NOBILI, *La nuova procedura penale*, cit. 157, secondo il quale sarebbe arbitrario interpretare il termine "legge" riportato nella disposizione alla stregua di "legge procedurale".

[153] CAMON, *Le riprese visive come mezzo di indagine*, cit., 1211.

compressione, conterrebbe un limite implicito all'acquisizione della prova[154] o, meglio, una condizione di ammissibilità implicita.

Come si vedrà a breve, la stessa giurisprudenza di legittimità pare, da ultimo, assestata su una posizione similare.

3.1. Il quadro delineato dalla giurisprudenza costituzionale e di legittimità.

Per quanto si sia sostenuto, in dottrina, che la categoria dell'incostituzionalità della prova rappresenti un punto fermo nel nostro ordinamento[155], la disamina delle pronunce della giurisprudenza costituzionale e di legittimità sul tema delle prove atipiche incidenti sui diritti fondamentali degli individui consente di delineare un quadro solo apparentemente stabile e coerente degli approdi ermeneutici raggiunti.

L'analisi non può che partire dalla pronuncia della Corte costituzionale del 6 aprile 1973, n. 34[156], avente ad oggetto una questione di legittimità costituzionale dell'allora vigente art. 226 c.p.p. che, consentendo l'intercettazione di comunicazioni telefoniche, si sarebbe, a parere del giudice *a quo* posto in irrimediabile contrasto con gli artt. 15 e 24 Cost., realizzando un sostanziale aggiramento della facoltà, riconosciuta dall'art. 78 del codice allora vigente al soggetto sospettato della commissione del reato, di non rispondere agli interrogatori degli inquirenti.

---

[154] CONTI, *Accertamento del fatto e inutilizzabilità*, cit., 153 ss., che evidenzia altresì come l'interpretazione secondo la quale il termine «legge» di cui all'art. 191 c.p.p. sarebbe suscettibile di ricomprendere anche la Costituzione abbia carattere altamente discrezionale e sia in apparente contrasto con lo stesso tenore letterale della disposizione. Quanto alla ricostruzione riportata nel testo, l'autrice evidenzia, a sostegno della medesima, come tra due possibili interpretazioni di una norma debba essere scelta quella compatibile con la Carta fondamentale, specificando altresì che la medesima soluzione si impone anche con riferimento agli atti di indagine atipici, anche nel caso in cui si reputi, in relazione ai medesimi, inoperante l'art. 189 c.p.p. In quest'ultimo caso, il divieto di ammissione della prova dovrebbe desumersi dal combinato disposto degli artt. 55 e 348 c.p.p., norme che, al pari dell'art. 189 c.p.p., non prevedono i casi e i modi della compressione del diritto fondamentale e vietano, dunque, implicitamente la realizzazione di atti suscettibili di comportarne la restrizione.

[155] COMOGLIO, *L'inutilizzabilità "assoluta" delle prove "incostituzionali",* in *Riv. dir. proc*., 2011, 1, 43. Secondo l'autore, peraltro, la categoria sarebbe «sicuramente operante anche in quei processi (ad es., civile, amministrativo e tributario), nei quali manchi una previsione generale assimilabile all'art. 191 c.p.p. – è stato più volte affermato e ribadito dalla Corte costituzionale. Si è sottolineato, infatti, che, pur in assenza di «specifiche norme processuali», la protezione costituzionale dei beni fondamentali della segretezza e della privacy delle comunicazioni interpersonali sia tale, da imporsi di per sé, mediante corrispondenti (ed impliciti) divieti probatori, in qualsiasi tipo di processo, per effetto di previsioni direttamente precettive e vincolanti».

[156] Corte Cost., 6 aprile 1973, n. 34, in *Giur. Cost*., 1973, 338.

Nella pronuncia in commento la Corte, pur escludendo qualsivoglia violazione della normativa costituzionale invocata dal giudice di merito[157], evidenziava, con parole che vale la pena di riportare testualmente, che «il principio enunciato dal primo comma della norma costituzionale [n.d.r., art. 15 Cost.] sarebbe gravemente compromesso se a carico dell'interessato potessero valere, come indizi o come prove, intercettazioni telefoniche assunte illegittimamente senza previa, motivata autorizzazione dell'autorità giudiziaria. Se ciò avvenisse, un diritto "riconosciuto e garantito" come inviolabile dalla Costituzione sarebbe davvero esposto a gravissima menomazione. A questo proposito la Corte sente il dovere di mettere nella dovuta evidenza il principio secondo il quale attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito».

Il carattere solenne dell'affermazione contenuta nella pronuncia non sembra, però, giustificare conclusioni altrettanto nette quanto all'esatta portata delle conseguenze, sul piano processuale, della situazione di contrasto ipotizzata dalla Corte (in termini, peraltro, meramente teorici vista l'esclusione di qualsivoglia profilo di illegittimità costituzionale della normativa oggetto dello scrutinio). È evidente, infatti, che affermare, in via di principio, che i risultati di attività compiute in spregio di diritti fondamentali dei singoli non possano assurgere a fondamento di atti processuali a carico di chi le abbia subite non equivale ancora a postularne l'inutilizzabilità, sul piano probatorio, pronunciabile dallo stesso giudice in assenza di qualsivoglia pronuncia di illegittimità costituzionale. Una simile soluzione, invero, sarebbe dovuta transitare per un'esplicita presa di posizione della Corte in merito a due complesse questioni, entrambe oggetto di ampie disquisizioni dottrinali in quegli anni e ancora ben lungi dal trovare una sistematizzazione precisa tanto sul piano giurisprudenziale, quanto su quello normativo. Il riferimento è, per un verso, al carattere "*self-executing*" o meno della normativa costituzionale a tutela dei diritti fondamentali; per altro verso, alla configurabilità, nel sistema processuale penale all'epoca vigente, di una forma di invalidità assimilabile a quella oggi prevista dall'art. 191 c.p.p.

[157] Il principale argomento adoperato dalla Corte faceva leva sulla non pertinenza del richiamo alla garanzia del diritto di difesa, in collegamento con la facoltà di serbare il silenzio dinanzi agli investigatori, alla ipotesi di indagine effettuata col mezzo delle intercettazioni telefoniche, operando la garanzia del diritto al silenzio solo con riferimento alla situazione dell'interrogatorio.

Sotto il primo profilo, si è già accennato precedentemente al fatto che proprio la questione relativa alla possibilità, per il giudice penale, di far leva sulla norma costituzionale al fine di espellere dal quadro probatorio i risultati probatori ottenuti in contrasto con i diritti sanciti dalla Costituzione, al cuore del dibattito sviluppatosi negli anni '70 a proposito della controversa categoria della prova incostituzionale, fosse legata a doppio filo a un'altra questione – quella della diretta applicabilità della norma costituzionale da parte del giudice ordinario – tutt'altro che incontroversa, quanto meno al tempo dell'emissione della pronuncia in commento.

È noto che la questione relativa alla diretta applicabilità o meno delle norme costituzionali è strettamente connessa a quella del carattere precettivo o programmatico delle disposizioni costituzionali e, in definitiva, della loro natura normativa. Tale ultimo tema fu oggetto proprio della prima pronuncia della Corte costituzionale, la n. 1 del 1956, nella quale, però, si discuteva di una sola delle specifiche implicazioni della questione, quella attinente alla forza abrogativa delle regole costituzionali su norme primarie con esse contrastanti, con la conseguente possibilità del giudice ordinario di dichiarare il contrasto e l'avvenuta abrogazione della norma primaria. Nella sentenza in questione, la Corte assunse una netta posizione nel senso della natura schiettamente normativa dei precetti costituzionali, che rappresentano parte integrante dell'ordinamento giuridico. Secondo un'autorevole dottrina, tuttavia, avrebbe nondimeno lasciato impregiudicato l'interrogativo se il contrasto con la Costituzione potesse comportare l'abrogazione della legge piuttosto che, sempre e solo, la sua incostituzionalità[158]. Vero è che anche l'obbligo del giudice di fornire un'interpretazione conforme alla carta costituzionale altro non è se non una forma di applicazione diretta della medesima[159]. Nondimeno, la diretta applicabilità invocata con riferimento all'espulsione di una prova dalla piattaforma probatoria per contrasto con la Costituzione avrebbe postulato il riconoscimento in capo al giudice di un potere ben più incisivo di quello che si manifesta nell'interpretazione conforme, in quanto la sua conseguenza applicativa (l'espulsione della prova) deriverebbe non già dalla interpretazione e dalla "applicazione conforme" della norma primaria (e solo

[158] CRISAFULLI, *Incostituzionalità o abrogazione?*, in *Giur. cost.* 1957, 271 ss.

[159] si veda, per tutti, BIN, *L'applicazione diretta della Costituzione, le sentenze interpretative, l'interpretazione conforme a Costituzione della legge*, testo provvisorio della relazione svolta al convegno AIC 2006, in www.astridonline.it.

indirettamente di quella costituzionale), ma dall'immediata applicazione di quella costituzionale per trarne specifiche conseguenze sul piano processuale. Che ciò fosse ammissibile, al momento dell'emissione della pronuncia del 1973, era tutt'altro che pacifico. Con ciò non si vuole negare che vi fossero stati casi in cui la Corte aveva ricavato l'esistenza, in capo al giudice ordinario, del potere di attingere direttamente alle norme costituzionali, anche di principio, per l'attribuzione di diritti ai singoli. A questo proposito, viene generalmente citata dalla dottrina un'importante giurisprudenza della Corte con riferimento al diritto alla giusta retribuzione del lavoratore, di cui all'art. 36 Cost.[160], tema sul quale la Consulta «arrivò ad affermare l'esistenza di una vera e propria "riserva di diritto giurisprudenziale" circa l'applicazione dell'art. 36 Cost., suscettibile quest'ultimo di prevalere anche nei confronti delle norme di legge ordinaria»; tuttavia, anche in questo caso di applicazione diretta della norma costituzionale da parte del giudice non poteva a rigore parlarsi, essa «necessitando, comunque, per la sua concreta operatività, di un richiamo allo strumento della contrattazione collettiva; per meglio dire, la norma costituzionale di principio (la c.d. giusta retribuzione) verrà sì applicata direttamente dal giudice, ma in quanto integrata dai contenuti di dettaglio della contrattazione collettiva»[161].

Sotto il secondo profilo – quello relativo alla configurabilità, all'epoca, di una forma di invalidità degli atti processuali assimilabile all'inutilizzabilità – come si è avuto modo di anticipare, tale causa di invalidità specificamente afferente al sistema probatorio sarebbe stata codificata più di dieci anni dopo la sentenza in commento, con l'entrata in vigore del nuovo codice di procedura penale. Nel momento in cui la Corte costituzionale esprimeva i principi in commento, dunque, l'unica sanzione processuale suscettibile di colpire le prove irritualmente raccolte era quella della nullità.

Appare difficile, quindi, sostenere che con la decisione in questione – caratterizzata peraltro da un certo tasso di vaghezza – la Corte costituzionale intendesse pronunciarsi su un tema tanto controverso in maniera sostanzialmente apodittica – cioè evitando di prendere posizione esplicita in merito alle complesse questioni che si agitavano al fondo del medesimo – indicando quale soluzione costituzionalmente imposta quella

[160] Corte Cost., 13 luglio 1963, n. 129 e Corte Cost., 6 luglio 1971, n. 156, con cui Corte ha dichiarato incostituzionale la legge sui minimi salariali nella parte in cui intende «inibire al giudice di adeguare […] il trattamento economico previsto dai contratti individuali di lavoro alle situazioni sopravvenute».

[161] Per entrambe le citazioni, MANNELLA, *Giudice comune e Costituzione: il problema dell'applicazione diretta del testo costituzionale*, in *Federalismi.it*, 29 dicembre 2010, 17.

dell'inutilizzabilità *tout court* dei risultati probatori acquisiti in spregio dei diritti fondamentali. Piuttosto, la pronuncia sembra aver rappresentato, per il Giudice delle leggi, l'occasione per esprimere il suo punto di vista su due questioni che in quegli anni erano al centro del dibattito dottrinale in tema di prove e per suggerire al legislatore l'introduzione, nel sistema codicistico, dell'inutilizzabilità quale strumento di estromissione dei dati acquisiti in violazione dei diritti fondamentali[162].

Scontato, dunque, che per passare da mere affermazioni di principio a prese di posizione più nette in relazione al tema oggetto di analisi si dovesse attendere l'entrata in vigore del nuovo codice che, come visto, pur introducendo la categoria dell'inutilizzabilità della prova non conteneva – né contiene – alcuna disposizione esplicita in materia di prova incostituzionale.

Nel 1993, la Corte costituzionale tornava a pronunciarsi in materia[163] nell'ambito di un giudizio di legittimità costituzionale riguardante l'art. 266 del nuovo codice di procedura penale del 1988, sollevato in relazione all'art. 15 Cost. In particolare, la questione sottoposta alla Corte aveva ad oggetto la compatibilità della disciplina codicistica con il parametro costituzionale nella parte in cui limitava alle sole operazioni di intercettazione del contenuto di conversazioni telefoniche le garanzie ivi stabilite. La Corte, dopo aver escluso l'estensione delle garanzie previste in materia di intercettazioni ai tabulati telefonici in ragione della ontologica diversità tra un'attività di captazione delle comunicazioni e un'attività di acquisizione dei dati esterni alle stesse, ha nondimeno posto l'accento sull'ampiezza della tutela accordata dall'art. 15 della Costituzione alla libertà e alla segretezza della comunicazione, tale da ricomprendere fra i propri oggetti anche i dati esteriori. Da ciò, tramite anche il richiamo alla sentenza n. 34 del 1973 prima commentata, il Giudice delle Leggi ha tratto la conseguenza che nonostante la mancanza di una specifica normativa processuale sul punto[164], «l'acquisizione come mezzi di prova dei dati medesimi non può non avvenire nel più rigoroso rispetto delle regole che la stessa Costituzione pone direttamente, con norme

---

[162] CONTI, *Accertamento del fatto e inutilizzabilità*, cit., 48.

[163] Corte Cost. 11 marzo 1993, n. 81, in *Giur. it*., 1993, I, c. 117 s., con nota di DI FILIPPO, *Dati esteriori delle comunicazioni e garanzie costituzionali* e PACE, *Nuove frontiere della libertà di «comunicare riservatamente» (o, piuttosto, del diritto alla riservatezza)?*; vedi anche CAMON, *Sulla inutilizzabilità accordata nel processo penale dei tabulati relativi al traffico telefonico degli apparecchi «cellulari» acquisiti dalla polizia senza autorizzazione dell'autorità giudiziaria*, in *Cass. pen.*, 1996, 12, 3721 ss.

[164] Cui si sarebbe addivenuti con l'approvazione del cd. "Codice della Privacy", il d.lg. 30 giugno 2003, n. 136.

precettive, a garanzia della libertà e della segretezza di ogni forma di comunicazione». Quanto al diritto sancito dall'art. 15 Cost., la regola precettiva posta dalla disposizione costituzionale per la compressione della prerogativa in argomento sarebbe stata da rinvenirsi nel necessario requisito della previa adozione di un atto dell'autorità giudiziaria, sorretto da adeguata e specifica motivazione diretta a dimostrare il concreto sussistere delle esigenze istruttorie connesse, nel caso di specie, all'esecuzione della misura.

L'aspetto più interessante e senz'altro innovativo della pronuncia in commento è da rinvenirsi nel fatto che, per la prima volta esplicitamente, la Corte ricavava direttamente dal testo costituzionale precisi limiti, operanti sul piano processuale, per l'acquisizione di determinati risultati istruttori. Limiti che, ove valicati, sarebbero stati suscettibili di riverberarsi nel processo, comportando l'esclusione dalla piattaforma probatoria delle conoscenze acquisite in violazione dei diritti fondamentali dei singoli. In altre parole, veniva affermato il principio secondo il quale l'utilizzabilità, nel processo penale, delle prove acquisite con modalità suscettibili di restringere i diritti fondamentali presuppone il rispetto delle guarentigie costituzionali poste a presidio dei medesimi.

Si delineava, quindi, una sorta di interazione tra regole codicistiche che presiedono alla formazione della prova e regole ricavabili dallo stesso testo costituzionale, in virtù della quale quest'ultimo può assurgere a limite implicito dell'acquisizione di mezzi di prova innominati nel processo penale.

Questo peculiare rapporto è stato ulteriormente lumeggiato da un'altra importante pronuncia, questa volta delle Sezioni unite della Corte di cassazione. Il riferimento è, ovviamente, alla nota sentenza del 27 marzo 1996, *Sala*[165], intervenuta in materia di perquisizione illegittima e conseguente sequestro e contenente un espresso avallo alla teoria della prova incostituzionale quale categoria «comprensiva della prova della prova "illegittima" ed "illecita, ed avente un unico, irrinunciabile presupposto, e cioè l'essere la sua antigiuridicità riconducibile ad una lesione dei diritti soggettivi fondamentali, riconosciuti e tutelati dalla nostra Costituzione». La Corte, che pure ha concluso – in apparente contraddizione con le premesse sviluppate – nel senso della legittimità del sequestro conseguente a una perquisizione illegittima in ragione della asserita mancanza di una relazione di necessaria consequenzialità giuridica tra il primo e il secondo atto

[165] Sez. un., 27 marzo 1996, n. 5021, Sala, in *Cass. pen*., 1996, 3272.

quando si tratti dell'apprensione del corpo del reato o delle cose ad esso pertinenti[166], delineava con particolare precisione il fondamento giuridico della teoria in argomento. Si legge, infatti, nella decisione che «i "divieti probatori" sono non solo quelli espressamente previsti dall'ordinamento processuale […] ma possono anche essere desumibili dall'ordinamento, e ciò accade tutte le volte in cui i divieti, in materia probatoria, non sono dissociabili dai presupposti normativi che condizionano la legittimità intrinseca del procedimento formativo o acquisitivo della prova». Appare evidente il riferimento all'art. 191 c.p.p., in relazione al quale al termine "legge" viene associato un significato ampio, suscettibile di ricomprendere, oltre alla legge processuale, altresì quella costituzionale[167].

Successivamente, il giudice di legittimità[168], tornato a occuparsi della tormentata vicenda relativa all'acquisizione dei tabulati del traffico telefonico e telematico, ha chiaramente esplicitato il ragionamento giuridico sotteso alla sentenza *Sala*: «le prove formate o acquisite in violazione dei diritti soggettivi tutelati dalla "legge", ed a maggior ragione, quindi, quelle acquisite in violazione dei diritti tutelati in modo specifico dalla Costituzione. Ipotesi quest'ultima sussumibile nella previsione dell'art. 191 c.p.p., proprio perché l'antigiuridicità di prove così formate od acquisite attiene alla lesione di diritti fondamentali, riconosciuti cioè come intangibili dalla Costituzione […] Con la conseguenza che le acquisizioni così avvenute sono destinate a subire una sorta di ablazione nel momento della valutazione da parte del giudice, rispetto al contesto della trama probatoria»[169].

---

[166] Si legge nella sentenza che «se è vero che l'illegittimità della ricerca della prova del commesso reato, allorquando assume le dimensioni conseguenti ad una palese violazione delle norme poste a tutela dei diritti soggettivi oggetto di specifica tutela da parte della Costituzione, non può, in linea generale, non diffondere i suoi effetti invalidanti sui risultati che quella ricerca ha consentito di acquisire, è altrettanto vero che allorquando quella ricerca, comunque effettuata, si sia conclusa con il rinvenimento ed il sequestro del corpo del reato o delle cose pertinenti al reato, è lo stesso ordinamento processuale a considerare del tutto irrilevante il modo con il quale a quel sequestro si sia pervenuti: in questa specifica ipotesi, e ancorché nel contesto di una situazione non legittimamente creata, il sequestro rappresenta un "atto dovuto", la cui omissione esporrebbe gli autori a specifiche responsabilità penali».

[167] Pochi anni dopo, in una pronuncia del 1998, la Corte costituzionale, peraltro, tornava ad affermare, in relazione a un provvedimento di sequestro avente ad oggetto scritti formati dall'imputato quali appunti per la preparazione dell'interrogatorio, che i principi costituzionali sono «immediatamente applicabili in forza di un'interpretazione *secundum Constitutionem* degli artt. 247 e 253 c.p.p.» (Corte Cost., 19 giugno 1998, n. 229, in *Cons. Stato*, 1998, II, 800).

[168] Sez. un., 13 luglio 1998, Gallieri, in *Foro it.*, 1999, 2, 87.

[169] Tali principi sarebbero stati poi ribaditi dalle Sez. un., 23 febbraio 2000, n. 6, D'Amuri, in *Foro it.*, 2000, II, 529, ove si afferma che «il disposto dell'art. 191 del codice di rito, applicabile anche alle c.d. "prove incostituzionali", perché assunte con modalità lesive dei diritti fondamentali dell'individuo, costituzionalmente protetti; prove come tali colpite dalla patologia irreversibile dell'inutilizzabilità, a

Nonostante la apparente stabilità di simili approdi ermeneutici, nel 2006 le Sezioni unite hanno affrontato di nuovo il tema delle prove atipiche impattanti sui diritti fondamentali[170] con una pronuncia che, di fatto, si è posta in netta discontinuità rispetto alla ricostruzione sinora tratteggiata.

Il caso sottoposto all'attenzione della Corte riguardava il regime giuridico applicabile alle riprese audiovisive, che nel nostro ordinamento non erano – e non sono – destinatarie di alcuna disciplina specifica. In particolare, le riprese erano state effettuate nei camerini di un locale nel corso di un'indagine avente ad oggetto il reato di associazione per delinquere finalizzata alla commissione di reati in materia di sfruttamento della prostituzione. Vi era stata un'autorizzazione del giudice secondo la scansione procedimentale prevista in materia di intercettazioni tra presenti.

Due sono i profili di maggiore interesse della pronuncia: il primo, quello relativo al distinguo operato dalla Corte in materia di diritto alla riservatezza e inviolabilità del domicilio; il secondo, inerente al regime applicabile alle prove non previste dalla legge implicanti restrizioni di diritti fondamentali.

La decisione distingue le videoriprese a seconda che siano effettuate in luogo pubblico o aperto al pubblico, nel domicilio ovvero in luogo coperto da un'aspettativa di riservatezza. Nel primo caso, esse potrebbero essere utilizzate tanto se acquisite fuori dal procedimento (la disciplina applicabile sarebbe, in questa ipotesi, quella prevista in materia di prova documentale), quanto se realizzate dagli stessi inquirenti (con la conseguente applicazione del regime previsto in materia di prova atipica dall'art. 189 c.p.p.).

Nel caso in cui, invece, si tratti di luoghi non costituenti domicilio, ma comunque adoperati per attività che si vogliono mantenere riservate, le riprese visive potrebbero acquisirsi – ai sensi dell'art. 189 c.p.p. – sulla base di un provvedimento motivato dell'autorità giudiziaria, in ragione della mera incidenza della misura su diritti costituzionali non presidiati da riserva di legge. In questo caso, si legge nella pronuncia, a essere incisi sarebbero i soli diritti alla riservatezza e al rispetto della vita privata, il

---

prescindere dal fatto che la legge contempli divieti espliciti al loro impiego nel procedimento. Non è necessario, infatti, che le garanzie siano puntualmente previste nel testo normativo che disciplina una materia; possono rinvenirsi in altre norme o nei principi generali, anche contenuti nella Carta costituzionale, che disciplinano le attività processuali (arg. da sentenza C. Cost. n. 34/73)».

[170] Sez. un., 28 marzo 2006, n. 26795, Prisco, in *Cass. pen.*, 2006, 3937 ss., con note di RUGGIERI, *Riprese visive e inammissibilità della prova* e DI BITONTO, *Le riprese video domiciliari*, cit., 1347 ss.

cui fondamento è da rinvenirsi negli artt. 2 Cost., 8 della Convenzione europea dei diritti dell'uomo e 17 del Patto internazionale sui diritti civili e politici[171].

L'*iter* argomentativo seguito dalla Corte si complica con riferimento alle videoriprese acquisite nel domicilio: la misura verrebbe a incidere, in questo caso, su un diritto fondamentale presidiato, ai sensi dell'art. 14 Cost., da riserva di legge oltre che di giurisdizione. Ne conseguirebbe, dunque, l'inapplicabilità dell'art. 189 c.p.p. e la necessità di una disciplina legislativa specifica che regoli i casi e i modi dell'intrusione nel diritto fondamentale. Tale disciplina, secondo la Corte, sarebbe rinvenibile nel codice di rito solo con riferimento alle riprese visive di comportamenti comunicativi, riconducibili alla disciplina prevista in materia di intercettazioni. Mancherebbe, invece, una normativa in materia di riprese di comportamenti non comunicativi[172] che, conseguentemente, potrebbero essere regolate dal solo legislatore, in ossequio alla riserva di legge prevista dalla norma costituzionale. In conseguenza di ciò, le videoriprese di comportamenti non comunicativi acquisite all'interno del domicilio dovrebbero considerarsi vietate e non potrebbero confluire nella piattaforma probatoria, quanto meno fintantoché il legislatore non approntì una disciplina specifica in materia, in attuazione della riserva di legge prevista dall'art. 14 Cost.

Per addivenire a questo risultato, differentemente da quanto ci si sarebbe attesi alla luce dei principi già espressi dalla giurisprudenza degli anni precedenti in materia di prova atipica impattante sui diritti fondamentali, la Corte ha fatto leva su una ricostruzione giuridica inedita, di fatto evitando di prendere posizione in merito alla teoria della prova incostituzionale, la qual cosa avrebbe postulato l'individuazione di un divieto probatorio sanzionato con l'inutilizzabilità di cui all'art. 191 c.p.p. nell'art. 14 Cost. Secondo le

[171] Si legge, a proposito, nella decisione che «sul piano costituzionale il diritto alla riservatezza non gode di una tutela analoga a quella apprestata dall'art. 14 Cost. per il domicilio, ed è per questa ragione che anche in mancanza di una disciplina specifica le riprese visive che lo sacrificano devono ritenersi consentite e suscettibili di utilizzazione probatoria a norma dell'art. 189 c.p.p.».

[172] La distinzione operata dalla Corte di cassazione tra videoriprese di comportamenti comunicativi e non comunicativi trovava un autorevole antecedente in Corte Cost., 24 aprile 2002, n. 135, in *Giur. cost*., 2002, 1062 ss., che si era pronunciata sulla questione di legittimità costituzionale degli artt. 189 e 266-271 c.p.p., sollevata con riferimento agli art. 3 e 14 Cost., nella parte in cui non estendevano la disciplina delle intercettazioni ambientali disposte nel domicilio alle riprese visive effettuate nei medesimi luoghi, dichiarandola infondata in ragione della eterogeneità della limitazione della libertà e segretezza delle comunicazioni e dell'invasione della libertà domiciliare. Nella decisione, la Corre costituzionale aveva, infatti, distinto l'ipotesi della videoregistrazione di comportamenti comunicativi da quella relativa a comportamenti non comunicativi, concludendo che questa seconda, non avendo carattere di intercettazione di comunicazioni, avrebbe potuto essere disciplinata soltanto dal legislatore, nel rispetto delle garanzie costituzionali dell'art. 14 Cost.

Sezioni unite, «per giungere alla conclusione che non possono considerarsi ammissibili, come prove atipiche, le videoregistrazioni di comportamenti non comunicativi effettuati in ambito domiciliare non occorre però prendere posizione sul dibattito relativo agli effetti che la violazione delle norme costituzionali di garanzia può avere sull'attività probatoria prevista dal codice di rito, né stabilire se la sanzione dell'inutilizzabilità attenga solo alla violazione dei divieti stabiliti dalla legge processuale o riguardi anche la violazione di norme costituzionali o di altri rami dell'ordinamento, e segnatamente di quello penale». Piuttosto, a parere della Corte, è la categoria dell'inammissibilità a venire in rilievo, atteso che l'inutilizzabilità riguarderebbe, in linea di principio, le sole prove tipiche, non essendo quelle atipiche qualificabili come prove prima che intervenga un provvedimento ammissivo del giudice. Detto altrimenti, l'art. 189 c.p.p. – letto in combinato con l'art. 190 c.p.p., comma 1, che impone l'esclusione delle prove "vietate dalla legge" – «presuppone logicamente la formazione lecita della prova e soltanto in questo caso la rende ammissibile», non potendo considerarsi, *sic et simpliciter*, non disciplinata dalla legge una prova che la legge vieta, come nel caso delle riprese visive di comportamenti non comunicativi avvenuti in ambito domiciliare.
La ricostruzione prospettata dalle Sezioni unite si pone, dunque, in discontinuità rispetto alle soluzioni interpretative che avevano caratterizzato la precedente giurisprudenza costituzionale e di legittimità quanto al fondamento teorico dell'esclusione dalla piattaforma probatoria delle conoscenze acquisite con metodi lesivi dei diritti fondamentali dei singoli e in spregio delle garanzie costituzionali poste a presidio degli stessi[173]. Non muta, tuttavia, l'epilogo: la costatazione della impossibilità di ricondurre determinati strumenti di acquisizione della prova all'interno delle categorie a disciplinate dalla legge comporta, nel caso di misura incidente su un diritto costituzionale presidiato dalla riserva di legge, l'estromissione del risultato conoscitivo raccolto dalla piattaforma probatoria o, meglio, l'impossibilità, *tout court*, di introdurvelo stante lo sbarramento dell'inammissibilità.

[173] Secondo DI BITONTO, *Le riprese video domiciliari*, cit., 3959 ss., la pronuncia ha il pregio di lumeggiare i rapporti il principio di legalità e la prova atipica: visto che le prove atipiche non hanno una specifica regolamentazione all'interno del codice di rito, occorrerebbe fare riferimento altresì alla regolamentazione extracodicistica al fine di valutarne la legittimità.

Benché, dunque, la pronuncia rappresenti tutt'altro che un approdo definitivo in tema di prova incostituzionale[174] – e abbia, anzi, contribuito a generare ulteriori incertezze quanto all'inquadramento giuridico della questione – la stessa si pone, quanto meno, in linea di continuità con la precedente giurisprudenza quanto alla necessità di escludere dal bagaglio conoscitivo del giudice risultati probatori ottenuti in spregio dei diritti fondamentali[175].

Permangono, tuttavia, alcuni aspetti particolarmente critici nella ricostruzione operata dalle Sezioni unite, soprattutto se letta alla luce di alcuni principi affermati nella precedente giurisprudenza costituzionale e di legittimità. Come si vedrà nell'ultimo paragrafo, tali criticità sembrano amplificarsi quando il tema della prova atipica impattante sulle prerogative costituzionali interseca quello dei mezzi di indagine tecnologicamente avanzati. Prima, però, occorre verificare in che modo gli approdi finora raggiunti in materia operino nella fase investigativa, nella quale si situa il ricorso a tali strumenti di ricerca della prova.

---

[174] Peraltro, appena due anni dopo l'emissione della pronuncia in commento la Corte Costituzionale è tornata a pronunciarsi sul tema delle videoriprese in ambito domiciliare riaffermando la soluzione giuridica consolidata nella sua giurisprudenza e in quella di legittimità prima della pronuncia delle Sezioni unite del 2006 in commento. La sentenza, in particolare, ha dichiarato inammissibile la questione di legittimità costituzionale dell'art. 266, comma 2, c.p.p., nella parte in cui non estende la disciplina delle intercettazioni di comunicazioni tra presenti «a qualsiasi "captazione di immagini in luoghi di privata dimora"», ancorché «non configurabile in concreto come forma di intercettazione di comunicazioni tra presenti», perché irrilevante. Si legge nella pronuncia che «il rimettente non prende, però, affatto in esame – anche solo per escluderne, eventualmente, la praticabilità – la soluzione interpretativa esattamente opposta. Secondo quest'ultima, in mancanza di una norma che consenta e disciplini il compimento dell'attività in parola – soddisfacendo la doppia riserva, di legge (quanto ai «casi» e ai «modi») e di giurisdizione, cui lart. 14, secondo comma, Cost. subordina l'eseguibilità di atti investigativi nel domicilio – l'attività stessa dovrebbe ritenersi radicalmente vietata, proprio perché lesiva dell'inviolabilità del domicilio, sancita dal primo comma dello stesso art. 14 Cost.; mentre i risultati delle riprese effettuate in violazione del divieto rimarrebbero inutilizzabili […] È evidente, d'altro lato, che l'adozione della diversa soluzione interpretativa dianzi indicata renderebbe il quesito di costituzionalità irrilevante nel giudizio *a quo*, giacché – ove le riprese visive di cui si discute, eseguite ad iniziativa della polizia giudiziaria, risultassero, in concreto, lesive dell'inviolabilità del domicilio – esse sarebbero già ora inutilizzabili, alla stregua di detta interpretazione», Corte Cost., 7 maggio 2008, n. 149, in *Giur. cost.*, 2008, 3, 1825, con nota di CAPRIOLI, *Nuovamente al vaglio della Corte costituzionale l'uso investigativo degli strumenti di ripresa visiva*; vedi anche FILIPPI, *La consulta riconosce che l'*home watching *è una prova incostituzionale*, in *Giust. pen.*, 2008, 1, 343 ss.

[175] Appare significativa, in questo senso, l'affermazione secondo la quale «se il sistema processuale deve avere una sua coerenza risulta difficile accettare l'idea che una violazione del domicilio che la legge processuale non prevede (e che per questa ragione risulta in contrasto con il contenuto precettivo dell'art. 14 Cost.) possa legittimare la produzione di materiale di valore probatorio e che inoltre per le riprese di comportamenti non comunicativi possano valere regole meno garantiste di quelle applicabili alle riprese di comportamenti comunicativi, regolate, come si è visto dagli artt. 266-271 c.p.p.».

4. Attività di investigazione atipica incidente sui diritti fondamentali e applicazione dell'art. 189 c.p.p. nella fase delle indagini preliminari.

Alla scelta di introdurre, con riferimento al dibattimento, un sistema improntato alla tassatività, sia pur temperata, dei mezzi di conoscenza giudiziale ha fatto da contraltare, nel disegno del legislatore del 1988, la decisione di non imbrigliare in regole di accertamento rigide le indagini preliminari. Queste ultime, concepite per essere la fase che "non conta e non pesa"[176] – in virtù del principio di separazione delle fasi e di tendenziale impermeabilità del dibattimento agli esiti delle indagini – si caratterizzano per una spiccata flessibilità, in considerazione del carattere ancora fluido dell'ipotesi accusatoria e della finalizzazione dell'acquisizione di elementi probatori al solo scioglimento dell'alternativa tra l'azione e l'inazione.

Sotto altro profilo, l'opzione a favore di una maggiore elasticità degli strumenti di formazione della conoscenza nella fase delle indagini appare una conseguenza necessitata della normale situazione di squilibrio informativo che, all'inizio del procedimento penale, caratterizza le posizioni dell'investigatore e dell'investigato. Il procedimento penale, infatti, prende avvio con l'acquisizione della notizia di reato, ovvero con nulla più che una mera ipotesi che deve essere successivamente suffragata da elementi di riscontro. Nella fase primitiva del procedimento, dunque, a fronte della piena conoscenza dei fatti da parte del soggetto sottoposto all'indagine – colpevole o innocente che sia – l'investigatore è, sostanzialmente, *tabula rasa*.

Se, dunque, il dibattimento è la sede deputata alla formazione della conoscenza processuale per il tramite di schemi probatori tendenzialmente rigidi, la fase preliminare risponde a un principio di tendenziale atipicità. Con una formulazione particolarmente ampia, non a caso, l'art. 348 comma 2 c.p.p. stabilisce che, al fine di raccogliere elementi utili alla ricostruzione del fatto e all'individuazione del colpevole, la polizia giudiziaria procede, «fra l'altro», alle attività di ricerca della prova indicate nella medesima disposizione. Tale locuzione depone nettamente nel senso che la polizia sia legittimata a porre in essere atti ulteriori – e, dunque, atipici[177] – rispetto a quelli ivi specificati.

---

[176] NOBILI, *Diritti per la fase che "non conta e non pesa", in* Id., *Scenari e trasformazioni del processo penale*, Cedam, 1998.

[177] La giurisprudenza è, infatti, pacifica nel ricondurre nell'ambito dell'attività investigativa di polizia non disciplinata dalla legge tutta una serie di attività, quali, pedinamenti, appostamenti, riconoscimenti fotografici e così via. Sez. II, 30 ottobre 2008, in *Guida dir*. 2009, 90; Sez. V, 6 aprile 1999, *CED Cass*.,

Tale assetto determina l'insorgere di due questioni di fondamentale rilievo sistematico: da un lato, si impone l'esigenza di comprendere se, in che misura e con quali effetti l'art. 189 c.p.p. possa operare in relazione agli atti atipici di indagine; per altro verso, quella di verificare l'operatività delle conclusioni raggiunte in materia di prova atipica impattante sui diritti fondamentali in tale fase.

Occorre prendere le mosse dalla prima delle due questioni, che è altresì quella più complessa.

Come si è detto, in virtù del principio di tendenziale atipicità dell'investigazione, il codice di rito riconosce alla polizia giudiziaria un ampio margine di manovra quanto alla individuazione delle modalità di acquisizione degli elementi di riscontro all'ipotesi investigativa. La dottrina ha rilevato come ciò faccia sorgere l'interrogativo circa l'attribuzione o meno di tale prerogativa anche al pubblico ministero, in qualità di *dominus* delle indagini e in considerazione della sua posizione di preminenza rispetto alla stessa polizia giudiziaria. Da un punto di vista sistematico, infatti, sarebbe arduo sostenere che i poteri di indagine della polizia giudiziaria siano più ampi di quelli riconosciuti al pubblico ministero, che è organo non solo ad essa sovraordinato[178], ma anche dotato di prerogative d'indipendenza suscettibili di rappresentare un più forte presidio di legalità a fronte di atti per i quali proprio la mancanza di un modello normativo prestabilito pone rischi di deviazioni dai binari propri dell'accertamento penale.

Tanto condurrebbe a concludere per l'applicabilità dell'art. 189 c.p.p. anche agli atti compiuti dal pubblico ministero nella fase delle indagini preliminari[179], anche in virtù della considerazione per la quale i principi espressi dal codice in materia di prove nel libro terzo dovrebbero essere estesi alla fase delle indagini preliminari[180]. Tale conclusione, tuttavia, non è apparsa scontata e, anzi, sembrerebbe esclusa dal tenore letterale dell'art. 189 c.p.p., che pone quale condizione di ammissibilità della prova atipica l'instaurazione del contraddittorio delle parti in merito alle modalità di

241872; Sez. IV, 11 febbraio 1998, *CED Cass*., 2104444; Sez. II, 12 dicembre 1997, in *Riv. pen*., 1998, 811; Sez. IV, 8 novembre 1995, in *Riv. pen.* 1996, 1278. In dottrina, per tutti, si veda AA.VV., *Le indagini atipiche*, a cura di Scalfati, Giappichelli, 2019.

[178] CAMON, *Le indagini preliminari*, in AA.VV., *Fondamenti di procedura penale*, Cedam, 2021, 423.

[179] Come si vedrà in seguito, la conclusione è pacifica in giurisprudenza. In dottrina, si veda la ricostruzione di SCALFATI, *Premessa*, in AA. VV., *Le Indagini Atipiche. Leggi penali tra regole e prassi*, a cura di Scalfati, 2014, Giappichelli.

[180] CAMON, *Le prove*, in AA.VV., *Fondamenti di procedura penale*, Cedam, 2021, 284 ss.; PISANI, *Le prove. Appunti sul Titolo I, Libro III*, cit., 202.

acquisizione della stessa. Contraddittorio previo che, trattandosi di mezzi di ricerca della prova tendenzialmente esperiti "a sorpresa", avrebbe l'effetto di vanificare il compimento dell'atto e risulterebbe, quindi, difficilmente esperibile.

Alcuni autori, conseguentemente, hanno negato l'esistenza di una categoria processuale che includa i mezzi atipici di ricerca della prova, sottolineando come la disposizione di cui all'art. 189 c.p.p. esprima il principio secondo il quale, quando la prova è disciplinata dalla legge, l'accertamento deve compiersi secondo le disposizioni procedurali specificamente previste, non potendosi ipotizzare l'esistenza di fattispecie parallele che sostituiscano quelle disciplinate dalla legge e, tanto, neppure se a venire in risalto è una fase – quella delle indagini preliminari – improntata a minore formalismo rispetto al dibattimento[181]. Conseguentemente, i risultati di attività atipiche di ricerca della prova non potrebbero confluire, secondo il meccanismo di cui all'art. 189 c.p.p., nel dibattimento.

Altri, al contrario, hanno avanzato soluzioni di compromesso, reputando estensibile l'art. 189 c.p.p. anche ai mezzi di ricerca della prova in considerazione della possibilità di recupero del contraddittorio in un momento successivo al compimento dell'atto atipico e, dunque, all'acquisizione del risultato probatorio che mira a realizzare[182]. Il contraddittorio, cioè, verrebbe a svilupparsi al momento della richiesta di ammissione della prova in dibattimento e avrebbe ad oggetto non già le modalità della acquisizione – ormai avvenuta – del risultato probatorio, ma il procedimento seguito dagli investigatori. Si tratterebbe, dunque, di una valutazione postuma di quanto già svolto, sicché «ove il giudice, sulla base delle argomentazioni delle parti, si convincesse che l'*iter* d'assunzione non garantisce un risultato probatorio attendibile sotto il profilo gnoseologico, rifiuterebbe l'ammissione della prova»[183].

A una simile soluzione parrebbe ostare, però, la considerazione per la quale un contraddittorio solo successivo all'acquisizione del risultato probatorio risulterebbe per lo più inefficace, nel senso che non potrebbe assolvere alla funzione alla quale è preposto nel dibattimento che, come si è visto, è quella di assicurare che le modalità di

---

[181] Così, NOBILI, *Scenari e trasformazioni del processo penale*, Cedam, 1998, 43 ss.; in senso dubitativo, GALANTINI, *L'inutilizzabilità della prova*, cit., 213.

[182] In questo senso, si vedano, *ex multis*, CONTI, *Accertamento del fatto ed inutilizzabilità*, cit., 160; LARONGA, *Le prove atipiche nel processo penale*, Cedam, 2002, 32.

[183] CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove incostituzionali*, in *Cass. pen.*, 1999, 4, 1195.

acquisizione della prova, proprio perché stabilite a seguito di un confronto tra le parti, siano le più idonee ad assicurare la affidabilità cognitiva del risultato di prova ottenuto. Come si è osservato, «la necessità dell'ascolto delle parti in contraddittorio non deriva da una esigenza collaborativa tra parti e giudice, ma dalla intima interconnessione tra comportamenti legali processuali e conoscenze legali giudiziali, tra regole del procedimento e valore del giudizio»[184]. Tanto impedirebbe un'estensione dell'art. 189 c.p.p. agli atti compiuti dal pubblico ministero, andando a rafforzare, su un piano sistematico, la conclusione già desumibile dalla formulazione letterale della norma, che fa riferimento testuale al "giudice"[185].

Della questione, come noto, si sono occupate altresì le Sezioni unite *Prisco*[186], che hanno legittimato la penetrazione nel dibattimento di risultati di mezzi atipici di ricerca della prova. Nella pronuncia, in particolare, ha trovato accoglimento la tesi di quanti sostenevano che il contraddittorio di cui all'art. 189 c.p.p. ben potrebbe esperirsi nel dibattimento, al momento del vaglio sull'ammissione del mezzo di prova.

La posizione assunta dalla giurisprudenza ha suscitato svariate critiche da più voci della dottrina, che hanno, anzitutto, evidenziato come l'opzione esegetica accolta rappresenti il risultato di un'interpretazione non già adeguatrice, ma schiettamente analogica dell'art. 189 c.p.p., trasformando il contraddittorio per la prova previsto dalla norma in un mero contraddittorio sulla prova già formata senza alcun intervento delle parti, dei loro difensori o di esperti dai medesimi nominati. Peraltro, il contraddittorio postumo ipotizzato dalla giurisprudenza interverrebbe in una fase in cui, oramai, i diritti del soggetto inciso dalla misura sono stati già compromessi[187]. La funzione del contraddittorio preventivo previsto dall'art. 189 c.p.p. sulle modalità di assunzione della prova sarebbe, infatti, anche quella di individuare le procedure acquisitive più adeguate a limitare l'impatto sui diritti fondamentali degli individui normalmente connaturato all'incedere del procedimento, soprattutto nella sua fase istruttoria[188].

---

[184] FALATO, *Sulla categoria dei mezzi atipici*, cit., 2420.
[185] GRIFFO, *Perquisizione informatica*, cit., 2.
[186] Sez. un., 28 marzo 2006, n. 26795, Prisco, cit.
[187] MANCUSO, *La perquisizione on line*, in *Jusonline*, 2017, 3, 429.
[188] Per l'osservazione secondo la quale «l'intera materia probatoria presenti una spiccata rilevanza costituzionale, in quanto inevitabilmente incidente sui diritti fondamentali dell'imputato o degli altri soggetti protagonisti del processo», MAZZA, *I diritti fondamentali dell'individuo*, cit., 8.

Secondo alcuni commentatori, dunque, la Corte non avrebbe colto quella correlazione tra il contraddittorio previsto dall'art. 189 c.p.p., la valenza cognitiva del risultato probatorio raggiunto e le modalità della conoscenza giudiziale[189].

A ciò potrebbe aggiungersi che stante la maggiore «fluidità degli strumenti investigativi»[190] rispetto ai mezzi di prova dibattimentale espressamente previsti – derivante, come si è visto, dal fatto che il legislatore ha ritenuto di non tipizzare eccessivamente la fase delle indagini preliminari – è facilmente pronosticabile che, con l'emergere di sempre nuovi strumenti di ricerca grazie all'incessante progresso scientifico, sarà sempre più ampia la "fetta" di mezzi di ricerca atipici della prova rispetto a quelli tipici. Tanto con la conseguenza, inevitabile, di un'alterazione degli equilibri tra indagini preliminari e dibattimento pensati dal legislatore del 1988[191]. La tendenziale irripetibilità di tali atti, infatti, sta già provocando un progressivo spostamento del baricentro del procedimento penale dalla fase dibattimentale a quella le indagini[192], con gli ovvi rischi che ne conseguono non solo in termini di tenuta complessiva del sistema, ma anche sul piano dell'effettività del diritto di difesa e della qualità dell'accertamento[193].

Le criticità appena descritte si intensificherebbero oltremodo quando a venire in risalto fosse una prova atipica a contenuto altamente tecnologico per la strutturale idoneità di tale tipologia di prova[194] a incidere su diritti costituzionali di rango elevato con un'efficacia intrusiva che non appartiene ai mezzi, sia pur atipici, di ricerca della prova

---

189 Così, ancora, MAZZA, *I diritti fondamentali dell'individuo*, cit., 6, secondo il quale l'art. 189 c.p.p., riferendosi alle modalità assuntive della prova, lascia chiaramente intendere che di prove atipiche possa parlarsi solo con riferimento al dibattimento per accogliere mezzi di prova costituenda, atteso che solo con riferimento a questi ultimi ha senso, sotto il piano logico giuridico, parlare di modalità assuntive da definire in contraddittorio.

190 DI CHIARA, *Atipicità e sistemi probatori*, cit., 373.

191 Osserva che un'apertura indiscriminata a favore di controlli segreti atipici rischia di incrementare oltremodo le deroghe al principio di formazione della prova in contraddittorio da NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 11.

192 Nel senso che l'avvento telle nuove tecnologie di indagine sta comportando un ampliamento degli atti irripetibili e una sempre più spiccata posticipazione del contraddittorio, SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, 7.

193 Non pare peregrino evidenziare come proprio la disciplina delle intercettazioni sia stata, in qualche modo, antesignana di tale mutamento degli assetti esistenti. Non è un mistero che, soprattutto nei processi di criminalità organizzata, la stragrande maggioranza della piattaforma probatoria è rappresentata proprio dagli esiti delle intercettazioni disposte nel corso delle indagini, dunque da materiale cognitivo formato in maniera unilaterale e in relazione al quale residuano alla difesa spazi angusti di esplicazione del contraddittorio, molto spesso limitato al significato da attribuire a questa o a quell'altra espressione adoperata nel corso delle interlocuzioni.

194 Si vedano le considerazioni del cap. 1.

meno recenti[195]. Tanto, peraltro, nel contesto di una fase – quella delle indagini preliminari – connotata da una inevitabile mutabilità dell'accusa e, conseguentemente, dall'affievolirsi del principio di necessaria pertinenza[196] che, invece, connota con maggiore pregnanza l'accertamento condotto nel corso del dibattimento[197].

L'art. 189 c.p.p., dal canto suo, non è sembrato suscettibile di porre rimedio alcuno ai rischi e alle criticità appena segnalati: si tratta di una norma dal contenuto per lo più indeterminato, la quale «non àncora l'ammissione della conoscenza innominata ad un criterio di proporzione fra l'ipotesi d'accusa e l'eventuale compressione di diritti o interessi giuridicamente rilevanti; non pone riserve in capo all'autorità giurisdizionale e nemmeno in capo all'autorità giudiziaria; se la ricerca probatoria si snoda nel tempo, non fissa limiti di durata; e così via. Il risultato, si è sostenuto, è quasi una zona franca dell'ordinamento processuale, nella quale i nuovi strumenti d'indagine o non subiscono vincoli o, se li subiscono, pongono comunque difficilissimi problemi di qualificazione giuridica»[198].

Una più attenta analisi della pronuncia delle Sezioni unite e un'interpretazione sistematica dell'art. 189 c.p.p., tuttavia, conducono a conclusioni distinte da quelle propugnate dalla dottrina più critica nei confronti della sentenza e, in generale, a una rimeditazione dell'operatività della norma in questione con riferimento agli atti di indagine.

Tanto si sostiene sulla scorta di due considerazioni, sulle quali è bene spendere alcune riflessioni.

In primo luogo, il dibattito sviluppatosi intorno al tema che occupa sembra poggiarsi su un equivoco in merito cosa debba intendersi per applicabilità dell'art. 189 c.p.p. agli atti di indagine. In secondo luogo, a differenza di quanto sembra aver inteso una parte della dottrina, la soluzione accolta dalle Sezioni unite Prisco non implica affatto la mancanza di qualsivoglia sbarramento, tanto in fase dibattimentale quanto in fase investigativa, alla possibilità di introdurre nell'ambito della conoscenza giudiziaria saperi acquisiti in violazione delle prerogative costituzionali.

---

[195] Evidente, ad esempio, che un pedinamento elettronico o satellitare operato con mezzi tecnologici è altamente più intrusivo di un pedinamento "tradizionale", necessariamente contingentato nel tempo.

[196] Non v'è dubbio, però, che tale principio operi anche nella fase delle indagini preliminari. Così, NOBILI, *La nuova procedura penale,* cit., 113.

[197] CAMON, *La fase che "non conta e non pesa": indagini governate dalla legge?* in *Dir. pen. e proc.*, 2017, 4, 431.

[198] CAMON, *Le indagini preliminari*, in AA.VV., *Fondamenti di procedura penale*, Cedam, 2021, 423.

È bene prendere le mosse dalla prima considerazione.

Quando si parla di atti di indagine atipici, altro è chiedersi se e come il pubblico ministero sia ammesso ad acquisire elementi di prova non tipizzati e in che misura il giudice delle indagini preliminari possa porre tali elementi alla base delle decisioni che, eventualmente, sia chiamato incidentalmente ad assumere; altro è chiedersi come i risultati di quegli atti atipici di indagine possano entrare a far parte della piattaforma probatoria propria del dibattimento. È evidente che la questione relativa all'operatività del contraddittorio previsto dall'art. 189 c.p.p. con riferimento agli atti investigativi attiene esclusivamente a questo secondo segmento.

Con riguardo al primo segmento, in considerazione di quanto si è visto in apertura del paragrafo, non pare possano esservi dubbi in merito al fatto che il pubblico ministero sia ammesso ad acquisire elementi di conoscenza per il tramite di mezzi di ricerca della prova non tipizzati. È altresì evidente che tale possibilità incontri dei limiti nella parziale operatività dei principi previsti dallo stesso art. 189 c.p.p. in fase di indagine, in forza della considerazione secondo la quale, laddove compatibili con le peculiarità della fase investigativa, i principi stabiliti in materia di prove dal terzo Libro del codice devono reputarsi estesi a tale fase. In ragione di ciò, dunque, un mezzo atipico di ricerca della prova mai potrebbe pregiudicare la libertà morale della persona e dovrebbe, comunque, essere idoneo all'accertamento dei fatti. La natura fluida dell'indagine preliminare e il carattere interinale delle eventuali decisioni che il giudice potrebbe assumere in quella sede sulla base degli elementi di conoscenza in questione determinano l'inoperatività della regola relativa alla determinazione, nel contraddittorio, delle modalità di acquisizione della prova. Tale regola, evidentemente, opererà in dibattimento, essendo quella la sede deputata alla formazione della conoscenza giudiziale secondo le regole del contraddittorio e all'assunzione di una decisione sul merito suscettibile di acquisire carattere di definitività. Ciò non significa, naturalmente, che il giudice per le indagini preliminari che fosse chiamato ad assumere una decisione (si pensi all'applicazione di un sequestro preventivo o di una misura cautelare personale) sulla base del materiale acquisito tramite il mezzo atipico di ricerca della prova possa utilizzare i risultati di conoscenza in questione senza compiere sugli stessi un previo vaglio in merito alla circostanza che non pregiudichino la libertà morale delle persone e che siano idonei all'accertamento dei fatti (nonché, come si vedrà in chiusura

del paragrafo, al fatto che l'atto non sia stato compiuto in spregio dei diritti fondamentali), sia pure secondo gli *standard* valutativi, meno rigorosi, propri della fase delle indagini.

Da questo punto di vista, il ragionamento condotto dalle Sezioni unite sembra corretto: l'art. 189 c.p.p., a rigore, riguarda la prova e, precisamente, la fase della sua ammissione in dibattimento. Il solo fatto che le parti possano chiedere al giudice l'ammissione in dibattimento di mezzi di prova finalizzati a introdurre nella piattaforma probatoria del processo conoscenze acquisite nella fase investigativa non mortifica la *ratio* del contraddittorio di cui all'art. 189 c.p.p. perché proprio attraverso il confronto delle parti si stabiliranno le modalità con le quali tale conoscenza dovrà confluire nel dibattimento. Ad esempio, il giudice potrebbe reputare opportuno realizzare una perizia, acquisire prove testimoniali e così via. Nel corso dell'udienza deputata all'ammissione delle prove, dunque, il contraddittorio scavalla i confini previsti dall'art. 190 c.p.p. per estendersi anche alla validità cognitiva dei risultati di prova raggiunti, anche in dipendenza delle modalità attraverso le quali sono stati reperiti, e alle concrete modalità di introduzione di quelle conoscenze nella piattaforma dibattimentale. L'esplicazione del contraddittorio in quella sede è, anzi, essenziale perché i mezzi di prova e di ricerca della prova atipici non sono assistiti da una "presunzione", sia pure relativa, di idoneità dimostrativa, di non impatto sulla libertà morale e di adeguatezza delle modalità della loro acquisizione all'accertamento dei fatti che, invece, caratterizza quelli tipici.

Da questo punto di vista, se vi è un aspetto criticabile nella ricostruzione operata dalla sentenza Prisco, è quello che attiene all'operatività dell'art. 431, lett. b) e c), c.p.p. Con riferimento alle videoregistrazioni – ma l'argomento è estensibile a qualunque altro mezzo atipico di ricerca della prova – la pronuncia afferma che «è stata anche posta e dibattuta la questione sulla possibilità di inserire le videoregistrazioni nel fascicolo per il dibattimento, a norma dell'art. 431, comma 1, lett. b) c.p.p., considerandole alla stregua di verbali di atti non ripetibili compiuti dalla polizia giudiziaria […], e si è detto che mentre nessuna difficoltà si frappone all'introduzione nel fascicolo per il dibattimento del verbale della polizia giudiziaria descrittivo delle attività compiute per effettuare la videoripresa, alla stessa conclusione non potrebbe pervenirsi per il supporto contenente le immagini riprese, che l'art. 431 c.p.p. non prevede, verosimilmente perché il legislatore sarebbe stato "attento soprattutto alle tradizionali forme di documentazione

scritta". La conclusione negativa non convince dal momento che l'art. 134, comma 4, c.p.p. nel disciplinare la documentazione degli atti riconosce che al verbale "può essere aggiunta la riproduzione audiovisiva se assolutamente indispensabile". In questo caso la riproduzione audiovisiva diventa un elemento integrativo del verbale, che deve accompagnarlo e che quindi, unitamente al verbale, è destinato a far parte del fascicolo per il dibattimento».

In realtà, vi sono almeno due argomenti che depongono nel senso che il concetto di "verbali di atti irripetibili" cui fa riferimento l'art. 431 c.p.p. sia suscettibile di ricomprendere solo quelli tipici e non anche quelli innominati.

Anzitutto, si è appena visto che, a differenza dei mezzi tipici di prova e ricerca della prova, quelli atipici non sono assistiti da alcuna presunzione di conformità alle regole che presiedono, in via generale, alla formazione della conoscenza processuale spendibile per la decisione sul merito della *regiudicanda*. Tanto induce ad escludere che possano confluire *de plano* nel fascicolo dibattimentale, tendenzialmente destinato a contenere materiale utile per la decisione per tutta la durata di una fase in cui la formazione della conoscenza deve soddisfare certe prerogative di affidabilità. Vero è che, come evidenziano anche le Sezioni unite, la circostanza che possano confluire nel fascicolo di cui all'art. 431 c.p.p. non comporta «l'effetto di attribuire alla videoregistrazione valore probatorio senza il preventivo vaglio di ammissibilità da parte del giudice, dopo aver sentito le parti a norma dell'art. 189 c.p.p. 5». Così come è vero che, ad ogni modo, è solo attraverso il sistema delle letture che gli elementi contenuti nel fascicolo acquisiranno piena dignità di prove spendibili per la decisione. Ma è altrettanto vero che salvaguardare la verginità cognitiva del giudice rispetto a elementi che neppure in astratto si presumono idonei a formare la conoscenza processuale è essenziale proprio per garantire che non vi siano aggiramenti surrettizi dei principi che presiedono alla edificazione della conoscenza giudiziale in un sistema processuale come quello vigente.

A ciò va aggiunta un'ulteriore considerazione: in presenza di atti che hanno natura tendenzialmente irripetibile, la disciplina codicistica in materia di indagini preliminari prevede, generalmente, l'esplicazione del diritto di difesa, sia pur secondo modalità tarate sulle peculiarità di una fase pur sempre caratterizzata, oltre che dalla già menzionata fluidità dell'ipotesi investigativa, anche dall'esigenza di una certa celerità

nel compimento di alcuni atti e da quella di mantenere l'effetto sorpresa in merito ad altri. Una dimostrazione plastica di ciò si rinviene, ad esempio, nel coinvolgimento della difesa nel caso di compimento di accertamenti tecnici irripetibili così come nel diritto all'assistenza tecnica nel caso di svolgimento di attività di perquisizione e sequestro. Il fatto che, nonostante ci si trovi in una fase preliminare, siano comunque assicurati spazi per l'estrinsecazione del diritto di difesa si spiega anche e soprattutto in ragione del fatto che i risultati di quelle attività investigative, tendenzialmente, confluiranno nel fascicolo dibattimentale. In tutti questi casi, ove vi sia una persona sottoposta alle indagini e non si proceda a carico di ignoti, la difesa deve essere coinvolta. Con riferimento agli atti atipici, al contrario, nessuna norma obbliga il pubblico ministero a garantire l'esercizio del diritto di difesa al soggetto sottoposto alle indagini.

Per tali ragioni, deve ritenersi che i verbali relativi agli atti di indagine atipici non possano confluire nel fascicolo del dibattimento: perché ciò accada, deve previamente svolgersi il vaglio richiesto dall'art. 189 c.p.p., in tutte le sue componenti. Detto altrimenti, l'operatività dell'art. 189 c.p.p. con riferimento alle prove derivanti da atti di indagine atipici, per come ricostruito finora, postula uno sbarramento all'introduzione *de plano* nel fascicolo dibattimentale dei risultati conoscitivi in tal modo acquisiti. Tanto vale e con riferimento ai verbali eventualmente redatti e con riferimento ai supporti contenenti gli elementi raccolti: da questo punto di vista, anzi, vale la pena di evidenziare come appaia del tutto fuori fuoco il riferimento, operato dalle Sezioni unite, all'art. 134, comma 4, c.p.p.: è questa una norma che si riferisce alle modalità di documentazione dello svolgimento degli atti e non già ai risultati conoscitivi eventualmente acquisiti per il loro tramite.

Ciò precisato in merito alla prima delle questioni formulate, può passarsi alla seconda, (ovvero quella relativa alla possibilità di introdurre nella fase delle indagini conoscenze acquisite in violazione delle prerogative costituzionali): tutto quanto finora ricostruito non significa affatto che elementi di conoscenza ottenuti in spregio dei diritti fondamentali possano avere cittadinanza nel procedimento, né nella fase dibattimentale, né in quella delle indagini. Una soluzione del genere, infatti, è del tutto estranea alla logica della pronuncia Prisco così come alla ricostruzione dogmatica operata in tema di prove incostituzionali. In altre parole, che si faccia leva su tale ultima teoria o sulle conclusioni raggiunte dalle Sezioni unite nel 2006 per escludere dal procedimento le

conoscenze acquisite in spregio dei diritti fondamentali, non v'è dubbio che tale conclusione non potrebbe essere limitata alla fase dibattimentale, ma si estenderebbe a quella delle indagini. Se si accogliesse la teoria della prova incostituzionale, ciò deriverebbe dall'operatività dell'art. 191 c.p.p. in ogni stato e grado del procedimento; se, invece, si aderisse ai principi espressi dalle Sezioni unite Prisco, si tratterebbe di un corollario della più generale regola dell'operatività, in fase di indagine, delle norme relative al sistema delle prove in quanto compatibili: non v'è dubbio che tra queste rientri quella secondo la quale il sistema processuale pone un limite implicito all'ammissibilità[199] di risultati di conoscenza acquisiti in violazione delle prerogative fondamentali degli individui.

In considerazione di tutto quanto si è appena visto, i principi espressi dalla giurisprudenza in merito alle prove atipiche incidenti sui diritti fondamentali si applicano senz'altro agli atti di indagine atipici. Ciò, però, non sempre conduce a risultati del tutto soddisfacenti, soprattutto laddove si tratti di atti ad alto contenuto tecnologico.

5. L'intrinseca inadeguatezza dello stato dell'arte in tema di prova atipica impattante sui diritti fondamentali con riferimento alle investigazioni *online*.

L'assetto delineato dalle pronunce sopra richiamate in materia di prova atipica incidente sui diritti fondamentali risulta per diverse ragioni insoddisfacente, in particolare quando si tratta di atti investigativi ad alto contenuto tecnologico.

Già su un piano generale, la breve disamina delle pronunce della giurisprudenza costituzionale e di legittimità in materia dimostra come le argomentazioni e le soluzioni adottate siano, nonostante il carattere ormai risalente del dibattito sul punto, ancora soggette a un certo tasso di variabilità che mal si concilia con l'aspettativa di maggiore rigore e prevedibilità delle restrizioni connaturata a qualsivoglia attività processuale impattante su diritti di rango costituzionale.

Tanto senza considerare come non manchino, nella ricostruzione operata in alcune pronunce in merito alle garanzie necessarie per la restrizione di determinate prerogative, passaggi argomentativi in qualche misura apodittici e dalle conseguenze applicative a

[199] Essendo in fase di indagini, tale termine va inteso in senso atecnico, ma l'effetto è il medesimo, ovvero quello di evitare che conoscenze acquisite in violazione dei diritti fondamentali possano essere legittimamente adoperate, quale che sia la fase procedimentale di riferimento.

dir poco incerte. Il riferimento è, ad esempio, alla teoria delle "garanzie minime", elaborata dalla Corte costituzionale fin dalla sentenza n. 81 dell'11 marzo 1993[200], in materia di tabulati telefonici, che, pur riconducendo alle prerogative di cui all'art. 15 Cost. la tutela dei dati esteriori delle comunicazioni telefoniche e telematiche ha, nondimeno, concluso nel senso che per l'acquisizione della documentazione relativa agli stessi sia sufficiente – pur in mancanza di una disciplina normativa sul punto – un decreto motivato dell'autorità giudiziaria. Tanto, evidentemente, sul presupposto – la cui veridicità è tutta da dimostrare[201] – che l'acquisizione dei dati esterni del traffico telefonico incida, sì, sulla libertà e segretezza delle comunicazioni ma in misura più lieve di un'intercettazione. Soluzione che pare, quanto meno, arbitraria nella misura in cui sembra obliterare radicalmente l'esistenza di una riserva di legge all'interno della disposizione costituzionale richiamata.

Lo stesso dicasi con riguardo alla soluzione adottata dalle Sezioni unite *Prisco*[202] con riferimento alle videoriprese in luoghi non domiciliari ma, nondimeno, coperti da un'aspettativa di riservatezza. In tal caso, secondo le Sezioni unite, la misura inciderebbe esclusivamente sul diritto alla riservatezza – ricondotto al combinato disposto degli artt. 2 Cost., 8 della Convenzione europea dei diritti dell'uomo e 17 del Patto internazionale sui diritti civili e politici – con la conseguenza che, anche in questo caso, sarebbe sufficiente un decreto motivato dell'autorità giudiziaria.

Soluzione, quest'ultima, che non sembra tenere conto del fatto che la riconduzione delle prerogative impattate dalla misura investigativa anche all'art. 8 della Convenzione avrebbe implicato il riconoscimento della necessaria operatività delle garanzie ivi sancite, tra le quali l'esistenza di una base legale per l'adozione della misura.

Trapiantate nel campo delle investigazioni *online*, le argomentazioni "fluide" adottate dalla giurisprudenza si dimostrano viepiù inadeguate. A fronte del vero e proprio sdoganamento di strumenti investigativi atipici a contenuto altamente tecnologico, simili soluzioni rischiano di divenire il viatico per legittimare ogni forma di intrusione nelle aspettative di riserbo dei singoli, complice anche la mancanza di approdi esegetici

[200] Corte Cost., 11 marzo 1993, n. 81, in *Giur. It.*, 1995, 1, c. 117 s.

[201] Sul punto, volendo, CASCONE, *La Corte di Giustizia dell'Unione Europea definisce le condizioni per la legittimità delle normative nazionali in materia di acquisizione dei tabulati. Le ripercussioni sull'ordinamento italiano della sentenza del 2 marzo 2021 (c-746/18) nel caso H.K.*, in *Cass. pen.*, 2022, 2, 419 ss.

[202] Sez. un., 28 marzo 2006, n. 26795, Prisco, cit.

stabili in tema di definizione della base costituzionale dei diritti connessi all'uso delle nuove tecnologie. Si finisce, in tal modo, per affidare alla sensibilità del singolo giudice la gradazione della minore o maggiore intrusività delle misure investigative di volta in volta adottate sui diritti costituzionalmente tutelati e, di conseguenza, la scelta di ritenere sufficiente un provvedimento motivato del pubblico ministero per l'adozione della misura ovvero reputare necessaria una base legislativa specifica in ossequio alla riserva di legge. Tanto con ricadute rilevantissime sul piano pratico, atteso che solo in questo secondo caso dovrebbero considerarsi sempre inutilizzabili i risultati conoscitivi acquisiti o inammissibili i relativi mezzi di prova.

Risultati altrettanto insoddisfacenti conseguono, poi, all'applicazione dei distinguo operati dalla giurisprudenza in tema di diritto alla riservatezza e tutela del domicilio alla materia dei controlli occulti da remoto.

Si è visto come, sul punto, le Sezioni unite abbiano adottato una soluzione esegetica tesa a distinguere l'intensità delle garanzie riconosciute ai singoli in materia di videoregistrazioni a seconda del luogo nel quale le stesse vengono realizzate, concludendo nel senso dell'assenza di qualsivoglia aspettativa di riservatezza in caso di comportamenti tenuti in luoghi pubblici o aperti al pubblico.

Addirittura, la Corte costituzionale è giunta a escludere l'operatività delle tutele previste dall'art. 14 Cost. nel caso di comportamenti che, pur tenuti all'interno di un luogo domiciliare, non siano assistiti dall'adozione, da parte dell'agente, di misure finalizzate a renderli non visibili a terzi[203].

Simili distinzioni non sono più sostenibili con riferimento ai nuovi mezzi di controllo occulto sempre più adoperati nel corso delle indagini penali. A dover essere messo in discussione è, in particolare, il dogma secondo il quale il singolo non nutre alcuna aspettativa di tutela del riserbo con riferimento ai comportamenti tenuti in luoghi

[203] Corte Cost., 7 maggio 2008, n. 149, in *Giur. cost.*, 2008, 3, 1825, ove si legge che «affinché scatti la protezione dell'art. 14 Cost., non basta che un certo comportamento venga tenuto in luoghi di privata dimora; ma occorre, altresì, che esso avvenga in condizioni tali da renderlo tendenzialmente non visibile ai terzi. Per contro, se l'azione – pur svolgendosi in luoghi di privata dimora – può essere liberamente osservata dagli estranei, senza ricorrere a particolari accorgimenti (paradigmatico il caso di chi si ponga su un balcone prospiciente la pubblica via), il titolare del domicilio non può evidentemente accampare una pretesa alla riservatezza; e le videoregistrazioni a fini investigativi non possono, di conseguenza, che soggiacere al medesimo regime valevole per le riprese visive in luoghi pubblici o aperti al pubblico. In una simile ipotesi, difatti, le videoregistrazioni non differiscono, sostanzialmente, dalla documentazione filmata di un'operazione di osservazione o di appostamento, che ufficiali o agenti di polizia giudiziaria potrebbero compiere collocandosi, di persona, al di fuori dell'abitazione».

pubblici[204]. Le tecnologie ad oggi disponibili consentono forme di controllo non ipotizzabili in passato, suscettibili di estendersi in un contesto spazio-temporale che non rende più praticabile una distinzione della specie di quella in argomento: detto altrimenti, non si comprenderebbe come una variabilità tanto spiccata delle garanzie connesse all'esecuzione di certe forme di controllo possa giustificarsi alla luce della mera presenza del soggetto in un'abitazione, nel privée di un locale o, semplicemente, sulla pubblica via a fronte della possibilità di sottoporre a una vera e propria sorveglianza occulta ogni suo spostamento e ogni suo comportamento[205].

Da questo punto di vista, risulta ancora più evidente l'esigenza, già precedentemente segnalata[206], di emancipare la tutela delle aspettative di riservatezza connesse all'uso degli strumenti tecnologici di ultima generazione sia da qualsivoglia distinguo relativo a contesti spaziali – reputati più o meno riservati –, sia dalla tipologia di dati e comportamenti che possono essere carpiti con il ricorso a tali strumenti.

[204] Si vedano, sul punto, le convincenti riflessioni di NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*. *Un tentativo di sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Cedam, 2020, 32 ss.

[205] Si vedano le considerazioni di BONINI, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Proc. pen. giust*., 2019, 2, 346, che in relazione alla tutela della vita privata osserva come «taluni dati presentano un livello di riservatezza elevato, in quanto relativi alla dimensione più intima dell'individuo (così è a dirsi, ad esempio, per i dati sanitari, sessuali, per i dati genotipici), altri sembrano presentare una maggiore evanescenza se sono singolarmente valutati, ma acquistano un rilievo tutt'altro che insignificante quando vengano trattati in modo massiccio o per lunghi archi temporali […] il profilo spaziale assume un rilievo non dirimente, o a causa della straordinaria attinenza del dato alla intimità della persona ovvero in ragione della particolare estensione dell'attività di apprensione delle informazioni personali, che intaccano la riservatezza dell'individuo anche quando abbiano ad oggetto comportamenti posti in essere in luoghi pubblici».

[206] Cfr. cap. 1, par. 3.3.

Capitolo III

ONLINE SEARCH (PERQUISIZIONE E SEQUESTRO *ONLINE*)

Sommario: 1. Perquisizione e sequestro: il tramonto del paradigma tradizionale; 1.1. Dallo spazio reale a quello virtuale: accresciute esigenze di tutela; 1.2. *Online search*: perquisizione e sequestro *online*; 2. L'incompatibilità della disciplina codicistica; 2.1. Prime applicazioni giurisprudenziali; 2.2. Le criticità della ricostruzione operata nelle pronunce di legittimità in materia; 3. Il piano costituzionale; 3.1. I diritti incisi; 3.2. Le conseguenze della violazione sul piano processuale; 4. La perquisizione e il sequestro *online* come categoria probatoria: una proposta *de iure condendo;* 4.1. Alcune preliminari coordinate: il principio di proporzionalità; 4.1.1. (segue) La riserva di giurisdizione; 4.1.2. (segue) I percorsi tracciati dalle Corti europee in punto di legittimità delle restrizioni al diritto alla vita privata; 4.1.3. (segue) La regolamentazione degli aspetti tecnici; 4.2. Le garanzie antecedenti all'esecuzione della misura: presupposti applicativi e autorità competente; 4.3. Le garanzie connesse all'esecuzione della misura; 4.4. Le garanzie successive all'esecuzione della misura: controlli, rimedi e limiti all'utilizzazione dei dati in altri procedimenti.

1. Perquisizione e sequestro: il tramonto del paradigma tradizionale.

Tra gli istituti tradizionali del processo penale, la perquisizione e il sequestro rappresentano due classici mezzi di ricerca della prova caratterizzati da uno spiccato collegamento funzionale, essendo la prima generalmente finalizzata all'esecuzione del secondo.

La perquisizione consiste, infatti, in un'attività di ricerca eseguibile in maniera coercitiva, suscettibile di avere ad oggetto persone o luoghi e prodromica al rinvenimento e alla conseguente apprensione del corpo del reato o delle cose pertinenti al reato oppure all'arresto dell'imputato o dell'evaso (art. 247 c.p.p.). Il sequestro, dal canto suo, consiste nell'apposizione, su determinate cose, di un vincolo di indisponibilità che, nel caso di sequestro probatorio – ovvero la tipologia di sequestro che viene in rilievo in questa sede – è finalizzato ad assicurare al procedimento penale possibili prove: per questo, esso è destinato a ricadere sul "corpo del reato" o sulle "cose pertinenti" al reato.

Connaturato all'esecuzione di tali mezzi di ricerca della prova è il tendenziale conflitto tra le esigenze di accertamento del reato e i diritti di libertà, nel senso che l'esecuzione di simili atti comporta un'incidenza su taluni diritti costituzionali più o meno intensa a seconda dei casi. Così, ad esempio, l'esecuzione di una perquisizione locale in un'abitazione incide sull'inviolabilità del domicilio, mentre una perquisizione eseguita sulla persona incide sulla libertà personale della stessa. Quanto al sequestro, l'apposizione di un vincolo di indisponibilità, sia pure temporaneo, sulla cosa incide generalmente sui diritti di proprietà del titolare della medesima, ma può restringere altresì altre libertà costituzionalmente tutelate, come quella di iniziativa economica prevista dall'art. 41 Cost.[207]. Tale conflitto è, poi, ancora più evidente nel caso in cui tali misure riguardino beni di soggetti terzi rispetto all'accertamento condotto in sede penale: in tal caso, infatti, nell'ideale bilanciamento tra i contrapposti interessi in campo occorre considerare quello del terzo a essere tenuto indenne dalle conseguenze di una vicenda processuale che non lo riguarda direttamente, non essendo in prima persona sospettato o accusato della commissione di alcun reato.

La disciplina codicistica in materia rappresenta proprio il frutto del tentativo legislativo di addivenire a una composizione ragionevole e proporzionata di simili conflitti e, nel corso degli anni, è stata destinataria di interventi di adeguamento ai cambiamenti che l'avanzamento tecnologico ha imposto anche in tale ambito, rimodulando l'assetto degli interessi in campo e richiedendo un mutamento dei termini di tale bilanciamento.

In conseguenza del progresso tecnologico, la disciplina normativa dettata in materia di perquisizione e sequestro probatorio, concepita per un contesto caratterizzato dalla materialità, si è ben presto dimostrata inadeguata: lo stesso linguaggio adottato dal legislatore nell'indicazione del "corpo del reato e delle cose pertinenti al reato" nella normativa in materia di perquisizione (art. 247 c.p.p.) e sequestro (art. 253 c.p.p.) suggerisce il riferimento a entità dotate di una qualche fisicità[208].

Sempre più spesso, però, dati e informazioni potenzialmente rilevanti per l'accertamento penale si trovano custoditi non già in luoghi fisici ma digitali: ne è conseguito, inevitabilmente, l'interrogativo se il termine "cosa" adoperato nelle disposizioni normative in argomento fosse suscettibile di ricomprendere anche i dati

[207] CAMON, *Le prove*, in AA.VV., *Fondamenti di procedura penale*, Cedam, 2021, 372.

[208] SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, 217 ss.

informatici, normalmente ascritti al mondo dell'immaterialità[209] o dell'idealità[210], tra le *res* suscettibili di sequestro e tra i luoghi sottoponibili a perquisizione.

Con la Legge di "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica", fatta a Budapest il 23 novembre 2001, vale a dire la l. 18 marzo 2008, n. 148, il legislatore ha fugato ogni dubbio: con tale intervento normativo la disciplina concernente alcuni mezzi tradizionali di ricerca della prova (tra cui perquisizioni, ispezioni e sequestri) è stata interpolata con disposizioni espressamente legittimanti la ricerca e l'apprensione dei dati informatici in contesti digitali[211]. L'opzione legislativa, dunque, è stata quella di adattare i tradizionali schemi giuridici in materia a tali nuovi strumenti informatici di ricerca della prova, mantenendo sostanzialmente invariate, salvo alcune differenze di rilievo[212], le scansioni e le garanzie procedimentali già previste per l'esecuzione di tali mezzi di ricerca della prova in contesti non digitali.

Si è, in tal modo, intrapresa la via più semplice per l'adeguamento della normativa interna a quella internazionale pattizia, ignorando, però, alcune esiziali differenze intercorrenti tra sequestri e perquisizioni tradizionali e quelli informatici, in quanto la natura digitale delle *res* rende oltremodo problematico la riconducibilità delle due tipologie di atti ad un unico schema legale. Le perquisizioni e i sequestri informatici

---

[209] Così, MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, 12, 4509; MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, 3, 1261, che parla di «assoluta assenza di concrete determinazioni spaziali»; si veda anche DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc*., 2011, 2, 284, il quale, tuttavia, precisa che l'immaterialità del dato non implica che lo stesso sia privo di qualsivoglia fisicità, atteso che trattasi pur sempre di impulsi elettrici che rispondono ad una sequenza prestabilita; per la tesi per la quale, atteso che il dato informatico è pur sempre incorporato mediante segnali elettrici, luminosi o magnetici su basi materiali, sarebbe preferibile parlare di "dematerializzazione", piuttosto che di immaterialità, si veda TORRE, *Il riesame del sequestro probatorio di documenti informatici*, in *Giur. it*, 2019, 6, 1439. Nel senso che per "immaterialità" debba intendersi che la rappresentazione del dato esiste indipendentemente dal supporto fisico nel quale lo stesso è incorporato, si veda TONINI, *Documento informatico e giusto processo*, in *Dir. pen. e proc.*, 2009, 4, 403.

[210] Si veda, ad esempio, LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, 4, 1525, secondo la quale il documento informatico si differenzia da quello tradizionale per la procedura, ideale e non reale, di saldatura del messaggio sul supporto materiale.

[211] Tramite tali modifiche, peraltro, il legislatore ha inteso espressamente assimilare alle "cose" i dati informatici. Prova ne sia, ad esempio, la formulazione dell'articolo 260 che, al primo comma, fa espressamente riferimento, per l'individuazione delle modalità attraverso le quali procedere all'apposizione dei sigilli, alla natura delle "cose", prevedendo che il sigillo possa apporsi elettronicamente o informaticamente.

[212] Il riferimento è, ad esempio, alle disposizioni finalizzate ad imporre agli inquirenti il ricorso a misure tecniche adeguate ad assicurare la conservazione degli originali dei dati e ad impedire la loro alterazione (si veda, ad esempio, il comma 1 *bis* dell'art. 247 c.p.p.).

determinano un mutamento non solo quantitativo, ma anche qualitativo delle misure in questione, in ragione dell'enorme massa di informazioni acquisibili attraverso la loro esecuzione, oltre che a causa della diversa e più estesa ampiezza dei beni giuridici incisi dalla stessa.

Tali aspetti meritano di essere debitamente analizzati prima di passare al tema relativo alle perquisizioni e ai sequestri *online*, atteso che i referenti codicistici più contigui a tali operazioni appaiono essere proprio le norme in materia di perquisizioni e sequestri informatici. Nondimeno, come si vedrà, proprio lo svolgimento da remoto delle operazioni rappresenta un fattore suscettibile di "stressare" ulteriormente le categorie giuridiche in argomento e di impedire una convincente *reductio ad unitatem*.

1.1. Dallo spazio reale a quello virtuale: accresciute esigenze di tutela.

Nonostante la scelta operata dal legislatore nel disciplinare la ricerca e l'apprensione di dati informatici all'interno di spazi digitali sia stata quella di ricorrere alle tradizionali categorie di mezzi di ricerca della prova, uno sguardo attento all'attuale sistemazione della materia consente di cogliere alcune non secondarie differenze esistenti tra un sequestro e una perquisizione tradizionali e i loro corrispettivi informatici. Gli stessi sono senz'altro accomunati dalla finalità perseguita, che in entrambi i casi è quella di raccogliere elementi utili a fini di prova nel processo penale che dovesse instaurarsi a seguito delle indagini preliminari.

La natura digitale dell'oggetto su cui ricade l'attività investigativa comporta, tuttavia, un disallineamento rispetto agli istituti tradizionali quanto meno su un triplice piano.

Anzitutto, la sistematica riproducibilità dei dati informatici in esemplari di per sé indistinguibili dall'originale[213] pone il problema dell'effettività dei rimedi avverso un'applicazione illegittima della misura. A tale riguardo, si era, infatti, inizialmente consolidato nella giurisprudenza di legittimità un orientamento che negava la permanenza dell'interesse a impugnare il decreto di sequestro nel caso di estrapolazione dei dati con copia forense e conseguente restituzione degli originali[214]. Orientamento,

[213] Risultato che viene ottenuto con la tecnica di *bitstream image*, consistente nell'effettuazione di una copia del dato informatico *bit a bit* con la conseguente creazione di un dato "clone" di quello "originale". Sul punto, si veda ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen. e proc.*, 2008, 6, 62 ss.

[214] Per tutte, Sez. un., 24 aprile 2008, n. 18253, Tchmil, in *Cass. pen.*, 2008, 4031, con osservazioni di Aprile. Tale indirizzo giurisprudenziale aveva la conseguenza paradossale di negare in maniera

poi, ribaltato dalle Sezioni unite della Suprema Corte[215], che hanno precisato che a determinate condizioni – ovvero quando il ricorrente deduca un interesse concreto e attuale alla esclusiva disponibilità dei dati – la restituzione degli originali dei dati sottoposti a sequestro mediante copia informatica non fa venir meno l'interesse al riesame[216]. Tanto in quanto il valore del dato informatico può risiedere proprio nell'esclusione di altri dall'apprensione e dalla conoscenza del suo contenuto, sicché la restituzione degli originali, tendenzialmente, non fa venir meno la situazione di spossessamento conseguente all'apposizione del vincolo. In tali casi, atteso che il documento proietta il suo valore anche sulla copia, permane un interesse a impugnare al fine di riottenere l'esclusiva disponibilità del dato.

Simile conclusione rappresenta l'inevitabile conseguenza della presa d'atto del secondo elemento differenziale enucleabile nella comparazione tra la declinazione tradizionale e quella informatica degli istituti in discorso, consistente nel fatto che una perquisizione e un sequestro informatici hanno strutturalmente un'incidenza non limitata ai soli diritti dominicali sui beni oggetto dell'attività investigativa[217].

Infine – ma i temi sono strettamente correlati – non sfugge come il risultato investigativo raggiungibile per il tramite di una perquisizione e di un sequestro informatico non sia né quantitativamente, né qualitativamente paragonabile a quello che

---

sistematica l'ammissibilità del riesame avverso il decreto di sequestro probatorio proprio nei casi nei quali l'esigenza di un rimedio effettivo è maggiormente avvertita alla luce dell'incidenza della misura su diritti ulteriori rispetto al mero diritto di proprietà.

[215] Sez. un., 20 luglio 2017, n. 40963, Andreucci, in *Cass. pen.*, 2018, 1, 131, con nota di RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio del materiale informatico*.

[216] Sul punto deve segnalarsi una recente pronuncia della Corte di cassazione che ha ulteriormente precisato i contorni dell'onere di allegazione del ricorrente con riferimento alla sussistenza del requisito dell'interesse all'esclusiva disponibilità dei dati. Molto opportunamente, la Corte ha evidenziato che quanto la misura ha ad oggetto dispositivi per loro natura destinati a contenere dati informatici di natura strettamente personale (nel caso di specie, si trattava di *smartphone* e *tablet*) è sufficiente che il ricorrente deduca la presenza di siffatti dati nel dispositivo, essendo ultronea la pretesa che fornisca altresì la pleonastica dimostrazione, in termini positivi, dell'interesse a possedere tali dati in via esclusiva. Cfr. Sez. VI, 3 febbraio 2022, n. 18502, inedita.

[217] Evidenzia che mentre un sequestro ordinario incide normalmente sul solo diritto di proprietà del titolare del bene, il sequestro informatico comporta una intrusione nella sfera di riservatezza dell'utilizzatore del sistema, MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen*., 2012, 2, 708. Si veda, altresì, DANIELE, *La prova digitale nel processo penale*, cit., 289, che relativamente alle indagini informatiche osserva che «la loro capacità lesiva della *privacy* è addirittura superiore a quella delle intercettazioni; queste ultime si limitano a carpire le informazioni che la persona intercettata ha deciso di rivelare ad altri, mentre l'analisi dei sistemi informatici e delle reti possono rivelare il contenuto di intere esistenze: abitudini, opinioni politiche, preferenze di ogni genere. In ogni caso, dati riservati che nulla hanno a che fare con la commissione dei reati, e che sono facilmente divulgabili proprio grazie alle tecnologie informatiche e ad internet, in grado di renderle conoscibili da un numero sterminato di persone».

rappresenta il frutto di una perquisizione o di un sequestro "ordinari", comportando normalmente l'apprensione di un quantitativo di dati, informazioni e documenti, sostanzialmente inimmaginabili neppure nella più fortunata delle perquisizioni tradizionali. Tutto ciò, peraltro, con una strabiliante semplicità, essendo sufficiente lo svolgimento di poco più di una manciata di operazioni sul dispositivo informatico. In questo senso, le differenze esistenti, su un piano quantitativo, tra un sequestro informatico e uno "ordinario" sono suscettibili di riverberarsi sul piano qualitativo della misura, modificandone l'ordinaria fisionomia di strumento di acquisizione di materiale utile alla prova dei fatti in mezzo dalle potenzialità esplorative spiccate, vista la ingente quantità di dati acquisibili.

Non a caso, è affermazione ormai costante nella giurisprudenza di legittimità degli ultimi anni quella per cui in materia di sequestro informatico non si possa prescindere dal rispetto dei principi di proporzionalità e adeguatezza[218]. Tanto implica, anzitutto, che sia di regola illegittima l'acquisizione indiscriminata dell'intero contenuto di un sistema informatico, trattandosi di una misura suscettibile di travalicare i confini segnati dalle specifiche esigenze probatorie perseguite mediante l'apposizione del vincolo; e, in secondo luogo, che rilievo fondamentale ai fini della verifica dell'effettiva proporzionalità della misura assuma la motivazione del decreto che dispone il sequestro, gravando sull'autorità giudiziaria l'onere di motivare le ragioni per le quali la *res* si reputa pertinente al reato e la sua apprensione necessaria per la prova dei fatti. Non v'è dubbio, infatti, che anche nel caso di sequestro informatico il vaglio di proporzionalità si debba effettuare sulla scorta delle indicazioni fornite dalla giurisprudenza di legittimità in tema di sequestro probatorio[219].

Conseguentemente, la motivazione del decreto di sequestro in relazione alla sussistenza *ex ante* dei presupposti applicativi dello stesso, con particolare riferimento alle esigenze probatorie da soddisfare con l'esecuzione della misura e, ancor prima, alla pertinenza al reato delle *res* sottoposte a vincolo, rappresenta *condicio sine qua non* ai fini della

[218] Si vedano, in questo senso, Sez. VI, 24 febbraio 2015, n. 24617, Rizzo, in *Cass. pen. 2016*, 186, con nota di Schena e *Arch. n. proc. pen.*, 2016, 269, con nota di Costanzi; Sez. VI, 11 novembre 2016, n. 53168, Amores; Sez. un., 20 luglio 2017, n. 40963, Andreucci, cit.; Sez. VI, 14 novembre 2018, n. 4857, in *Guida* dir., 2019, 83; Sez. V, 17 maggio 2019, n. 38456; Sez. VI, 26 settembre 2019, n. 43556; Sez. VI, 4 marzo 2020, n. 13166.

[219] Sez. un., 19 aprile 2018, n. 36072, in *Cass. pen.*, 2018, 4088, con commento di GRAMUGLIA, *Le sezioni unite tornano sul confine dell'onere di motivazione del decreto di sequestro probatorio del* corpus delicti, in *Dir. pen. cont.*, 2018, 9.

verifica di stretta necessità della misura. Inoltre, la necessità di una motivazione dettagliata in ordine alla "utilità" probatoria attesa dall'esecuzione dell'atto si pone in naturale *continuum* funzionale con il successivo controllo di legittimità che la legge processuale affida al giudice dell'impugnazione, eventualmente adito da quanti subiscano l'imposizione del vincolo.

L'applicazione del principio di proporzionalità alla materia, infatti, implica la l'operatività di garanzie non solo antecedenti – come è quella rappresentata dall'onere di adeguata motivazione del decreto – ma anche successive all'esecuzione della misura – consistenti primariamente nel controllo *ex post* di legittimità della stessa effettuato dal giudice penale proprio sulla base del perimetro cognitivo delineato dalla motivazione del provvedimento[220].

Il convergere di tali garanzie dovrebbe, dunque, assicurare il rispetto del principio di stretta necessità e adeguatezza della misura. Tanto, evidentemente, in un contesto nel quale assume assoluta centralità il carattere palese dell'atto investigativo, che contribuisce ad assicurare la proporzionalità – e, dunque, la legittimità – della misura non solo nel momento successivo alla sua attuazione (tramite il controllo giudiziale di cui si è appena detto) ma altresì contestualmente allo svolgimento delle operazioni. Momento, quest'ultimo, nel quale risulta fondamentale il diritto del difensore di fiducia di assistere al compimento dell'atto e di verificare l'effettiva continenza dello stesso e la riconducibilità delle operazioni di ricerca e apprensione al perimetro tracciato dal decreto motivato di perquisizione e sequestro.

Va da sé che l'effettività di tali garanzie, rilevante per qualsiasi attività di sequestro e perquisizione, risulta viepiù fondamentale in materia di perquisizione e sequestro operati in spazi digitali, in ragione delle più spiccate potenzialità invasive connaturate all'esecuzione di simili attività.

1.2. *Online search*: "perquisizione e sequestro" *online*.

Si sono già tracciati, nel capitolo 1, i principali elementi differenziali tra le due macrocategorie di attività investigative esperibili *online*: l'*online search* e l'*online surveillance.* Si è altresì evidenziato, in quella sede, come la distinzione tra le due– utile

[220] Sull'effettività di simili garanzie in caso di sequestro informatico e sulle criticità della ricostruzione giurisprudenziale in materia si veda, volendo, CASCONE, *Il sequestro informatico nel prisma del principio di proporzione*, in *Dir. pen. e proc.*, 2022, 1, 123 ss.

sul piano teorico al fine di individuare le principali caratteristiche distintive delle due tipologie di attività – sconti un certo tasso di approssimazione e variabilità non solo in ragione del fatto che alcune attività di ricerca e acquisizione sembrano porsi sul crinale tra le due categorie, ma anche in conseguenza del concreto uso che viene effettuato dello strumento tecnologico in questione[221].

Sulla distinzione in discorso, ad esempio, influisce in maniera rilevante il fattore temporale: vale a dire, cioè, che indipendentemente dalla tipologia di attività svolta e dalla natura dei dati oggetto di attenzione investigativa, il carattere reiterato o perdurante dell'attività stessa è elemento da tenere in considerazione onde determinare se si versi in un'attività di *search* o di *surveillance*. Su questo punto sembrano opportune ulteriori precisazioni al fine di delineare una categoria investigativa unitaria alla quale ascrivere attività di indagine aventi caratteristiche determinate e verificarne la riconducibilità agli istituti della perquisizione e del sequestro informatico analizzati nel paragrafo precedente.

Oggetto di analisi in questo capitolo sono esclusivamente le attività di ricerca ("perquisizione" *online*) ed eventuale apprensione ("sequestro" *online*) dei dati digitali che si pongono al di fuori del perimetro di una vera e propria attività di sorveglianza. Ci si riferisce, dunque, alle sole attività svolte – da remoto e occultamente – in un tempo contingentato e *una tantum* e non in modo continuativo o reiterato[222]. Tendenzialmente,

---

[221] Come si vedrà in seguito parlando delle possibili prospettive *de iure condendo*, infatti, onde mantenere distinte le due categorie anche sul piano operativo – così evitando l'aggiramento dei limiti normativi che dovrebbero prevedersi per l'una e per l'altra – risulta essenziale una minuziona regolamentazione che riguardi anche gli aspetti più strettamente tecnici della materia.

[222] Vale la pena di segnalare la classificazione operata da DI TARANTO, RUGGIERI e CUPELLI, *Nuove tecniche d'investigazione nell'era digitale: il* malware *di Stato*, in *Ciberspazio e dir*., 2017, vol. 18, n. 57, 125 e 149, sulla base di un parametro definito IA (indice di acquisizione), che dovrebbe contrassegnare il rapporto esistente tra la protrazione nel tempo dell'attività e il quantitativo di dati scaricati dagli inquirenti. Secondo gli autori, «se la raccolta dei dati estrapolati dal software di gestione della posta elettronica installato sul dispositivo – per esempio Outlook, Mail, Thunderbird, etc. –, al netto della particolare natura dell'informazione in esame, avverrà in modo "sporadico", allora questa potrà essere identificata come captazione informatica (*online search*); al contrario, se la medesima attività verrà eseguita in modo "ricorrente", fatta salva la necessità di quantificare quest'ultimo aggettivo, risulterà alquanto difficile non far ricadere tale attività nella categoria dell'intercettazione telematica (*online surveillance*). In conclusione, qualora i criteri elencati fossero complessivamente verificati e concordanti, si potrebbe affermare, con un elevato grado di certezza, di essere in presenza di una categoria piuttosto che dell'altra; diversamente, se uno o più criteri risultassero discordanti – come si rileva nell'esempio precedente – si dovrà valutare, caso per caso, l'inquadramento dell'attività esplicata, dapprima sotto il profilo tecnico e, successivamente, dal punto di vista giuridico». Conseguentemente, gli autori distinguono tra varie tipologie di attività, ovvero: «-- "perquisizione informatica da remoto", quando si procede all'acquisizione, mediante copia, dei dati contenuti all'interno di un dispositivo digitale in un arco temporale finito e che si caratterizza come singola operazione tecnica non reiterabile; -- "captazione informatica", quando viene effettuata una "perquisizione informatica da remoto" ma in maniera ripetuta.

dunque, tali attività hanno a oggetto dati già memorizzati nel dispositivo sottoposto a controllo remoto e, quindi, preesistenti all'effettuazione delle operazioni tecniche aventi come scopo la loro apprensione. Esse possono, poi, limitarsi all'acquisizione di un numero limitato di informazioni oppure realizzarsi tramite una copia integrale del contenuto del sistema informatico bersaglio. Deve, anzi, evidenziarsi come, quanto meno dal punto di vista degli inquirenti, questa possa essere reputata la modalità esecutiva preferibile in ragione delle caratteristiche dello stesso oggetto dell'attività investigativa. Ci si riferisce, in particolare, alla volatilità che caratterizza i dati informatici, facilmente modificabili e cancellabili sia per le caratteristiche funzionali e operative del sistema informatico, sia in ragione di possibili iniziative dell'utilizzatore del medesimo. Di conseguenza, l'esigenza di mettere al sicuro i dati informatici memorizzati nel dispositivo bersaglio ben potrebbe indurre gli inquirenti a procedere a un *download* integrale del contenuto del sistema informatico sui dispositivi in uso ai medesimi al fine di procedere solo successivamente alla ricerca e alla selezione del materiale utile all'indagine. Verrebbe, così, a replicarsi quella peculiare caratteristica propria del sequestro e della perquisizione informatici previsti e regolati dal codice di rito, consistente nella sistematica inversione dei rapporti tra i due mezzi di ricerca della prova[223]. Mentre, cioè, il sequestro penale consegue generalmente a una perquisizione che abbia consentito di rinvenire cose pertinenti al reato per cui si procede, nel caso di materiale informatico il sequestro tende a precedere la perquisizione, che viene svolta solo successivamente sul materiale già raccolto al fine di selezionarne la porzione utile per l'accertamento dei fatti.

Tale modalità operativa, pur suscettibile di inficiare il necessario requisito di proporzionalità della misura[224], nel caso di effettuazione delle operazioni *online* consentirebbe, d'altro canto, di assicurare il carattere istantaneo o, comunque, contingentato nel tempo dell'intervento sul sistema informatico bersaglio, così permettendo di distinguere con maggiore facilità l'attività di *search* da quella di

---

Tale attività si differenzia anche dalla intercettazione informatica perché la relativa attività di captazione avviene in modo "sporadico" (e, dunque, a basso indice IA); -- "intercettazione informatica", quando l'attività di acquisizione del dato digitale non avviene in maniera sporadica – come nel caso della captazione informatica – ma in modo reiterato, presentando, dunque, un elevato IA».

[223] MOLINARI, *Questioni in tema di perquisizione e sequestro*, cit., 708.

[224] Non essendo svolta una previa verifica in ordine alla pertinenza dei dati sottoposti a vincolo e alla necessità degli stessi ai fini dell'accertamento, una simile modalità operativa assume, infatti, sistematicamente i contorni di una restrizione sproporzionata del diritto di riservatezza informatica del titolare dei dati. Volendo, sul punto, CASCONE, *Il sequestro informatico*, cit., 123 ss.

surveillance. È ovvio, infatti, che maggiore è la durata delle operazioni finalizzate alla ricerca e selezione dei dati, maggiore è il rischio di un assottigliamento del confine tra le due categorie di attività oggetto di analisi. Tanto in quanto nel corso delle operazioni di ricerca e selezione del materiale è non solo possibile, ma anzi altamente probabile che nel dispositivo informatico si accumulino nuovi contenuti, anche in ragione dell'uso che potrebbe farne l'utilizzatore. Potrebbero, in tal modo, essere captati dati non preesistenti all'inizio delle operazioni ma formati successivamente. A rigore, una simile acquisizione dovrebbe ascriversi al perimetro della *online surveillance* piuttosto che dell'*online search*. Va ribadito, infatti, che sono momentaneamente fuori dal campo dell'indagine le attività svolte in maniera dinamica tramite l'acquisizione progressiva di dati informatici anche non ancora formati sul dispositivo bersaglio al momento dell'inizio dell'attività investigativa[225]. Trattasi, in quest'ultimo caso, di attività astrattamente assimilabile all'intercettazione, pur non essendo la categoria in argomento sempre adeguata in ragione della natura anche non comunicativa dei dati captabili tramite l'attività di sorveglianza.

A quest'ultimo proposito, sembra opportuno spendere alcune ulteriori considerazioni al fine di delineare in maniera più netta il confine tra l'attività investigativa di cui si discorre e quella, che a primo acchito potrebbe sembrare assimilabile, di cui all'art. 266 *bis* c.p.p. Tanto con l'avvertenza che quanto si dirà in questa sede è utile a tracciare il confine non solo tra le attività di *online search* e *seizure*[226] e quelle di intercettazione telematica, ma altresì – e anzi, soprattutto – tra queste ultime e la categoria dell'*online surveillance* che sarà trattata nel prossimo capitolo, fermo restando che in quella sede il tema verrà ulteriormente ripreso e approfondito.

La formulazione dell'art. 266 *bis* c.p.p. potrebbe indurre a ritenere che l'oggetto dell'attività captativa ivi prevista sia notevolmente più esteso di quello di cui al precedente art. 266 c.p.p. La norma, infatti, fa riferimento a «l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi». Tanto ha, inizialmente, indotto la giurisprudenza a interpretare la disposizione nel senso che la stessa consentisse l'acquisizione di qualsivoglia dato (o *bit*) presente e "in movimento" su un sistema informatico, indipendentemente dal fatto che lo stesso fosse oggetto di un'attività di comunicazione in senso stretto tra due o più soggetti

[225] Del tema si parlerà nel prossimo capitolo.
[226] D'ora in poi, più semplicemente, "*online search*".

mediante l'uso del sistema telematico o informatico[227]. Tale soluzione, peraltro, è stata ripresa anche da una più recente pronuncia di legittimità del 2016[228]. Secondo tale lettura, dunque, il legislatore avrebbe inteso introdurre una tipologia di intercettazione avente caratteristiche distinte – e un raggio applicativo ben più ampio – rispetto a quelle che la giurisprudenza ha ricostruito con riferimento all'attività tradizionale di intercettazione.

In mancanza di una definizione codicistica del concetto di "intercettazione", infatti, fin dal 2003, con il filone ermeneutico inaugurato dalle Sezioni Unite Torcasio[229], la giurisprudenza è orientata nel senso che si sia in presenza di un'attività intercettiva laddove ricorrano tre presupposti: la captazione occulta e contestuale di una comunicazione o conversazione tra più soggetti; la terzietà del captante; la volontarietà dell'atto comunicativo, vale a dire che oggetto della captazione deve essere un atto finalizzato a trasmettere a un altro soggetto il contenuto di un pensiero tramite l'uso della parola o mediante altri atteggiamenti comunque idonei a manifestarlo[230]. Secondo l'indirizzo ermeneutico in commento, invece, le intercettazioni telematiche si caratterizzerebbero per consentire altresì la captazione di flussi di dati indipendentemente dall'esistenza di una comunicazione tra due o più soggetti avente le caratteristiche appena menzionate.

Una simile conclusione non appare condivisibile per svariate ragioni che, però, è più opportuno analizzare nel prossimo capitolo[231]. Per quanto di rilievo in questa sede, infatti, neppure la lettura tanto ampia del concetto di intercettazione telematica offerta

---

[227] Sez. un., 13 luglio 1998, n. 21, Gallieri, in *Foro it.*, 1999, 2, 87, secondo la quale «appare evidente che la novità della citata previsione non è rappresentata dall'ammissibilità di intercettare il contenuto di conversazioni tra persone che vengono trasmesse con il sistema elettronico numerico oggi adottato nella telefonia, che già poteva farsi rientrare nell'art. 266, proprio perché detta norma (con il riferimento testuale "altre forme di telecomunicazione") rinviava ad ogni specie di telecomunicazione, idonea di per sé a convogliare le conversazioni tra persone. La novità è rappresentata, invece, ad avviso di questo Collegio, non solo dall'aver esteso l'ambito di ammissibilità delle intercettazioni ai procedimenti aventi ad oggetto i "computer crimes", ma dall'aver consentito l'intercettazione dei flussi di dati numerici (bit), nell'ambito dei singoli sistemi oppure intercorrente tra più sistemi. Cioè, l'oggetto della tutela del Capo III concerne a questo punto, a seguito della modifica legislativa, non solo il contenuto delle conversazioni, con qualsiasi forma di telecomunicazione avvenga, ma tutti i dati informatici (sequenza di bit) in movimento nel sistema elettronico della telefonia, dall'ingresso in rete alla destinazione, nelle fasi quindi dell'ingresso, elaborazione, registrazione, comprensivo delle interconnessioni con altre reti o stazioni intermedie di comunicazione».

[228] Sez. IV, 28 giugno 2016, n. 40903, Grassi, in *CED Cass*. n. 268228.

[229] Sez. un., 28 maggio 2003, n. 6747, Torcasio, in *CED Cass.*, n. 225465-468.

[230] Così la giurisprudenza di legittimità consolidata. Si vedano, *ex multis*, Sez. III, 7 luglio 2010, n. 37197; Sez. V, 17 novembre 2015, n. 11419; Sez. III, 21 novembre 2019, n. 15206.

[231] Cfr. cap. 4, par. 2.

dalla giurisprudenza sopra richiamata sembra suscettibile di ricomprendere le attività di *online search* di cui si discute. Secondo la soluzione ermeneutica in questione, infatti, pur potendo non avere ad oggetto dati comunicativi, l'intercettazione telematica rimarrebbe comunque caratterizzata dalla contestualità della captazione rispetto alla formazione del dato informatico appreso. Le attività di ricerca della prova di cui si discute in questa sede, al contrario, come già detto, sono solo quelle finalizzate all'apprensione dei dati preesistenti nel sistema informatico e non anche di quelli "in movimento" all'interno dello stesso.

Il tema, invece, come si vedrà, assume ben maggiore rilievo con riferimento alle attività di *online surveilance*, caratterizzate proprio dalla contestualità dell'apprensione dei dati rispetto al loro generarsi nel sistema informatico. Evidenti ragioni sistematiche, dunque, consigliano di rimandare l'analisi critica dell'indirizzo giurisprudenziale in commento al prossimo capitolo.

Volendo riassumere quanto detto finora, rientrano nell'ambito della categoria "perquisizione e del sequestro" *online*[232] ("*online search*") quelle attività finalizzate a una "setacciatura" temporalmente contingentata del sistema informatico bersaglio, con eventuale estrapolazione dei dati – preesistenti all'avvio delle operazioni – reputati utili per l'indagine tramite il *download* dei medesimi sui dispositivi informatici degli inquirenti.

Come si vedrà in seguito, una simile perimetrazione appare utile, al fine di procedere a un tentativo di inquadramento sistematico di tali attività, anche per individuare le prerogative individuali incise dalle attività in questione e, conseguentemente, verificare la spendibilità sul piano processuale dei risultati delle investigazioni condotte.

2. L'incompatibilità della disciplina codicistica.

Definiti con maggiore precisione i contorni della categoria investigativa oggetto di analisi, è possibile verificare la riconducibilità della stessa a istituti già regolati dal codice di rito.

Che la cosiddetta *online search* e il conseguente, eventuale, *online seizure* non trovino alcun convincente succedaneo nei mezzi di ricerca della prova tipici già regolati dalla

[232] Il riferimento alla perquisizione e al sequestro è, per ora, operato in senso atecnico e a meri fini di semplificazione, non essendo, come si vedrà, affatto pacifico che tali attività siano riconducibili agli istituti tradizionali.

legge è conclusione della quale non pare possibile dubitare soprattutto laddove, com'è corretto e inevitabile trattandosi di attività suscettibili di incidere su diritti fondamentali, si adotti un criterio d'analisi improntato al massimo rigore: vale a dire, cioè, che dinanzi ad attività incidenti su prerogative costituzionalmente protette dalla riserva di legge[233] assume particolare rilievo la verifica di coincidenza dei casi e dei modi della restrizione del diritto fondamentale con quelli previsti dall'istituto codicistico che rappresenta, caso per caso, l'oggetto della comparazione al fine della verifica di tipicità del mezzo di ricerca della prova[234]. L'esito negativo di una simile verifica comporta la scontata conclusione per la quale l'atto ha carattere innominato, con le conseguenze che si vedranno.

Nella ricerca di un istituto codicistico al quale ricondurre l'attività in questione appare del tutto scontato prendere le mosse dalla perquisizione e dal sequestro informatici introdotti nel nostro sistema giuridico in conseguenza dell'adozione della l. n. 48/2008. Sol che si guardi alla concreta disciplina prevista per l'esecuzione di tali mezzi di ricerca della prova, però, il paragone risulta quanto mai fallace.

Come si è già avuto modo di evidenziare, il suddetto intervento normativo si è, in realtà, limitato a rendere ammissibili, anche con riferimento ai dati informatici, i consueti strumenti della perquisizione e del sequestro. Se qualche novità può ravvisarsi nella nuova disciplina codicistica, questa appare limitata alla previsione secondo la quale le modalità operative concretamente adottate nello svolgimento dell'atto investigativo devono essere tali da assicurare la conservazione dei dati e ad impedirne l'alterazione. Per il resto, la disciplina applicabile rimane quella già prevista in materia di perquisizione e sequestri.

In dottrina si è evidenziato come già sotto il profilo della necessaria finalizzazione dell'attività di ricerca all'apprensione del corpo del reato e delle cose allo stesso pertinenti l'*online search* si distinguerebbe dalla perquisizione e dal sequestro codicistici. Secondo questa ricostruzione, tali ultimi istituti sarebbero caratterizzati dalla circoscrizione della ricerca in un perimetro ben definito – che è quello della necessaria pertinenza ai fatti di reato oggetto di accertamento – la cui effettiva continenza e proporzionalità è, almeno in teoria, assicurata dalla motivazione del decreto di

[233] Come è certamente nel caso di specie, cfr. *infra*, par. 3.1.

[234] MARCOLINI, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, in *Cass. pen*., 2010, 7-8, 2858.

perquisizione e sequestro, che deve contenere, oltre all'indicazione dei concreti elementi suscettibili di fondare l'integrazione dei requisiti di legittimità dell'atto, anche la determinazione, sia pure indiretta, delle cose al cui rinvenimento l'attività investigativa è mirata. L'ampiezza del "luogo" virtuale nel quale viene svolta la ricerca conferirebbe, invece, all'attività di *remote search* e *seizure* la caratteristica di prescindere in maniera pressoché sistematica dalla ricerca del corpo del reato e delle cose allo stesso pertinenti, trasformando lo strumento in questione in un mezzo connotato da potenzialità esplorative più elevate rispetto al caso in cui la ricerca sul sistema informatico si svolga in presenza[235]. Il rilievo, però, non sembra del tutto pertinente se solo si considera che simile caratteristica – ovvero quella di consentire lo svolgimento di attività di ricerca non connotate dal requisito della stretta pertinenzialità all'indagine in corso – appare, almeno astrattamente, propria anche del sequestro e della perquisizione informatici previsti dal codice, che pure si svolgono in un ambiente, quello digitale, estremamente più ampio di un qualunque luogo fisico sottoponibile a perquisizione. Non sembra, quindi, che l'elemento appena evidenziato si atteggi alla stregua di un vero e proprio *discrimen* tra le attività considerate.

Sotto altro profilo, poi, non pare metodologicamente corretto ravvisare un elemento differenziale tra due istituti o attività investigative in caratteristiche che non sono proprie della regolazione normativa delle stesse, ma di prassi degenerative che, in quanto tali, non dovrebbero influenzare, in un senso o nell'altro, valutazioni che devono rimanere su un piano strettamente giuridico. La tendenza delle investigazioni informatiche a sfociare in attività aventi carattere esplorativo e a fuoriuscire dai limiti di una ricerca mirata all'apprensione di cose determinate pertinenti al reato – dovuta, per l'appunto, alla ingente mole di dati acquisibili tramite l'analisi del contenuto dei sistemi informatici di uso comune – determina un incremento del rischio di adozione di provvedimenti giudiziari non adeguatamente motivati in merito al perimetro delle ricerche in relazione a qualsiasi attività investigativa avente carattere digitale, sia essa regolata o meno. Ciò, però, non è nella fisiologia delle cose. Trattasi, dunque, di un piano che dovrebbe rimanere estraneo alle valutazioni da svolgere in questa sede.

[235] GRIFFO, *Perquisizione informatica, … e dintorni*, in *Giur. pen. web*, 2019, 5, 3.

Coglie, invece, nel segno chi[236] evidenzia come il principale elemento differenziale tra le due attività sia rappresentato dal carattere occulto o palese delle stesse e, conseguentemente, dalle garanzie connesse allo svolgimento delle operazioni nei due casi. L'intervento legislativo del 2008, infatti, ha lasciato inalterato lo statuto di tutele connesso allo svolgimento dell'attività di ricerca e apprensione dei dati digitali che, dunque, continua ad essere un'attività a sorpresa ma palese, non eseguibile da remoto e i cui esiti restano soggetti ai consueti rimedi processuali. Connaturato alla *online search*, invece, parrebbe il carattere occulto dell'attività: se il soggetto che subisce l'intrusione fosse a conoscenza della stessa ben potrebbe agire tempestivamente al fine di vanificarne gli esiti, alterando o eliminando il contenuto del dispositivo informatico che, durante lo svolgimento delle operazioni, rimarrebbe nella sua disponibilità. Ciò determina, ovviamente, la radicale inoperatività delle garanzie previste dagli articoli 247 e 352 c.p.p. e dalle altre disposizioni di legge in materia di perquisizioni e sequestri[237], che risultano non solo inapplicabili (per la banale ragione che la loro operatività presuppone il carattere palese dell'atto), ma altresì del tutto inappaganti[238], atteso che la maggiore intrusività degli strumenti in questione presupporrebbe la messa a punto di un reticolato di garanzie ben più incisivo. In buona sostanza, si è dinanzi a "casi e modi" di aggressione del tutto divergenti da quelli previsti per una perquisizione o per un sequestro tradizionali, essendo diversi sia le modalità di aggressione del bene giuridico che viene in rilievo e le garanzie connesse allo svolgimento dell'atto, sia i rimedi e le forme di controllo che il titolare del medesimo può esperire in conseguenza della

[236] Così, CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. bras. dir. proc. pen*., 2017, 2, 489; IOVENE, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont*., 2014, 3-4, 340; MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, in AA.VV., *Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura*, a cura di Giarda, Giunta e Varraso, Cedam, 2018, 205; PARLATO, *Problemi insoluti: le perquisizioni on-line,* in AA.VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra e Orlandi, Giappichelli, 2018, 295; TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. pen. e proc.*, 2014, 6, 763; TROGU, *Intrusioni segrete nel domicilio informatico,* in AA.VV., *Le indagini atipiche*, a cura di Scalfati, Giappichelli, 2019, 577.

[237] Ci si riferisce, oltre alla conoscibilità dell'atto (di cui all'art. 250 c.p.p.), al diritto al deposito del verbale (art. 366 c.p.p.), all'assistenza del difensore nel corso dello svolgimento delle operazioni di perquisizione (art. 365 c.p.p.), al deposito del relativo verbale (art. 366 c.p.p.) e, ovviamente, alla possibilità di esperire il riesame (art. 257 c.p.p.)

[238] Come rileva correttamente BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali*, in *Riv. it. scienze giur*., 2017, 8, 348.

compressione del suo diritto[239]. Tanto con il paradossale risultato, esiziale in termini di proporzionalità della misura, che ad attività caratterizzate da un tasso di intrusività nettamente maggiore corrisponderebbe una drastica diminuzione delle garanzie applicabili.

Se, dunque, il carattere digitale dei dati acquisibili per il tramite di un'attività di perquisizione e sequestro informatici rende poco soddisfacente l'applicazione delle guarentigie dettate in relazione alle tradizionali categorie codicistiche, la natura occulta e remota dell'attività investigativa in argomento la rende del tutto insufficiente oltre che impraticabile.

Neppure sembra convincente un'assimilazione dello strumento in commento alle ispezioni informatiche, introdotte anch'esse nel 2008, per la banale ragione che queste «servono a fotografare la realtà esistente, senza alcuna apprensione di dati»[240].

Infine, anche una riconduzione all'istituto delle intercettazioni, sia pure informatiche o telematiche di cui all'art. 266 *bis* c.p.p., risulta insoddisfacente. Vero è, infatti, che trattasi di una disciplina più restrittiva di quella prevista in materia di sequestri e perquisizioni: a una selezione a monte delle fattispecie – solo quelle che raggiungono determinate soglie di gravità – per le quali può adottarsi la misura corrisponde, infatti, un arsenale di guarentigie ben più incisive[241], a partire da quella rappresentata dall'intervento autorizzativo del giudice. Nondimeno, come si è già detto, anche una lettura ampia del concetto di intercettazione telematica, tesa a ricomprendere non solo l'apprensione di dati strettamente comunicativi ma anche di qualsivoglia flusso di *bit*

[239] Si rinvia, sul punto, alla ricostruzione operata nel cap. 2, par. 2., in merito alle coordinate da tenere presenti onde verificare la tipicità o atipicità probatoria di nuovi strumenti di ricerca della prova.

[240] IOVENE, *Le c.d. perquisizioni online*, cit., 340.

[241] Nondimeno, occorre tenere presente quanto evidenziato da FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. e giust.*, 2016, 5, 124, in relazione al fatto che, a ben vedere, anche l'applicazione della disciplina delle intercettazioni si manifesterebbe, nel caso di specie, inadeguata quanto meno sul piano del controllo dell'autorità giudiziaria sullo svolgimento delle attività in razione della mancanza di conoscenze tecnico-informatiche che impedirebbe al pubblico ministero di individuare e disporre le operazioni idonee a carpire i dati di interesse: «in altri termini, quand'anche si volesse applicare il modello delle intercettazioni (telematiche o ambientali) l'organo dell'accusa emetterebbe, su autorizzazione del giudice per le indagini preliminari, un decreto corretto formalmente, ma nella sostanza inidoneo a individuare le modalità esecutive, peraltro necessarie, ai sensi dell'art. 271, comma 1, c.p.p., ai fini di utilizzabilità delle intercettazioni 41: né appare possibile selezionare anticipatamente i dati di interesse in modo da limitare l'indagine allo stretto necessario. Il giudice, da parte sua, non è sempre in grado di comprendere la portata euristica dell'indagine che deve autorizzare e dunque non può effettuare un efficace controllo preventivo. Infine, vi è con un'ulteriore questione relativa alle diverse tipologie di programmi spia: si consideri che questi sono prodotti da aziende specializzate rispetto alle quali sarebbe opportuna una verifica di professionalità: peraltro, si tratta di agenzie di intelligence, magari operanti all'estero, e non si può escludere il rischio di condivisione o diffusione delle informazioni captate».

all'interno del sistema informatico, non potrebbe includere le attività di cui si discorre in quanto le stesse non sono caratterizzate dalla contestualità della captazione alla formazione del dato che, ad ogni modo, rappresenta un requisito strutturale dell'intercettazione telematica anche secondo l'indirizzo ermeneutico meno rigorista prima analizzato in materia.

Appare, dunque, scontata la conclusione per la quale si è, a tutto voler concedere, dinanzi a una prova di carattere innominato. Su tale conclusione non pare compattamente orientata, tuttavia, la giurisprudenza che si è finora pronunciata sul tema. Invero, tutt'altro che cospicua.

2.1. Prime applicazioni giurisprudenziali.

La prima pronuncia di legittimità che si è soffermata sul tema che occupa risale al 2009[242] ed ha ad oggetto un decreto di acquisizione degli atti disposto dal pubblico ministero ai sensi dell'art. 234 c.p.p., finalizzato all'estrapolazione, tramite installazione di un *trojan virus*, di una copia della documentazione informatica memorizzata all'interno di un *personal computer* installato presso l'ufficio nel quale esercitava la sua attività lavorativa la persona sottoposta alle indagini. Il decreto, così come le attività investigative realizzate in conseguenza della sua adozione, avevano ad oggetto sia dati già formati e contenuti della memoria del *computer*, sia dati che fossero venuti ad esistenza solo in futuro. In ragione della delimitazione effettuata in apertura del presente capitolo, ci si soffermerà esclusivamente sulle conclusioni raggiunte dalla Corte con specifico riguardo alla prima categoria di dati acquisiti, esulando, per ora, dall'analisi che si intende condurre ulteriori considerazioni relative all'attività di acquisizione progressiva dei dati che, configurando quella che è stata definita alla stregua di una *online surveillance*, sarà analizzata nel prossimo capitolo.

Nel ricorso presentato dalla difesa veniva, anzitutto, evidenziato come l'attività concretamente svolta sarebbe consistita in una vera e propria intercettazione di comunicazioni telematiche che, in quanto tale, avrebbe dovuto essere sottoposta alla procedura prevista dall'art. 266 *bis* c.p.p. Secondo il ricorrente, infatti, le intercettazioni informatiche e telematiche sarebbero dirette a captare un flusso di comunicazioni relativo a sistemi oppure intercorrenti tra più sistemi informatici o telematici, non

[242] Sez. V, 14 ottobre 2009, n. 16556, Virruso, in *CED Cass.*, n. 246954.

avendo rilievo alcuno il numero degli utenti interagenti con il sistema intercettato. In buona sostanza, nel ricorso veniva offerta una lettura ampia del concetto di intercettazione telematica, sulla scorta del filone giurisprudenziale sopra richiamato[243], suscettibile di ricomprendere anche dati non aventi natura di comunicazione tra due o più soggetti. Per l'effetto, l'atto di impugnazione lamentava la violazione degli artt. 14 e 15 Cost., la prima norma invocata sul presupposto che l'ufficio nel quale era ubicato il dispositivo informatico, in quanto luogo preposto in modo stabile e continuativo all'esercizio dell'attività lavorativa da parte del ricorrente, assurgesse al rango di domicilio.

Nell'escludere qualsivoglia profilo di illegittimità dell'attività compiuta – e, conseguentemente, di inutilizzabilità dei suoi risultati conoscitivi – la Corte ha evidenziato, anzitutto, che «nella specie, l'attività autorizzata dal pubblico ministero, consistente nel "prelevare e copiare documenti memorizzati sull'"hard disk" dell'apparecchio in uso al BA., aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico", ossia "un flusso unidirezionale di dati" confinato all'interno dei circuiti del personal computer».

Conseguentemente, i giudici di legittimità hanno escluso l'operatività dell'art. 266 *bis* c.p.p., concludendo nel senso della correttezza dell'inquadramento sistematico realizzato dai giudici di merito i quali, investiti della medesima questione dal ricorrente, avevano evidenziato come l'attività concretamente condotta dagli inquirenti fosse riconducibile alla categoria della prova atipica, in quanto tale sottratta alla disciplina, invocata dal ricorrente, di cui agli artt. 266 ss. c.p.p.

Infine, la Corte ha evidenziato l'assenza di qualsivoglia violazione degli artt. 14 e 15 Cost. Quanto al primo, si legge nella pronuncia che «invero, l'apparecchio monitorato con l'installazione del captatore informatico non era collocato in un luogo domiciliare ovvero in un luogo di privata dimora, ancorché intesa nella sua più ampia accezione, bensì in un luogo aperto al pubblico»; quanto, invece, alla pretesa violazione della libertà e segretezza delle comunicazioni, secondo i giudici «quanto riprodotto in copia non era un testo inoltrato e trasmesso col sistema informatico, ma soltanto predisposto

[243] Cfr. par. 1.2.

per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario».

Un altro precedente[244] che occorre segnalare risale a ben otto anni dopo quello appena riportato. Anche in questo caso la vicenda aveva ad oggetto l'impiego di un *trojan virus* a fini di monitoraggio di un *personal computer*, ma, a differenza di quanto era avvenuto nell'indagine relativa alla sentenza di cui sopra, l'attività in questione era stata disposta sulla base della disciplina prevista in materia di intercettazioni. Disciplina che, a parere del ricorrente, sarebbe stata inadeguata: oggetto dell'attività, infatti, non sarebbe stata l'intercettazione di flussi telematici ai sensi dell'art. 266 *bis* c.p.p. ma, piuttosto, la captazione in tempo reale di un flusso di dati intercorso sul supporto informatico. Tanto con la conseguenza che si sarebbe integrata non già un'attività di intercettazione, ma di perquisizione e sequestro.

L'aspetto di maggiore interesse della pronuncia in commento in tema di acquisizione di dati già contenuti nel *personal computer* attiene alla qualificazione giuridica dell'attività in questione, pur essendo, invero, la stessa effettuata solo *incidenter tantum*. La Corte, infatti, pur reputando irrilevante pronunciarsi in merito alla questione se l'acquisizione di dati già presenti nel sistema informatico costituisca un'intercettazione, una prova atipica o, ancora, un'attività di perquisizione con conseguente sequestro[245], pare, in un distinto passaggio della decisione, adombrare la correttezza della prima soluzione, laddove, citando il provvedimento impugnato, afferma che l'«acquisizione di "dati contenuti nel computer, ovvero di flussi informatici transitati sui dispositivi" rientra nel concetto di intercettazione»[246].

Al netto di quanto si dirà nel prossimo paragrafo in merito alla criticabilità delle soluzioni accolte nelle due pronunce, può fin da ora evidenziarsi come la netta divergenza delle conclusioni raggiunte all'interno delle stesse tradisca un certo livello di spaesamento sul tema e la difficoltà di fornire un inquadramento complessivo e

[244] Sez. V, 30 maggio 2017, n. 48370, Occhionero, in *CED Cass.*, n. 271412.

[245] Per completezza, si segnala che l'irrilevanza della questione, a parere della Corte, era da ricondursi al carattere aspecifico dei motivi di ricorso presentanti, in quanto sarebbe spettato «al ricorrente precisare, in ossequio al principio di specificità delle impugnazioni, quali dei dati captati tramite trojan fossero eventualmente colpiti dalla sanzione dell'inutilizzabilità e, vieppiù, chiarirne l'incidenza sul complessivo compendio indiziario già valutato, sì da potersene inferire la decisività in riferimento al provvedimento impugnato».

[246] Evidenzia TORRE, *Il captatore informatico tra riforma Orlando e sistema processuale,* in *Giur. ita.*, 2018, 7, 1781, come la pronuncia contenga un'interpretazione estensiva del concetto di intercettazione idonea a ricomprendere anche la captazione telematica dei dati statici.

coerente delle attività in questione. Difficoltà che pare potersi mettere in diretta relazione, anzitutto, con l'assenza di una preliminare riflessione in merito all'opportunità di operare i necessari distinguo tra le singole tipologie di attività esperibili per il tramite dell'inoculazione di un *virus trojan*. In nessuna delle due sentenze, infatti, viene neppure ipotizzata l'esistenza di una qualche differenza tra un'attività diretta alla sola acquisizione di dati già memorizzati nel dispositivo bersaglio e una finalizzata a operare un monitoraggio costante del medesimo. Non senza una certa dose di assertività, le due decisioni si limitano a ipotizzare la riconducibilità dell'intera gamma di attività esperibili tramite il captatore a una piuttosto che a un'altra categoria probatoria. Ma le conclusioni raggiunte, oltre che non sostenute da un adeguato apparato argomentativo, sembrano criticabili sotto un profilo, anzitutto, dogmatico.

2.2. Le criticità della ricostruzione operata nelle pronunce di legittimità in materia.

Vi è una differenza ontologica tra le attività di ricerca e apprensione aventi ad oggetto i dati già memorizzati nel dispositivo informatico e quelle dirette all'acquisizione di dati suscettibili di confluirvi in un momento successivo all'inizio delle operazioni. Tale differenza si riflette, come si vedrà, anche sull'intensità della compressione dei diritti fondamentali connessa alla esecuzione della misura[247]. Trattasi di una distinzione, peraltro, ben consolidata anche nella sistematica del codice di rito, come attestato dalla differente articolazione della disciplina prevista in relazione ad alcuni mezzi di prova e di ricerca della prova per i quali viene delineato un diverso statuto di garanzie a seconda che l'oggetto dell'attività istruttoria sia preesistente o meno all'avvio della medesima. È quanto accade, significativamente, in relazione all'acquisizione di elementi probatori aventi ad oggetto la corrispondenza o le comunicazioni tra due o più soggetti. Si coglie perfettamente, nella gradazione di guarentigie messe a punto, per un verso, dall'art. 254 c.p.p. e dagli artt. 266 ss. c.p.p., la percezione, sul piano legislativo, della diversa intensità dell'aggressione al bene giuridico della libertà e segretezza della corrispondenza e delle altre forme di comunicazione nei due casi. Non v'è dubbio che la ragione del differente grado di rigore delle tutele connesse all'esecuzione delle

[247] Il tema sarà approfondito nel par. 3.

misure in questione sia da ricondursi proprio al fatto che mentre in un caso l'acquisizione riguarda elementi già formati al momento dell'inizio dell'attività investigativa, nel secondo caso non solo si ha di mira dati comunicativi non ancora formati, ma per di più il soggetto viene sottoposto a un'attività di controllo occulto suscettibile di protrarsi nel tempo. Trattasi di un'attività più subdola, in grado di incidere in maniera più significativa sulle aspettative di riservatezza del singolo.

Si è, dunque, dinanzi a due tipologie di attività le cui differenze sul piano delle modalità esecutive si riflettono sulla compressione dei diritti connessi all'esecuzione delle medesime: ciò, seguendo lo schema teorico illustrato *supra*[248], dovrebbe comportare la necessaria differenziazione della loro qualificazione giuridica, con la conseguente messa a punto di uno statuto di tutela adeguato alle caratteristiche specifiche delle stesse. Proprio il ragionamento condotto dalle due sentenze in relazione alla stessa qualificazione giuridica delle attività oggetto di analisi, invece, risulta del tutto insoddisfacente.

Con riferimento alla prima delle due pronunce analizzate, la sentenza *Virruso* del 2009, appare anzitutto criticabile la mancanza di una presa di posizione netta in merito alla qualificazione giuridica dell'attività operata, nel caso di specie, dal pubblico ministero, che l'aveva ricondotta a una mera acquisizione di documenti ai sensi dell'art. 234 c.p.p. Qualificazione che, se è certamente inadeguata in relazione ai dati formati sul dispositivo successivamente all'inizio delle attività[249], pare nondimeno poco appropriata anche in relazione all'acquisizione di dati preesistenti all'accertamento, essendo di tutta evidenza come lo strumento istruttorio in questione non sia minimamente assimilabile – né sul piano del risultato investigativo concretamente conseguibile né, tanto meno, sul piano delle prerogative individuali oggetto di compressione – a una mera acquisizione documentale.

Sotto altro profilo, pare criticabile l'argomento con il quale la Corte ha escluso la riconducibilità dell'attività svolta nel caso di specie alla categoria dell'intercettazione telematica. La conclusione, invero, appare di per sé corretta, soprattutto alla luce di quanto si vedrà nel prossimo capitolo in tema di necessaria distinzione tra le attività di

[248] Cfr. cap. 2, par.2.

[249] Quanto meno se si tiene ferma la tradizionale distinzione tra atto e documento, ben nota alla sistematica processualpenalistica, basata sul fatto che solo il primo è formato all'interno del procedimento penale.

vigilanza *online* realizzabili tramite il captatore informatico e l'intercettazione telematica. Nel caso in questione, tuttavia, a escludere la riconducibilità dell'attività investigativa realizzata a tale categoria giuridica è, anzitutto, la mancanza di contestualità tra l'acquisizione e la formazione del dato. In altre parole, non si era trattato di un'attività di acquisizione in tempo reale di dati informatici che, secondo una parte della giurisprudenza, pur criticabile come si vedrà, rientrerebbe nell'istituto di cui all'art. 266 *bis* c.p.p.

Il punto di maggiore criticità della pronuncia, tuttavia, è da ravvisarsi nel fatto che alla qualificazione della prova in questione alla stregua di una prova atipica – che, come visto e con le precisazioni che verranno operate tra un momento, appare corretta – non è seguita una adeguata analisi in merito ai diritti incisi dalla misura e, dunque, all'utilizzabilità dei suoi risultati.

La stessa configurazione di una prova atipica trova un «limite esterno invalicabile, consistente nel rispetto dei principi desumibili dalla Costituzione»[250]. La decisione in commento, invece, "liquida" la questione dei diritti fondamentali incisi da tale misura con poche righe nelle quali esclude tanto un impatto sulla prerogativa di cui all'art. 15 Cost., quanto un'incidenza sull'inviolabilità domiciliare di cui all'art. 14 Cost.

Se può, astrattamente, convenirsi sull'esclusione di una restrizione della libertà e segretezza delle comunicazioni – non essendo nel caso di specie stati captati dati comunicativi in tempo reale – lascia perplessi l'esclusione della garanzia di cui all'art. 14 Cost., essendo evidente come essa sia da collegare alla mancanza di qualsivoglia riflessione in merito a quella lettura evolutiva dell'inviolabilità del domicilio, ormai consolidata nella giurisprudenza e nella dottrina nazionale, tesa a ricomprendere anche il domicilio informatico. In questo senso, la riconduzione delle attività in questione al concetto di prova atipica rischia di convertirsi in un'elusione delle garanzie previste dalla legge e dalla stessa Costituzione per la compressione di certe prerogative individuali[251].

Quanto, poi, alla seconda pronuncia analizzata – la sentenza *Occhionero* – la riconduzione dell'attività in questione all'intercettazione telematica appare del tutto

[250] Così, testualmente, MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, cit., 213.

[251] FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., 132.

fuori fuoco stante quanto si è appena detto sulla mancanza di contestualità della captazione realizzata nel caso di specie.

Semmai, la pronuncia offre qualche spunto di riflessione sulla tendenza a ricondurre all'alveo dell'attività intercettiva l'intera gamma di operazioni effettuabili tramite lo strumento tecnologico in questione che appare, oltre che un marchiano errore prospettico, il precipitato di un fenomeno che è stato criticamente segnalato da una parte della dottrina. Il riferimento è alla progressiva erosione del principio di legalità della prova, alla cui accelerazione sta senz'altro contribuendo il diffondersi di nuove tecnologie che consentono mezzi sempre nuovi di aggressione ai diritti fondamentali e sospingono l'interprete verso «nuove teorizzazioni di una flessibilità della prova giustificata dal superiore fine cognitivo»[252]. È evidente, infatti, la tendenza a forzare le categorie giuridiche esistenti al fine di ricondurvi i nuovi e sempre più intrusivi mezzi di prova e di ricerca della prova consentiti dal progresso scientifico. Fenomeno, quest'ultimo, da mettere in diretta relazione con l'obsolescenza delle categorie giuridiche note al codice di rito. Tra queste, appare scontato il riferimento proprio alle intercettazioni: è stato convincentemente segnalato, in dottrina, come la nozione di "intercettazioni" sia «soggetta a un'inesorabile obsolescenza» e come «in mancanza di un'esaustiva disciplina, infatti, un incessante raffronto in via interpretativa tende a ricondurre, quando possibile, ogni specifica operazione captativa entro le aree applicative di istituti già noti al sistema»[253]. Una plastica dimostrazione di ciò, peraltro, è rappresentata proprio dalla conclusione raggiunta nella sentenza *Occhionero*.

Quanto appena segnalato, peraltro, appare ancor più preoccupante se solo si considera che la giurisprudenza pressoché pacifica esclude che le operazioni di estrazione dei dati possano essere considerate alla stregua di accertamenti tecnici irripetibili[254]; tanto anche, evidentemente, al fine di non vanificarne l'efficacia, atteso che l'opposta conclusione comporterebbe l'operatività delle garanzie previste dall'art. 360 c.p.p. e, dunque, il venir meno del carattere occulto dell'atto.

---

[252] Così, TAVASSI, *Le intercettazioni ubiquitarie fra legalità e non dispersione della prova,* in *Arch. pen.*, 2018, 2, 2, la quale ripercorre, con molteplici esempi, quelli che definisce «casi di erosione giurisprudenziale dei limiti imposti all'ordine probatorio».

[253] PARLATO, *Problemi insoluti: le perquisizioni on-line,* cit., 292.

[254] Si vedano, ad esempio, Sez. II, 4 giugno 2015, Sanu e altri, in *CED Cass.*, n. 264286; Sez. II, 19 febbraio 2015, Apicella e altri, in *CED Cass.*, n. 263797; Sez. V, 14 ottobre 2009, n. 16556, Virruso, cit.; Sez. I, 30 aprile 2009, Corvino, in *CED Cass.*, n. 244454. Sul punto, per una ricostruzione degli orientamenti in materia, si veda BUZZELLI, *Perquisizione di spazi virtuali e preview*, in AA.VV. *Dimensione tecnologica e prova penale*, Giappichelli, 2019, 119 ss.

Il combinato disposto delle opzioni interpretative appena riassunte è, dunque, non solo insoddisfacente ma finanche paradossale: di fatto, si è dinanzi a un'attività di ricerca della prova suscettibile di pregiudicare diritti fondamentali degli individui in modo estremamente più intenso di quanto non accada con il ricorso ai consueti mezzi di ricerca della prova e in relazione al quale, mancando una precisa disciplina normativa, le opzioni ermeneutiche operate dalla giurisprudenza si attestano su livelli di tutela nettamente inferiori a quelli che la legge prevede in relazione a istituti impattanti in minor misura sulle prerogative individuali.

3. Il piano costituzionale.

La conclusione per la quale lo strumento investigativo del quale si discute non è assimilabile alle categorie giuridiche già regolate dalla legge impone di qualificarlo alla stregua di un atto innominato. Conseguentemente, diviene cruciale interrogarsi su quale sia l'impatto della *online search* e *seizure* su diritti fondamentali costituzionalmente presidiati.

Tanto, anzitutto, al fine di verificare l'esistenza di una riserva di giurisdizione e, soprattutto, di una riserva di legge che impedirebbe l'uso probatorio del risultato conoscitivo acquisito in conseguenza dell'attività svolta, secondo gli approdi ermeneutici raggiunti dalla giurisprudenza in tema di prova non prevista dalla legge incidente sui diritti costituzionali. Come si è visto, infatti, laddove l'atto probatorio incida su diritti fondamentali tutelati da riserva di legge, la mancanza di una disciplina normativa esprime la scelta legislativa di non consentire lo svolgimento dell'atto. Né, come è stato efficacemente osservato[255], una simile mancanza può essere colmata invocando l'applicazione di una disciplina prevista per casi analoghi, quand'anche si tratti di una normativa ispirata a elevati livelli di garanzia, come, ad esempio, quella prevista in materia di intercettazioni. Tale conclusione, infatti, si risolverebbe in una vera e propria analogia *in malam partem*, in quanto avrebbe l'effetto di rendere ammissibile un esperimento probatorio che dovrebbe reputarsi vietato in virtù di una precisa scelta legislativa.

Anche in una prospettiva *de iure condendo* l'individuazione della base costituzionale appare, come si è già accennato, necessaria al fine di mettere a fuoco le componenti

[255] MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont., Riv. Trim.*, 2013, 3, 8.

essenziali dello statuto di garanzie che deve presidiare lo svolgimento di attività investigative del tipo di quelle analizzate. Il rango del diritto fondamentale compresso per effetto dell'atto investigativo e l'intensità della sua restrizione rappresentano, infatti, per il legislatore che si appresti a regolare la materia, delle bussole imprescindibili per mettere a punto un reticolo di limiti e prerogative connessi allo svolgimento dell'atto il cui rigore sia proporzionato alla "statura" del diritto costituzionale compresso.

Con ciò, evidentemente, non si intende prendere posizione in merito alla complessa questione se sia o meno identificabile, nella Costituzione italiana, una gerarchia di valori. È stato convincentemente e diffusamente sostenuto, nella dottrina costituzionalistica, che un simile assetto non è rinvenibile nel nostro sistema costituzionale, che rappresenta il frutto del compromesso tra le diverse componenti politiche e ideologiche che, in seno alla Costituente, condussero all'adozione un testo costituzionale espressione del pluralismo[256]. Sicché, a ben vedere, neppure l'individuazione di un nucleo essenziale dei diritti di volta in volta considerati sarebbe tale da escludere che gli stessi confliggano e da scongiurare la necessità di un bilanciamento. Tanto in netta contrapposizione con quanto avviene, invece, in altri ordinamenti e, segnatamente, nell'ordinamento tedesco, in cui è ravvisabile la presenza di una più rigida gerarchia assiologica tra i diritti costituzionali[257].

Nondimeno, è evidente come, su un piano anzitutto sistematico, elementari esigenze di complessiva ragionevolezza del sistema impongano al legislatore ordinario di adeguare lo statuto di garanzie delineato per nuovi mezzi di prova o di ricerca della prova ai livelli di rigore propri di istituti già normati e incidenti, con intensità assimilabile, sulle medesime prerogative costituzionali.

D'altronde, la disciplina codicistica prevista in materia di restrizione dei diritti e delle libertà fondamentali non è indifferente al rango del diritto di volta in volta compresso né, tanto meno, al grado della sua compressione. Basta guardare – per fare un esempio che, come si vedrà in seguito, appare particolarmente calzante nel caso di specie – all'assetto normativo che il legislatore ha conferito alle restrizioni in tema di inviolabilità del domicilio e della libertà personale. Trattasi di due libertà in relazione alle quali la Costituzione prevede garanzie parificabili, consistenti, in entrambi i casi, in

[256] PINO, *Conflitto e bilanciamento tra diritti fondamentali. Una mappa dei problemi*, in *Etica & Politica*, 2006, 1, 15.

[257] BALDASSARRE, *Diritti inviolabili*, in *Enc. giur*., XI, 1989, 14.

una riserva di legge e di giurisdizione. Eppure, la disciplina codicistica attua le due riserve in maniera sensibilmente divergente non solo con riferimento agli istituti che incidono sull'uno o sull'altro diritto fondamentale[258], ma altresì con riguardo a quelli che impattano con differente intensità sulla medesima prerogativa[259]. In buona sostanza, l'assetto normativo delineato nei due casi è il frutto di precise scelte legislative operate in materia di composizione del conflitto esistente tra i contrapposti interessi sottesi all'applicazione degli istituti in questione. Scelte che, a loro volta, non possono che essere espressione dalla percezione della differente intrusività degli istituti incidenti sulle due prerogative in questione, pur essendo alle stesse accordata una tutela costituzionale assimilabile (addirittura, l'art. 14 Cost. delinea lo statuto di tutele connesso alle restrizioni applicabili al domicilio facendo espresso rinvio all'art. 13 Cost.).

Un intervento normativo finalizzato a regolare nuovi istituti processuali incidenti su diritti costituzionali non può non tenere presente i livelli di tutela già previsti, sul piano della normazione primaria, per casi e restrizioni assimilabili.

3.1. I diritti incisi.

Onde procedere all'individuazione dei diritti incisi dall'attività investigativa oggetto di analisi appare imprescindibile prendere le mosse proprio dalla distinzione, operata in apertura del capitolo, tra le attività di ricerca miranti all'acquisizione di dati preesistenti nel dispositivo informatico e quelle finalizzate (anche o in via esclusiva) all'acquisizione di dati non ancora esistenti sul dispositivo.

---

[258] Ad esempio, mentre la riserva di giurisdizione è declinata, nell'ambito delle perquisizioni domiciliari, nel senso della sufficienza di un provvedimento motivato del pubblico ministero (cfr. art. 247 c.p.p.), nell'ambito delle restrizioni della libertà personale comportanti forme di detenzione si prevede l'intervento necessario del giudice (cfr. ad esempio l'art. 291 c.p.p.), quanto meno nel senso della successiva convalida del provvedimento disposto dal pubblico ministero (cfr. art. 390 c.p.p.). Quanto alla riserva di legge, poi, è evidente come anche questa sia declinata in maniera nettamente diversa, essendo i casi e i modi per poter procedere all'applicazione di misure detentive provvisorie individuati in termini ben più restrittivi di quanto accasa in materia di perquisizioni, anche domiciliari (così, gli artt. 273 ss. c.p.p. individuano stringenti presupposti applicativi, anche con riferimento alla gravità dei reati per i quali si procede, ben più rigorosi di quelli previsti dall'art. 247 c.p.p).

[259] È il caso, ad esempio, della disciplina codicistica in materia di libertà personale, che declina in maniera differente le garanzie connesse allo svolgimento di determinati atti che impattano con intensità differenti su tale prerogativa. Così, riprendendo l'esempio della perquisizione (in questo caso personale) e degli istituti che comportano l'applicazione di regimi detentivi, mentre è sufficiente, per la prima, un provvedimento motivato del pubblico ministero, per i secondi si impone sempre l'intervento del giudice. Lo stesso dicasi con riferimento alla riserva di legge, declinata, anche in questo caso, in maniera ben più rigida con riferimento all'applicazione di regimi detentivi provvisori.

La distinzione, dunque, è quella che si è precedentemente delineata tra *online search* (da intendersi alla stregua di un'attività di "perquisizione e sequestro" da remoto) e *online surveillance*.

Già su un piano fenomenologico, infatti, è intuitiva la differenza tra la "mera" intrusione nel sistema informatico e la permanenza all'interno dello stesso, essendo la prima delle due attività suscettibile di avere, almeno in via tendenziale, un impatto sui diritti fondamentali quantitativamente e qualitativamente inferiore rispetto alla seconda. Ciò dipende dalle peculiari caratteristiche dello spazio – non fisico – in cui insiste, in tal caso, l'attività investigativa. Tale affermazione richiede alcune precisazioni.

Anticipando la conclusione a cui si addiverrà alla fine del paragrafo circa l'impatto dell'attività investigativa in questione sul domicilio informatico del soggetto, deve evidenziarsi come sia ben noto che, in materia di violazione del domicilio, un'analisi della normazione primaria (il riferimento è, anzitutto, all'art. 614 c.p., ma lo stesso dicasi con riguardo all'art. 615 *ter* c.p., in materia di violazione del domicilio informatico) non consente di ravvisare – almeno sul piano della percezione legislativa – un differente disvalore connesso all'intrusione o alla permanenza nel domicilio. Trattasi di due condotte apparentemente del tutto parificate, come dimostrato dalla previsione del medesimo trattamento sanzionatorio.

Un simile assetto è perfettamente ragionevole in materia di domicilio fisico, in virtù delle tendenziali caratteristiche dell'intrusione nel medesimo. La fisicità dello spazio presuppone, infatti, la fisicità dell'intrusione del medesimo, che rende l'atto, almeno in via tendenziale (ma è evidente che dalla generalizzazione del fenomeno non può prescindersi in vista di una sua regolazione), palese. Di conseguenza, già l'ingresso nel domicilio perfeziona la lesione del bene giuridico tutelato dall'art. 14 Cost., mentre una permanenza nello stesso ha, semmai, l'effetto di aggravare il pregiudizio in maniera proporzionale al tempo della restrizione. Può dirsi, cercando di semplificare, che la violazione sia, in tal caso, istantanea, pur potendo avere effetti perduranti: essa comporta l'acquisizione di informazioni su uno spazio dal quale si ha il diritto di escludere gli altri perché vi si esprime la vita privata di una persona. Ma il carattere palese della violazione comporta altresì che quella intrusione sia limitata allo stato in cui il luogo si trova al momento della stessa.

È evidente come la situazione sia alquanto differente in caso di accesso da remoto e in modo occulto a un domicilio informatico: in tal caso, l'ingresso nel domicilio con acquisizione di dati preesistenti comporta senz'altro, quanto meno, una violazione del domicilio di cui all'art. 14 Cost. (nel senso, come si vedrà tra un momento, di domicilio informatico). La permanenza nel sistema, invece, pare suscettibile di determinare anche un mutamento del bene giuridico tutelato perché consentirebbe l'acquisizione potenzialmente indiscriminata di dati futuri, atteso il carattere occulto dell'attività e dunque il tendenziale mutamento dello stato del luogo riservato dovuto all'utilizzo del dispositivo da parte del titolare. È stato, d'altronde, già efficacemente sottolineato come «in caso di controllo diretto verso entità ancora "in divenire" […] il *gap* conoscitivo tra controllante e controllato viene mano a mano colmato prima ancora che il legittimo titolare dei dati possa adottare iniziative volte a contenerne la diffusione. In altri termini, le informazioni acquisite vengono subito sottratte al dominio esclusivo del sorvegliato»[260].

Tanto, come si vedrà in seguito[261], implica che, in tema di *online surveillance*, sia senz'altro riduttivo parlare di una compressione del domicilio informatico e appaia, piuttosto, necessario riferirsi a quella nuova prerogativa costituzionale che, nelle pagine precedenti, è stata definita come diritto all'uso confidenziale o riservato delle tecnologie informatiche e ricavata da una lettura evolutiva del combinato disposto, anzitutto, degli artt. 13 e 14 Cost.

Ciò precisato, appare evidente l'errore prospettico in cui si incorre nell'escludere, come accaduto nelle pronunce analizzate nei precedenti paragrafi, l'impatto di un'attività di *online search* sulla prerogativa di cui all'art. 14 Cost. Più precisamente, il riferimento è all'accezione "informatica" che del concetto di domicilio che, giusta l'evoluzione tecnologica degli ultimi decenni, ha affiancato quella "fisica", come ormai ampiamente riconosciuto da un cospicuo filone giurisprudenziale[262]. Sicché, lo *ius excludendi alios*

---

[260] NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Un tentativo di sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Cedam, 2020, 90, il quale evidenzia altresì come la durata del controllo sia suscettibile di modificare profondamente l'ingerenza nelle prerogative del singolo in ragione del quantitativo di dati che consente di acquisire, con la conseguenza che differenze apparentemente solo quantitative possono tradursi in differenze qualitative.

[261] Cfr. cap. 4.

[262] *Ex multis*, Sez. VI, 4 ottobre 1999, n. 3065, in *CED Cass.*, n. 214942; Sez. V, 6 febbraio 2006, n. 11689, in *CED Cass.*, n. 236221; Sez. V, 26 ottobre 2012, n. 42021, in *Foro it.*, 2012, 12, 2, 709; Sez. V,

che caratterizza il domicilio fisico – indipendentemente dalla sua ubicazione e dal carattere personale o meno del suo contenuto – in ragione della sua natura di luogo deputato all'estrinsecazione della personalità del titolare è ben riferibile anche alla sua variante informatica. Da tale trasposizione emerge un concetto di domicilio (informatico) del tutto autonomo da quello tradizionale, con l'ovvia conseguenza che, diversamente da quanto sostenuto dalla giurisprudenza prima ripercorsa, è assolutamente indifferente il posizionamento del dispositivo informatico in un luogo riconducibile o meno al concetto di domicilio fisico.

Se così è, si è dinanzi a un mezzo di ricerca della prova non disciplinato dalla legge che si risolve nella violazione di diritto fondamentale qualificato come inviolabile dalla Costituzione, senza il rispetto delle garanzie previste dalla Costituzione medesima in caso di sua restrizione, vale a dire la riserva assoluta di legge, la riserva di giurisdizione e l'obbligo di motivazione.

3.2. Le conseguenze della violazione sul piano processuale.

Tenendo presente le conclusioni raggiunte precedentemente in tema di trattamento processuale delle prove non disciplinate dalla legge acquisite in violazione dei diritti fondamentali[263], appare obbligata, *de iure condito*, la conclusione per la quale l'impiego del risultato probatorio ottenuto tramite l'ingresso occulto e da remoto in un sistema informatico deve reputarsi vietato[264]. Che si adotti la prospettiva della cosiddetta prova

---

19 febbraio 2020, n. 17360, in *Dir. e giust.*, 9 giugno 2020; Sez. V, 15 febbraio 2021, n. 15899, in *Dir. e giust.*, 28 aprile 2021. Cfr. anche cap. 1, par. 3 ss.

[263] Cfr. cap. 2, parr. 3 e 3.1.

[264] In tal senso pare, d'altronde, orientata compattamente la dottrina. *Ex multis*, si vedano BRONZO, *L'impiego del* trojan horse *informatico*, cit., 352; ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. e proc. pen.*, 2018, 2, 553. *Contra*, BONTEMPELLI, *Il captatore informatico in attesa della riforma* in *Dir. pen. cont.*, 2018, 4, 12; PARLATO, *Problemi insoluti: le perquisizioni on-line*, cit., 315. Per una ricostruzione singolare ma suggestiva, si veda ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della privacy e onde eversive*, in *Arch. pen*., 2015, 3, 923, secondo la quale l'inutilizzabilità deriverebbe dalla necessaria applicazione del principio di legalità e, dunque, anzitutto, dall'art. 111, comma 1, Cost., che riserva il bilanciamento tra i contrapposti interessi coinvolti dal processo penale al legislatore, chiamato a dettare disposizioni determinate e dettagliare a tal fine, sicché «la valenza garantista sottesa al principio di stretta legalità processuale – e, segnatamente, al corollario della riserva assoluta di legge – esige la compiuta regolamentazione normativa dei casi e dei modi di aggressione delle libertà fondamentali». Conseguentemente, secondo l'Autrice, dovendo ritenersi vietata l'attività di ricerca probatoria che, non espressamente regolata, incida su un diritto inviolabile della persona, i dati probatori in tal modo acquisiti devono considerarsi inammissibili e inutilizzabili alla luce

incostituzionale o quella, fatta propria dalle Sezioni unite Prisco nel 2006, dell'inammissibilità della prova non regolata dal legislatore incidente su prerogative costituzionali coperte da risperva di legge sulla scorta della costatazione per cui si tratterebbe non di prova atipica ma vietata *tout court*, il risultato non cambia.

Tale soluzione non pare riponibile in dubbio neppure alla luce della teoria, avanzata in termini del tutto apodittici da una parte della giurisprudenza e oggetto di un tentativo di sistematizzazione di una parte della dottrina[265], delle cosiddette "garanzie minime"[266]. Il riferimento è, in particolare, alla ricostruzione secondo la quale laddove la misura istruttoria non regolata dalla legge incida su una componente "periferica" del diritto costituzionale in rilievo nel caso di specie, un decreto motivato dell'autorità giudiziaria sarebbe sufficiente per l'adozione ed esecuzione della stessa, nonostante la presenza della riserva di legge. Tanto anzitutto in quanto, come si è avuto modo di osservare *supra*, una simile ricostruzione appare del tutto assertiva e non trova alcun aggancio testuale nelle norme costituzionali. La stessa, anzi, avrebbe l'effetto di affidare alla personale sensibilità del giudice lo svolgimento di valutazioni del tutto discrezionali se non arbitrarie. Ma, altresì, in quanto, pur reputando corretta una simile ricostruzione, se non su un piano squisitamente letterale, quanto meno su un piano sistematico, è evidente come non possa parlarsi, nel caso che occupa, di una misura suscettibile di comprimere una zona periferica dell'istanza costituzionale che viene in rilievo. Al contrario, il mezzo investigativo in questione sembra connotato da un grado di

---

del combinato disposto degli artt. 191 c.p.p. e 111 Cost., nel quale ultimo si riscontra l'esistenza di una regola di esclusione probatoria.

[265] Si veda, per esempio, la ricostruzione di BACCARI e CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy*: uno sguardo d'insieme,* in *Dir. pen. proc*., 2021, 6, 721, le quali ricostruiscono il seguente schema: «qualora l'attività comporti un sacrificio totale del nucleo duro dell'istanza, si è di fronte ad atti "non disciplinabili" dalla legge neppure in prospettiva futuribile giacché sarebbe impossibile – per così dire "ontologicamente" – rispettare il principio di proporzionalità. In definitiva, per ogni istanza costituzionale è possibile individuare in assoluto un contenuto minimo non comprimibile neppure a tutela di altri interessi di pari rilevanza costituzionale […] possono configurarsi prove atipiche che, pur riconducibili alla sfera di diritti fondamentali, non ne interessano il nucleo centrale, né la fascia intermedia bilanciabile alla luce dei parametri rigorosi indicati sub a), bensì si limitano ad intaccare una sorta di "zona periferica". Tale operazione esegetica è stata effettuata dalla giurisprudenza di legittimità con riguardo all'agente segreto attrezzato per il suono con ascolto non contestuale da parte della polizia giudiziaria. Ebbene, in tali ipotesi proprio la natura emergente o periferica del diritto inciso è la chiave per ritenere che, in base ai principi di adeguatezza e di proporzionalità, non sia necessario il rispetto della riserva di legge e di giurisdizione, ma sia sufficiente un modello di tutela più tenue, costituito da un provvedimento del pubblico ministero munito di un congruo apparato giustificativo: si è, dunque, dinanzi a prove atipiche che potremmo definire "rafforzate" e, di converso, ad un bilanciamento "attenuato"».

[266] Per una ricostruzione più precisa, si veda il cap. 2, par. 5.

intrusività nettamente superiore al suo corrispndente nel mondo fisico. Tanto in quanto, alla luce della quantità e qualità di dati che siamo soliti affidare loro, i nostri "domicili informatici" sono luoghi contrassegnati da un'aspettativa di riservatezza maggiore di quella che caratterizza un domicilio fisico.

È, inoltre, il caso di precisare che su tale soluzione – quella dell'impossibilità di un impiego probatorio dei materiali ottenuti tramite il ricorso a un simile mezzo di prova, almeno fintantoché il legislatore non interverrà a regolare la materia – non incide minimamente la questione – assai dibattuta e ancora ben lungi dal trovare un approdo esegetico definitivo – relativa alla cosiddetta inutilizzabilità derivata. Ci si riferisce, come noto, alla *querelle* relativa all'estensione del vizio dell'inutilizzabilità di cui all'art. 191 c.p.p. all'acquisizione probatoria realizzata in forza di una perquisizione o ispezione domiciliare o personale condotta al di fuori dei casi tassativamente previsti dalla legge. Sul punto si è, da ultimo, nuovamente pronunciata la Corte costituzionale, escludendo l'illegittimità costituzionale dell'art. 191 c.p.p. «nella parte in cui – secondo l'interpretazione predominante nella giurisprudenza di legittimità, qualificabile come diritto vivente – non prevede che la sanzione di inutilizzabilità delle prove acquisite in violazione di un divieto di legge riguardi anche gli esiti probatori – compreso il sequestro del corpo del reato e delle cose pertinenti al reato – degli atti di perquisizione e ispezione domiciliare e personale fuori dei casi tassativamente previsti dalla legge, ovvero non convalidati, comunque sia, dal pubblico ministero con provvedimento motivato»[267].

[267] Il riferimento è alla pronuncia Corte Cost. 3 ottobre 2019 n. 219, commentata da GALANTINI, *Alla ricerca della "inutilizzabilità derivata"*, in *Sist. pen.*, 2021, 3, 151 ss., MORSELLI, *L'idolo del sequestro come 'atto dovuto' che impedisce la declaratoria di illegittimità in caso di perquisizione illegittima,* in *Proc. pen. giust*., 2020, 10, 111 e PICARO, *Perquisizione illegittima e limiti della inutilizzabilità,* in *Arch. pen.* 2020, 1. Si veda anche Corte cost. 26 novembre 2020 n. 252, che ha dichiarato la manifesta inammissibilità di una nuova questione di legittimità costituzionale dell'art. 191 c.p.p. La letteratura sul punto è vastissima. Volendo citare i contributi essenziali, si vedano CORDERO, *Prove illecite nel processo penale*, in *Jus*, 1961, 68 ss.; Id., *Il procedimento probatorio,* in *Tre studi sulle prove penali*, Giuffrè, 1963, 122 ss.; DINACCI, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, Giuffrè, 2008, 91; FERRUA, *Prove illegittimamente acquisite: passato ed avvenire di un'illustre teoria*, in *Dir. pen. e proc*., 2020, 9, 1256; PIERRO, *Una nuova specie di invalidità: l'inutilizzabilità degli atti processuali penali*, Edizioni Scientifiche italiane, 1992,170; PANZAVOLTA, *Contributo allo studio della invalidità derivata*, Aras Edizioni, 2012, 263; SCELLA, *Prove penali e inutilizzabilità. Uno studio introduttivo*, Giappichelli, 2000, 134; TONINI e CONTI, *Il diritto delle prove penali*, Giuffrè, 2014, 15. Nella giurisprudenza di legittimità, *ex multis*, Sez. VI, 30 aprile 2019, n. 4119, in *CED. Cass.*, n. 27819; Sez. V, 10 ottobre 2019, n. 44114, in *CED. Cass.*, n. 277432; Sez. V, 29 ottobre 2019, n. 44114, in *CED. Cass.*, n. 277432; Sez. VI, 28 luglio 2020, n. 22790.

Al netto della elevatissima complessità della questione e delle varie soluzioni esegetiche percorribili, essa non pare giocare alcun ruolo nel caso di specie. Ciò per la banale ragione che l'eventuale acquisizione di dati informatici da remoto in conseguenza di un accesso al sistema informatico bersaglio si atteggia essa stessa alla stregua di un'attività vietata in quanto non riconducibile ad alcuna categoria probatoria attualmente regolata e suscettibile di inicidere su diritti fondamentali coperti da riserva di legge. Si tratta, quindi, di un fenomeno che nulla ha a che vedere con la trasmissione dell'invalidità da un atto illegittimo a uno che si ponga quale suo conseguente e che, dunque, non postula né il rinvenimento, a monte, di un "antecedente processuale" viziato, né l'esistenza di una regola probatoria che stabilisca, similmente a quanto accade in materia di nullità, la propagazione del vizio.

Ciò detto, appare nondimeno evidente come la soluzione sostenuta in questa sede circa l'inutilizzabilità del risultato probatorio acquisito in forza di una violazione, non regolata dalla legge, del domicilio informatico sia, comunque, insoddisfacente. Tanto in quanto l'inutilizzabilità dei dati acquisiti non è suscettibile di elidere la violazione delle prerogative costituzionali proprie dell'utilizzatore del sistema informatico ormai irrimediabilmente perpetrata. L'utilizzo procedimentale di quel materiale comporta, semmai, l'aggravamento del pregiudizio già perfezionatosi al momento dell'intrusione nel sistema o, al più, l'insorgenza di una nuova violazione che, tuttavia, si pone su un piano diverso e ulteriore[268]. E, si badi, si tratta di un rischio non virtuale se solo si considera che, ad oggi, l'impiego del captatore informatico è consentito dal codice di rito con riferimento allo svolgimento delle intercettazioni ambientali: vi è, pertanto, un concreto pericolo che, in forza dell'autorizzazione a realizzare tale genere di captazioni, vengano poi acquisiti dati ulteriori rispetto a quelli per i quali la legge ammette l'ingresso nel sistema informatico.

Tale situazione rende non rinviabile un intervento legislativo sul punto, in relazione al quale si tenterà, nel prossimo paragrafo, di tracciare alcune possibili coordinate.

4. La perquisizione e il sequestro *online* come categoria probatoria: una proposta *de iure condendo.*

[268] Sul punto, per tutti, si vedano le considerazioni di CAPRIOLI, *Intercettazioni e tutela della privacy nella cornice costituzionale*, in *Cass. pen.*, 2021, 4, 1144 ss.

Immaginare le coordinate di un intervento legislativo volto a regolare l'acquisizione da remoto e occultamente di dati contenuti nei dispositivi informatici di uso comune non è un'operazione semplice per almeno due ragioni: da un lato, si è dinanzi a uno strumento investigativo suscettibile di esacerbare la tensione normalmente connaturata all'incedere dell'accertamento penale tra diritti individuali e interesse statuale alla repressione delle forme di criminalità. Nella ricerca di un ragionevole bilanciamento tra le due esigenze contrapposte sta l'aspetto, al tempo stesso, più complesso e delicato della materia.

Altro fattore di complessità – peraltro affatto slegato da quello appena evidenziato – è da rinvenirsi nella impossibilità di scindere gli aspetti squisitamente giuridici della questione da quelli tecnici, essendo di tutta evidenza come questi ultimi siano suscettibili di incidere sensibilmente sul grado di compressione dei diritti fondamentali dei singoli coinvolti nello svolgimento dell'atto. Sicché, la predisposizione di una disciplina specificamente volta a regolare la categoria probatoria in oggetto non può prescindere dalle caratteristiche tecniche e operazionali dello strumento tecnologico impiegato.

Ciò premesso, la presente analisi non ha affatto la pretesa di delineare una disciplina puntuale ed esaustiva dell'istituto in questione, quanto piuttosto di individuarne le coordinate essenziali, tenendo conto dei due fattori di complessità appena evidenziati, sui quali pare opportuno spendere qualche considerazione preliminare.

4.1. Alcune preliminari coordinate: il principio di proporzionalità.

Un atto investigativo ontologicamente proiettato a incidere su ambiti nei quali si esprime la personalità di un individuo esige il rispetto delle prerogative costituzionali coinvolte e ciò non può non conformare, corrispondentemente, grado e natura delle garanzie individuali connesse allo svolgimento dell'atto.

Si è già evidenziato come, a parere di chi scrive, la misura in questione sia suscettibile di comprimere, quanto meno, l'inviolabilità del domicilio informatico, ricavato dalla lettura evolutiva dell'art. 14 Cost. L'enorme mole di dati, anche personali o sensibili, acquisibili tramite l'intrusione nel domicilio nel caso di specie, nondimeno, pare suscettibile di giustificare un livello di garanzie connesse allo svolgimento dell'atto ben più elevato di una violazione domiciliare "tradizionale" (si pensi, ad esempio, a una

perquisizione domiciliare). Ciò non solo in quanto, come si è già visto[269], elementari esigenze di sistematicità e ragionevolezza impongono di graduare le garanzie connesse all'attuazione di misure restrittive dei diritti fondamentali non solo in base alla natura del diritto fondamentale in questione ma anche in base al grado dell'intrusione nel medesimo laddove si sia dinanzi a istituti differenti che, pur incidendo su un medesimo bene giuridico, lo facciano con diverse intensità; la medesima conclusione, infatti, si impone anche per il necessario rispetto del principio di proporzionalità[270], del quale non può non tenersi conto alla luce del crescente rilievo che lo stesso sta progressivamente acquisendo non solo sul piano internazionale, ma anche su quello interno, proprio con specifico riferimento alla compressione delle garanzie individuali nelle indagini ad alto contenuto tecnologico.

L'applicazione del principio di proporzionalità[271], come noto, comporta l'adozione di un metodo argomentativo teso a verificare la correttezza dell'assetto raggiunto all'esito della composizione di un conflitto tra valori o interessi contrapposti. Tale metodo si sviluppa, notoriamente, in tre fasi. La prima fase è indirizzata alla verifica dell'idoneità dei mezzi adoperati per il raggiungimento del fine che si intende realizzare; la seconda fase, invece, è finalizzata a verificare la necessità della misura, vale a dire che il mezzo

---

[269] Cfr. par. 3.

[270] Si tratta della prospettiva fatta propria dalla dottrina più recente che, cimentandosi nel complesso tentativo di sistematizzazione della materia dei controlli occulti e realizzati in maniera continuativa, ha rinvenuto nel principio di proporzionalità la bussola per un adeguato tracciamento delle coordinate di un possibile intervento normativo in materia. Cfr. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 106 ss.

[271] Sul tema della proporzionalità in generale, nella pur sconfinata letteratura, si vedano BAILO, *Prosegue la "costituzionalizzazione" del principio di proporzionalità delle pene nella giurisprudenza della Consulta*, in *Giur. it.*, 2013, 1, 31; COGNETTI, *Principio di proporzionalità. Profili di teoria generale e di analisi sistematica*, Giappichelli, 2010; GRIMALDI, *Il principio di proporzionalità della pena nel disegno della Corte Costituzionale*, in *Giur. pen. web*, 2020, 5; MERLO, *Considerazioni sul principio di proporzionalità nella giurisprudenza costituzionale in materia penale*, in *Riv. it. dir. e proc. pen*., 2016, 3, 1427; MORRONE, voce *Bilanciamento* (giustizia costituzionale), in *Enc. dir., Annali*, vol. II, tomo II, Giuffrè, 2008; SANDULLI, *La proporzionalità dell'azione amministrativa*, Cedam, 1998; SCACCIA, *Il bilanciamento degli interessi come tecnica di controllo costituzionale*, in *Giur. it*., 1998, 6, 3953; Id., *Proporzionalità e bilanciamento dei diritti nella giurisprudenza delle Corti europee*, in *Rivista AIC*, 2017, 3. Con riferimento alle implicazioni del principio di proporzionalità in materia penale sostanziale, *ex multis*, MANES, *Principio di proporzionalità. Scelte sanzionatorie e sindacato di legittimità*, in *Libro dell'anno del Diritto*, Treccani, 2013; RECCHIA, *Il principio di proporzionalità nel diritto penale. Scelte di criminalizzazione e ingerenza nei diritti fondamentali*, Giappichelli, 2020. In materia processuale, per quanto attiene al tema delle misure cautelari, si vedano, per tutti NEGRI, *Fumus commissi delicti. La prova per le fattispecie cautelari*, Giappichelli, 2004, 8 ss.; ORLANDI, *Provvisoria esecuzione delle sentenze e presunzione di non colpevolezza*, in AA.VV., *Presunzione di non colpevolezza e disciplina delle impugnazioni (Atti del Convegno, Foggia-Mattinata, 25-27 settembre 1998)*, Giuffrè, 2000, 139.

adoperato deve essere, tra tutti quelli idonei e a disposizione, quello che comporta il minor sacrificio possibile degli interessi confliggenti; la terza e ultima fase, detta della "proporzionalità in senso stretto" o adeguatezza, attiene al bilanciamento operato tra gli interessi in conflitto e si svolge per il tramite di un confronto tra i benefici raggiunti tramite l'adozione della misura e i costi, in termini di necessaria compressione di uno o più diritti, della stessa[272].

Quale criterio di composizione dei conflitti fra diversi valori in gioco alla stregua di un metodo coerente e razionale, il *test* di proporzionalità è entrato a far parte dello strumentario dei giudici costituzionali[273], ordinari e amministrativi quanto meno tutte le volte in cui l'oggetto del processo è contrassegnato dall'antagonismo degli interessi tra pubblico e privato. Campo d'applicazione elettivo del principio di proporzionalità è, in effetti, rappresentato proprio dal diritto pubblico (costituzionale e amministrativo), in ragione della sua naturale attitudine a fungere «da limite armonizzante dell'esercizio del potere ovvero da strumento idoneo ad orientare efficacemente l'esercizio del potere, legislativo o esecutivo»[274]. Esso è, poi, generalmente implicato in ogni decisione concernente i diritti fondamentali[275] visto che la intrinseca struttura di questi ultimi richiede una costante opera di bilanciamento tra interessi in conflitto[276].

Nell'ultimo secolo, il principio in questione si è profondamente innervato nella maggior parte dei sistemi giuridici europei, innestandosi in ordinamenti non solo di *civil law* – quale è quello di origine[277] – ma anche di *common law*[278], con ciò dimostrando notevole

---

[272] Nei giudizi di alcune corti, le note tre fasi del *test* di proporzionalità sono precedute da una quarta, tesa a verificare la legittimità, alla luce dell'ordinamento di riferimento, della misura realizzata. Così STONE SWEET e MATHEWS, *Proportionality balancing and global constitutionalism*, in *Columbia journal of transnational law*, 47, 18; si veda anche CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, Relazione predisposta per la Conferenza trilaterale della Corti costituzionali italiana, portoghese e spagnola, Roma, Palazzo della Consulta 24-26 ottobre 2013, 5.

[273] Il principio di proporzionalità è, infatti, divenuto uno strumento di quotidiana applicazione non solo nelle corti costituzionali di moltissimi stati, ma anche in alcuni organi di diritto internazionale, come il World Trade Organization. Così, STONE SWEET e MATHEWS, *Proportionality balancing*, cit., 1.

[274] SANDULLI, voce *Proporzionalità*, in *Dizionario di diritto pubblico*, a cura di Cassese, Giuffrè, 2006, 4643.

[275] HUSCROFT, MILLER e WEBBER, *Introduction*, in *Proportionality and the rule of law. Rights, Justification, Reasoning,* in *Cambridge University Press*, 2014, 3.

[276] Si veda, a questo proposito, l'analisi di PINO, *Diritti fondamentali e principio di proporzionalità*, in *Ragion pratica*, 2014, 2, 543 ss.

[277] L'elaborazione del principio di proporzionalità risale, come noto, agli ultimi anni del diciannovesimo secolo e si deve agli approdi ermeneutici raggiunti dalla giurisprudenza tedesca nell'ambito del diritto di polizia ("*Polizeirecht*"), vale a dire in un settore caratterizzato da un immanente contrasto tra esigenze securitarie e diritti fondamentali della persona, nell'ambito del quale è sempre presente l'esigenza di una stretta verifica della legittimità delle scelte operate dai pubblici poteri. Si veda, a questo proposito, l'analisi di PINO, *Diritti fondamentali e principio di proporzionalità*, cit., 543 ss.

adattabilità e trasversalità[279]. L'ampia applicazione del principio nel panorama europeo viene generalmente collegata al suo recepimento nell'ambito del diritto comunitario e convenzionale[280], che ne ha consentito la diffusione anche in ordinamenti, come quello italiano, in cui non era riuscito a penetrare autonomamente[281].

Nell'ambito convenzionale, particolare rilievo nella materia delle intrusioni a carattere tecnologico nelle prerogative individuali assume il fatto che tale principio sia non solo apertamente richiamato dall'art. 52 della Convenzione europea dei diritti dell'uomo – che individua i limiti della compressione di ciascuno dei diritti riconosciuti dal sistema convenzionale –, ma indirettamente anche dall'art. 8 della medesima Convenzione, che tutela il diritto alla vita privata e famigliare e che, secondo la Corte europea dei diritti dell'uomo, estende la sua protezione al diritto di riservatezza vantato dagli individui nell'uso delle tecnologie informatiche[282]. Basta scorrere la giurisprudenza della Corte di Strasburgo per avvedersi del rilievo che il giudice europeo attribuisce al principio di proporzionalità nella verifica della legittimità delle indagini informatiche impattanti sulla prerogativa tutelata dall'art. 8 della Convenzione[283].

---

[278] Si veda, a proposito, GALETTA, *Principio di proporzionalità*, in *Diritto* on-line, *www.treccani.it,* 2012., la quale rileva come il principio di proporzionalità sia penetrato anche nell'ordinamento britannico, di fatto soppiantando il suo noto antecedente (il cosiddetto "*Wednesbury test*").

[279] CAIANIELLO, *Il principio di proporzionalità nel procedimento penale,* in *Dir. pen. cont*., 2014, 3-4, 144.

[280] SANDULLI, voce *Proporzionalità*, cit., 4464, che sottolinea come la Corte di Giustizia delle Comunità europee avesse iniziato ad applicare costantemente il principio già negli anni settanta e come lo stesso sia assurto al rango di principio generale dell'ordinamento comunitario. Sul punto, si veda anche CAIANIELLO, *Il principio di proporzionalità*, cit., 148. L'Autore evidenzia, per un verso, come l'intera impalcatura del diritto dell'Unione Europea ponga il criterio della proporzionalità al centro del rapporto tra l'individuo e l'autorità e, per altro verso, come anche la giurisprudenza della Corte europea dei diritti dell'uomo abbia tradizionalmente adoperato il canone della proporzione al fine di verificare la sussistenza di violazioni dei diritti convenzionali fondamentali.

[281] GALETTA, *Principio di proporzionalità,* cit., che sottolinea come, sulla scorta dell'effetto di "*spill-over*" caratteristico dei principi generali dell'Unione, anche paesi in cui il principio di proporzionalità era rimasto sostanzialmente sconosciuto hanno finito per applicarlo anche a fattispecie non aventi rilevanza esclusiva in per il diritto dell'Unione.

[282] Cfr. par. 4.1.2.

[283] Molteplici sono gli esempi in materia di sequestro di dati informatici effettuato in spregio del principio di proporzionalità, ambito nel quale il vaglio di proporzionalità della misura è condotto dalla Corte sulla base della previsione, contenuta nell'articolo 8 della Convenzione, secondo la quale l'ingerenza nel diritto tutelato dalla disposizione è legittima nei limiti in cui si tratti di misura necessaria, in una società democratica, al raggiungimento di una delle finalità previste dalla disposizione stessa. In tal senso si veda, ad esempio, Corte e.d.u., Sez. II, 3 dicembre 2019, Kirdök vs Turchia, relativa a un caso di sequestro di materiale informatico realizzato presso lo studio legale di alcuni avvocati, in forza del quale erano stati sottoposti a vincolo svariati *files* rinvenuti nel disco rigido del *computer* adoperato congiuntamente dagli avvocati dello studio e una chiavetta USB appartenente a una delle ricorrenti. Si veda, altresì Corte e.d.u., Sez. III, 30 maggio 2017, Trabajo Rueda vs Spagna, caso relativo al sequestro di un *personal computer* contenente materiale pedopornografico nel quale la Corte ha reputato l'analisi dei *files* contenuti nello stesso non proporzionata agli scopi legittimi individuati dall'articolo 8 della Convenzione. Ciò in quanto

D'altronde, la stessa Convenzione di Budapest sul *cybercrime*, approvata nel contesto del Consiglio d'Europa, all'articolo 15 subordinava la messa a punto, da parte degli Stati firmatari, di una normativa in materia di indagini informatiche al rispetto del principio di proporzionalità[284].

Non può, poi, non menzionarsi la crescente importanza assunta dal principio in parola nella giurisprudenza della Corte di Giustizia dell'Unione Europea in materia di compressione delle prerogative di cui agli artt. 7 e 8 della Carta di Nizza, tramite i continui moniti rivolti agli Stati per l'adozione di normative improntate al rispetto del principio di proporzionalità quale condizione imprescindibile per la legittimità di una restrizione dei diritti fondamentali in essa riconosciuti. Emblematiche sono, sotto questo profilo, le pronunce adottate dai Giudici di Lussemburgo nell'ultimo decennio in materia di dati relativi al traffico, e, più in generale, sulle questioni attinenti ai diritti scaturenti dall'uso delle nuove tecnologie digitali e al trattamento dei dati degli utilizzatori di simili tecnologie[285].

Tale prospettiva, però, va consolidandosi anche sul piano interno, come dimostrato non solo da alcune precise scelte normative operate proprio nel campo delle investigazioni informatiche, ma altresì dall'accresciuta importanza tributata al principio in parola da dottrina e giurisprudenza.

---

all'accesso al *personal computer* si era proceduto in assenza di autorizzazione del giudice pur in mancanza di una situazione di urgenza tale da giustificare il mancato intervento di quest'ultimo.

[284] Nel Rapporto esplicativo della Convenzione, consultabile sulla pagina web https://rm.coe.int/16800cce5b, tale linea guida viene ulteriormente ribadita ai paragrafi 145 e 146, secondo i quali le procedure adottate dagli Stati per l'implementazione della Convenzione avrebbero dovuto incorporare il rispetto del principio in parola, con la precisazione che con riferimento ai contraenti dell'area europea tale obbligo sarebbe comunque derivato dai principi contenuti nella Convenzione europea dei diritti dell'uomo.

[285] Tra le più significative, Corte Giust., 8 aprile 2014, Digital Rights Ireland vs Minister for Communications e a., C-293/12 e C-594/12, che ha annullato la direttiva 2006/24 in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica in quanto eccedente i limiti imposti da principio di proporzionalità alla luce degli artt. 7, 8 e 52 della Carta dei Diritti Fondamentali dell'Unione Europea; passando per Corte Giust., 13 maggio 2014, Google Spain SL e Google Inc. vs Agencia Española de Protección de Datos (AEPD), C-131/12, in materia di diritto all'oblio, e per la successiva sentenza Corte Giust., 6 ottobre 2015 Schrems vs Data Protection Commissioner, C-362/14, in materia di trasferimento dei dati personali dall'Unione Europea agli Stati Uniti; ancora, la pronuncia del 21 dicembre 2016, Tele2 Severige e Watson e a., C – 203/15 e C – 698/15, che ha ulteriormente ribadito i principi già enucleati nella precedente sentenza Digital Rights Ireland quanto ai requisiti minimi per il rispetto del principio di proporzionalità di una normativa nazionale in materia di conservazione dei dati relativi al traffico elettronico. Si vedano anche, sul punto, Corte Giust., 2 ottobre 2018, Ministerio Fiscal, C-207/16; Corte Giust., 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18.

Sotto il primo profilo, si è osservato in dottrina[286] come il legislatore del 2008, nel dare attuazione alla Convenzione di Budapest sul *cybercrime* mediante l'introduzione di specifiche norme relative alle investigazioni informatiche, abbia inteso dare compimento al principio di proporzionalità, come testimoniato dal riferimento, contenuto nelle diverse disposizioni che regolano ispezioni, perquisizioni e sequestri informatici, alla necessità di adottare misure tecniche idonee ad evitare l'alterazione dei dati in tal modo acquisiti.

Sotto il secondo profilo, e spingendosi anche al di là del confine delle sole investigazioni informatiche, non è mancato chi, in virtù della naturale attitudine del principio di proporzionalità a fungere «da limite armonizzante dell'esercizio del potere ovvero da strumento idoneo ad orientare efficacemente l'esercizio del potere, legislativo o esecutivo»[287], ha postulato la necessaria operatività del principio di proporzionalità alla stregua di un criterio capace di informare di sé l'intera dinamica procedimentale penale[288]. Essendo il processo penale caratterizzato dalla costante tensione tra le "ragioni" dell'individuo e quelle dell'autorità[289], infatti, l'applicazione del principio in parola non solo rappresenta un'utile guida nella fase dell'adozione e dell'esecuzione di misure processuali restrittive di diritti fondamentali[290], ma dovrebbe operare alla stregua di una vera e propria bussola anzitutto per il legislatore, cui è affidato il compito di adottare norme in grado di comporre di volta in volta in maniera adeguata tale conflitto, nel rispetto del principio di legalità processuale.

A questo proposito, non possono non condividersi le conclusioni di quanti ritengono che, nel contesto del progressivo ampliamento del ricorso a strumenti intrusivi di carattere tecnologico nel processo penale, l'unico rimedio idoneo a garantire la

---

[286] COSTANZI, *Perquisizione e sequestro informatico. L'interesse al riesame nel caso di estrazione di copie digitali e restituzione dell'originale*; in *Cass. pen*., 2016, 1, 278, che rileva che un'intrusione nella sfera privata dei soggetti interessati dalla misura sarebbe sproporzionata ove non offrisse adeguate garanzie di genuinità dei dati in tal modo acquisiti.

[287] SANDULLI, voce *Proporzionalità*, cit., 4643.

[288] In questo senso, CAIANIELLO, *Il principio di proporzionalità*, cit., 148, secondo il quale «*la proporzionalità può essere considerata un corollario della inviolabilità di certe prerogative individuali tutelate dalla Costituzione che tipicamente, anche se non esclusivamente, sono poste in tensione nell'alveo del procedimento penale*».

[289] Così, TORRE, *Indagini informatiche e principio di proporzionalità*, in *Proc. pen. e giust.*, 2019, 6, 1435.

[290] Osservano che il principio di proporzionalità ha un legame privilegiato con i diritti fondamentali HUSCROFT, MILLER e WEBBER, *Introduction*, cit., 3. La intrinseca struttura di questi ultimi, infatti, richiede una costante opera di bilanciamento con interessi in conflitto, come rileva PINO, *Diritti fondamentali e principio di proporzionalità*, cit., 543 ss.

legittimità della compressione dei diritti dei singoli sia proprio il rafforzamento della legalità processuale, tramite la realizzazione di una trama normativa suscettibile di fissare i criteri e i limiti dell'attività di bilanciamento poi operata, nel caso concreto, dal giudice[291]. In altre parole, la messa a punto di una disciplina legislativa in materia, capace di cogliere le peculiarità della stessa e di fissare, conseguentemente, in maniera più stringente i limiti dell'intervento coercitivo dello Stato sulle prerogative individuali è presupposto imprescindibile affinché il vaglio di proporzionalità possa essere adeguatamente condotto nel processo, risultando, altrimenti, del tutto sbrigliato da qualsivoglia criterio in grado di condurne razionalmente gli esiti. In tal senso, peraltro, si è recentemente espressa anche la Corte di Giustizia dell'Unione Europea, la quale, in un'importante pronuncia in materia di acquisizione dei tabulati relativi al traffico telefonico, ha stabilito che, onde soddisfare il principio di proporzionalità imposto in materia dalla normativa europea, è essenziale la messa a punto di una disciplina nazionale legalmente vincolante che preveda regole chiare e fissi requisiti minimi che garantiscano che l'ingerenza nei diritti fondamentali stabiliti dagli artt. 6 e 7 della Carta di Nizza sia limitata allo stretto necessario[292].

4.1.1. (segue) La riserva di giurisdizione.

La conclusione precedentemente raggiunta in ordine all'incidenza della misura, quanto meno, sulla prerogativa di cui all'art. 14 Cost. impone di svolgere una riflessione in merito all'operatività della riserva di giurisdizione ai fini dell'applicazione della medesima. In forza del richiamo operato dall'art. 14 Cost., la restrizione del diritto all'inviolabilità del domicilio, può avvenire solo con le garanzie che la Costituzione pone a presidio della libertà personale. Ciò implica che l'atto di ingerenza nel diritto fondamentale debba essere adottato dall'autorità giudiziaria e adeguatamente motivato.

Si ripropongono nella materia *de qua* i dubbi interpretativi che hanno storicamente riguardato la delimitazione del concetto di "autorità giudiziaria" adoperato dal legislatore costituente nell'art. 13 Cost. Comprendere se la locuzione si riferisca al solo

[291] In tal senso, NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. e proc. pen.*, 2020, 1, 32. Per il rilievo secondo il quale in materia di diritti fondamentali anche il legislatore dovrebbe ispirarsi al principio di proporzionalità onde verificare in che misura sia legittima la compressione di un diritto dichiarato inviolabile, vedi anche ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali, in Riv. it. dir. e proc. pen.*, 2014, 3, 1157.

[292] Corte Giust., Grande Sezione, 2 marzo 2021, C-746/18, H.K.

giudice o includa anche la figura del pubblico ministero, naturalmente, non è questione meramente teorica ma presenta risvolti pratici di estrema rilevanza, atteso che il nostro sistema processuale penale riconosce all'organo dell'accusa il potere di adottare provvedimenti suscettibili di incidere sulla libertà personale dei singoli[293].

La norma è stata storicamente interpretata nel senso più ampio, quale riferimento a quei «membri della magistratura, costituente un ordine autonomo e indipendente da ogni altro potere, di cui parla l'art. 104, comma 1, Cost. Insomma, si è voluto assicurare che, laddove sia in questione l'adozione di misure *contra libertatem*, a deliberarle sia un soggetto munito di obiettività ed indipendenza nei confronti del potere politico, anche e soprattutto per assicurare quell'eguaglianza di trattamento che la Carta fondamentale richiede all'art. 3»[294].

Nonostante, però, l'argomento letterale[295] sembrerebbe deporre nel senso appena detto, il dubbio che la formulazione della norma costituzionale debba, in realtà, ritenersi riferita al solo giudice e non anche al pubblico ministero è ragionevole e poggia su almeno due rilievi di ordine sistematico.

In primo luogo, l'art. 111, comma 7, Cost., nel sancire la garanzia della ricorribilità dei provvedimenti in materia di libertà personale, fa riferimento ai soli provvedimenti giurisdizionali. Sarebbe, allora, del tutto irragionevole consentire al pubblico ministero di adottare un provvedimento incidente sulla libertà personale del singolo in ordine al quale non sia costituzionalmente imposta la garanzia del ricorso, sempre previsto, invece, nel caso di adozione da parte del giudice, ossia da un organo che presenta, oltre alla garanzia dell'indipendenza, anche quella dell'imparzialità.

Sotto altro profilo, alla conclusione secondo la quale la riserva di cui all'art. 13 Cost. sarebbe da intendersi riferita anche al pubblico ministero osterebbe la storica ambiguità che, nel nostro ordinamento, è connaturata alla sua figura quale organo indipendente ma, cionondimeno, portatore di un interesse di parte e di un potere di impulso nell'esercizio dell'azione penale che non consente di ritenerlo neutrale. Si tratta di un'ambiguità che, come stigmatizzato da autorevole dottrina, neppure i padri costituenti

[293] GREVI, *Libertà personale dell'imputato*, in *Enc. dir.*, XXIV, Giuffrè, 1974, 343.
[294] DI BITONTO e MOSCARINI, *Introduzione alla procedura penale*, Giappichelli, 2018, 28.
[295] Come notano DI BITONTO e MOSCARINI, *Introduzione alla procedura penale*, cit., 28. laddove il testo costituzionale abbia inteso far riferimento alla sola autorità giurisdizionale lo ha fatto espressamente.

hanno, infine, inteso risolvere[296], con la conseguenza che il nostro sistema costituzionale non pare escludere che un organo non neutrale possa legittimamente adottare provvedimenti restrittivi della libertà personale e domiciliare.

Tali considerazioni hanno spinto una parte della dottrina a concludere nel senso della necessaria adesione a una interpretazione restrittiva della locuzione di cui all'art. 13 Cost., sulla scorta dell'osservazione secondo la quale, pur non emergendo dal dato testuale, essa sarebbe comunque imposta dal ruolo di parte svolto dal pubblico ministero, che «pur se spiegabile in termini di dovere anziché in termini di interesse – e come tale non confacente all'emanazione di provvedimenti che sono stati affidati all'autorità giudiziaria a presidio di una libertà in linea di principio inviolabile, nonché a garanzia – super partes – dell'osservanza della legge ordinaria»[297].

Tale soluzione, però, non è prevalsa né in dottrina né in giurisprudenza, con la conseguenza che tutti i poteri in materia di libertà personale e domiciliare riconosciuti al pubblico ministero dal vecchio così come dal nuovo codice di procedura penale si sono reputati conformi al testo Costituzionale. L'argomento letterale ha finito col prevalere su quelli sistematici, anche sulla base dell'osservazione per la quale i Costituenti, più che non prendere posizione sul punto, abbiano consapevolmente inteso adoperare la formula più ampia tenendo presente il sistema processuale allora vigente e non volendo escludere la legittimazione del pubblico ministero all'esercizio di tutta una serie di poteri di incidenza sulla libertà personale e domiciliare che la legge processuale gli riconosceva[298].

Cionondimeno, lo stesso legislatore ordinario ha, comunque, inteso aderire alla soluzione più garantista almeno con riferimento ai provvedimenti coercitivi più gravi[299],

---

[296] PISANI, *Libertà personale e processo*, Cedam, 1974, 388 ss., il quale evidenzia la «incertezza di fondo che ancora permane intorno alla configurazione dell'istituto, il quale continua a risentire oggi degli illogici compromessi da cui è stato plasmato nel corso dell'800 ed attraverso i due codici processuali di questo secolo. La separata disciplina del Pubblico Ministero, cioè, non fa che riflettere la mancata scelta, da parte della Costituzione, fra il ruolo di giudice e quello di parte, che esso va svolgendo da molti decenni. Circostanza questa assai grave, che riverbera una serie di conseguenze proprio in direzione della libertà personale dell'imputato». Nel senso che il problema dell'interpretazione della riserva di cui all'art. 13 Cost. può risolversi solo risolvendo quello, preliminare, della natura del pubblico ministero nella Costituzione, BARILE, *Le libertà nella costituzione*, Cedam, 1966, 119-120.

[297] PISANI, *La custodia preventiva: profili costituzionali*, in *L'ind. pen*., 1970, 187.

[298] Così, ELIA, *Libertà personale e misure di prevenzione*, Giuffrè, 1962, 95.

[299] FANUELE, *La libertà personale*, in AA.VV., *Processo penale e Costituzione*, a cura di Dinacci, Giuffrè, 2010, 218.

come dimostrato dall'attribuzione al giudice del potere di disporre tutte le misure cautelari personali, tanto le coercitive quanto le interdittive[300].

Ci si dovrebbe chiedere, dunque, se una simile soluzione si imponga anche in materia di misure restrittive incidenti sul diritto all'inviolabilità del domicilio informatico laddove, come accade per la misura investigativa oggetto di analisi, il livello di intrusione nella sfera di libertà del singolo sia tanto elevato. Sulla base delle conclusioni appena raggiunte, la risposta positiva non pare essere costituzionalmente imposta. Nondimeno, essa è senz'altro preferibile quanto meno alla luce di un dato: se è vero che l'adozione di misure così fortemente incidenti sui diritti di libertà dei singoli impone l'effettuazione di un rigoroso vaglio di proporzionalità non solo sul piano della configurazione legale dell'istituto, ma altresì su quello della singola vicenda giudiziaria, pare difficile sostenere che tale vaglio possa essere affidato a un soggetto che, in quello stesso procedimento, è portatore di uno degli interessi in conflitto, ovvero quello alla repressione dei reati e che, dunque, per definizione, non è terzo. Come si vedrà, tale soluzione sembra, oggi, imposta anche sul piano sovranazionale.

4.1.2. (segue) I percorsi tracciati dalle Corti europee in punto di legittimità delle restrizioni al diritto alla vita privata.

Ai fini dell'individuazione di uno statuto di garanzie minime applicabile a una misura investigativa suscettibile di comprimere il diritto alla vita privata, non può prescindersi dal tenere in considerazione alcune fondamentali direttive provenienti dalla giurisprudenza della Corte di Giustizia dell'Unione europea e dalla Corte europea dei diritti dell'uomo[301] in tema di legittimità di una misura restrittiva incidente sui diritti di cui agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea e dell'art. 8 della Convenzione europea dei diritti dell'uomo. Gli obblighi assunti, sul piano sovranazionale e internazionale, dall'ordinamento italiano, infatti, impongono al legislatore di adeguare la normativa interna ai livelli di tutela dei diritti fondamentali riconosciuti nei due atti sopra menzionati, benché siano profondamente differenti le

[300] DI BITONTO e MOSCARINI, *Introduzione alla procedura penale*, cit., 29.

[301] Si precisa che nella presente analisi si ometterà di ripetere tutto quanto già evidenziato nel precedente paragrafo in merito ai principi espressi, sul piano generale, dalle due Corti con riferimento al necessario rispetto del principio di proporzionalità delle misure restrittive dei diritti fondamentali dei singoli riconosciuti dai due sistemi giuridici. Tali principi, però, sono da intendersi richiamati in questa sede.

conseguenze giuridiche di una violazione dei medesimi[302]. D'altronde, la forte interrelazione che avvince le due fonti è unanimemente riconosciuta dalla giurisprudenza[303] delle relative Corti ed emerge plasticamente dalla lettura dell'art. 51 della Carta di Nizza, che stabilisce che laddove i diritti riconosciuti dalla medesima Carta siano corrispondenti a quelli previsti dalla Convenzione europea dei diritti dell'uomo, il loro significato e la loro portata sono uguali a quelli conferiti dalla stessa, salva la possibilità che il diritto dell'Unione conceda una protezione più estesa[304]. Tanto consiglia di procedere a un'analisi congiunta del "*corpus* normativo" risultante dall'interazione delle due fonti, prendendo, però, le mosse dalla disciplina Convenzionale.

---

[302] Per quanto concerne il diritto dell'Unione Europea, come noto, in presenza di un contrasto tra la normativa interna e quella europea al giudice nazionale si prospettano tre alternative: la disapplicazione della norma interna contrastante con quella sovranazionale che sia dotata di efficacia diretta; la proposizione di una questione di legittimità costituzionale, ove reputasse la norma europea non dotata di efficacia diretta; la proposizione di una questione pregiudiziale, ai sensi dell'art. 267 TFUE, ove reputasse necessario ottenere chiarimenti da parte della Corte di Giustizia in ordine all'interpretazione della disciplina sovranazionale. Corte Giust., sentenza 9 marzo 1978, Amministrazione delle Finanze dello Stato c. Simmenthal SpA, causa 106/77; Corte cost., 5 giugno 1984, n. 170; in dottrina, si veda, *ex multis*, Gallo, *Efficacia diretta del diritto UE, procedimento pregiudiziale e Corte Costituzionale: una lettura congiunta delle sentenze n. 269/2017 e 115/2018*, in *Riv. ass. it. cost.*, 2019, 1, 161-162. Con specifico riferimento alla vincolatività delle norme sancite dalla Carta dei diritti fondamentali dell'Unione Europea, deve precisarsi, però, che l'art. 51 della medesima Carta stabilisce che le disposizioni ivi previste si applicano agli Stati Membri esclusivamente nell'attuazione del diritto dell'Unione. Ne deriva che presupposto per rilevare un contrasto tra la normativa interna e quella europea in materia di tutela dei diritti fondamentali dei sia rappresentato dal fatto che la normativa nazionale rientri nello *scope* della Carta e sia attuativa di quella europea. Nella sentenza *Fransson* del 26 febbraio 2013, resa nella causa C-617/10, la Corte di Giustizia ha precisato il significato della disposizione *di* cui all'art. 51 della Carta confermando la giurisprudenza precedente (Corte Giust., 13 luglio 1989, C-5/88, Wachauf; Corte Giust., 18 dicembre 1997, C-309/96, Annibaldi) all'entrata in vigore del Trattato di Lisbona (che ha attribuito alla Carta di Nizza lo stesso valore giuridico dei Trattati), che aveva fornito della locuzione di cui all'art. 51 un'interpretazione piuttosto ampia. Secondo tale interpretazione, rientra nel concetto di «attuazione del diritto dell'Unione» ogni attività nazionale rientrante «nell'ambito» o «nel campo di applicazione» di tale diritto (cfr. AA.VV., *Manuale dei diritti fondamentali in Europa*, Il Mulino, 2019, 83). Quanto, invece, al diritto convenzionale, lo stesso opera, come noto, in via indiretta: le norme della Convenzione sono interposte nel giudizio di legittimità costituzionale della norma interna che ha quale parametro l'art. 117 Cost., come stabilito da Corte Cost., 24 ottobre 2007, n. 348, in *Giur. cost.*, 2007, 3475 ss., con nota di PINELLI, *Sul trattamento giurisdizionale della CEDU*, cit., 3535 ss., con nota di CARTABIA, *Le sentenze "gemelle": diritti fondamentali, fonti, giudici*.

[303] *Ex multis*, Corte Giust., 9 novembre 2010, causa C-92/09, Volker und Markus Schecke and Eifert, ove la Corte evidenzia che «le limitazioni diritto alla vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli artt. 7 e 8 della Carta» […] «possono essere legittimamente apportate al diritto alla protezione dei dati personali corrispondano a quelle tollerate nell'ambito dell'art. 8 della CEDU». Cfr. anche Corte Giust., 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18.

[304] Anche nelle "*Spiegazioni relative alla Carta dei diritti fondamentali*", in GUUE del 14 dicembre 2007, C 303,17, si precisa che «*I diritti di cui all'articolo 7 corrispondono a quelli garantiti dall'articolo 8 della CEDU*».

La ragione di tale opzione risiede nel maggior grado di approfondimento che l'elaborazione della Corte europea dei diritti dell'uomo ha raggiunto, nel tempo, in merito al reticolo di tutele relativo al diritto alla vita privata rispetto alla Corte di Giustizia dell'Unione. Visto che, conformemente all'art. 51 della Carta di Nizza, i principi in essa stabiliti vincolano gli Stati membri solo quando agiscono nell'attuazione del diritto dell'Unione, infatti, la Corte di Giustizia ha avuto meno occasioni di pronunciarsi sul punto. Nondimeno, come si vedrà, soprattutto negli ultimi anni ha avviato un'operazione sempre più incisiva di progressiva definizione dei diritti dei singoli con riguardo all'uso delle tecnologie informatiche e al suo impatto sulla vita privata.

Nonostante la mancanza, nella relativa Convenzione, di una norma specificamente posta a protezione della riservatezza informatica dei singoli, la Corte europea dei diritti dell'uomo ha costantemente ricavato dall'art. 8 il divieto, per gli Stati, di ingerirsi in maniera sproporzionata nelle prerogative individuali rilevanti in questo ambito, evidenziando come la raccolta e la conservazione di dati nell'ambito dei servizi di sicurezza e di *law enforcement* su determinati individui possa costituire un'interferenza nel loro diritto alla vita privata. Una conclusione, questa, che aveva già raggiunto all'inizio degli anni 2000[305] e che non ha mancato di ribadire anche in tempi più recenti[306].

Peraltro, i Giudici di Strasburgo hanno storicamente avallato una interpretazione del concetto di "vita privata" particolarmente ampia, suscettibile di comprendere non solo la protezione della "sfera intima" del singolo, ma altresì della proiezione esterna di tale sfera, consistente nella tendenza a intessere relazioni con altri esseri umani[307]. Tanto in perfetta assonanza con l'evoluzione che, come si è visto nel capitolo 1, ha contrassegnato in pressoché tutti gli ordinamenti occidentali il concetto di *privacy*.

Una lettura tanto ampia ha rappresentato un tassello fondamentale, nell'ottica della Corte, al fine di emancipare tale prerogativa dalla natura pubblica o privata del luogo o dei luoghi nei quali la stessa si svolge. Nell'importante causa Uzun vs Germania del

[305] Corte e.d.u., 4 maggio 2000, app. n. 28341/95, Rotaru vs Romania.
[306] Corte e.d.u., 24 aprile 2019, app. n. 43514/15, Catt. vs Regno Unito.
[307] Cfr. Corte e.d.u.., 24 gennaio 2017, app. n. 25358/12, Paradiso and Campanelli vs Italia; Corte e.d.u.., 5 settembre 2017, app. n. 61496/08, Barbulescu vs Romania, nella quale si specifica che il concetto di "vita privata" ricomprende il diritto della persona di avvicinare gli altri per instaurare rapporti con loro, ovvero il diritto a una "vita sociale privata"; Corte e.d.u.., 24 febbraio 1998, app. n. 21439/93, Botta vs Italia.

2010[308], così, la Corte ha evidenziato come «*article 8 protects,* inter alia*, a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"*».

Sulla base di queste premesse, i Giudici di Strasburgo hanno edificato un vero e proprio complesso di garanzie che devono circondare l'adozione, da parte degli Stati, di misure incidenti sul diritto al rispetto della vita privata su cui conviene soffermarsi brevemente.

I parametri per valutare la legittimità dell'ingerenza ai sensi dell'art. 8 della Convenzione sono rappresentati dall'esistenza di una base legale e dal requisito della necessità della misura, "in una società democratica", per il raggiungimento di una serie di finalità legittime tra cui, ovviamente, rientra quella dell'accertamento e repressione dei reati. Secondo la Corte, benché gli Stati conservino una certa discrezionalità nella scelta delle misure adottabili per il raggiungimento degli obiettivi legittimi di cui all'art. 8 della Convenzione, tale margine di apprezzamento è soggetto alla supervisione della Corte medesima per tutto quanto concerne le scelte legislative adottate e la loro attuazione sul piano giudiziale. Tale giudizio dipende da tutte le circostanze del caso, quali la natura, lo scopo e la durata della misura, i presupposti richiesti per la sua adozione, l'autorità competente ad autorizzarla, attuarla e supervisionarla e, infine, i rimedi previsti dal diritto nazionale in caso di possibili violazioni[309].

La verifica del rispetto di simili presupposti si compie, anzitutto, sulla scorta dell'analisi della base legale apprestata dal diritto interno in ossequio alla previsione di cui all'art. 8 della Convenzione, finalizzata ad assicurare la prevedibilità (*"foreseebility*") dell'ingerenza sul diritto fondamentale del singolo. L'interpretazione offerta dalla Corte di Strasburgo in merito a tale requisito è improntata a un criterio di effettività: la riserva prevista dall'art. 8 della Convenzione non riguarda solo l'esistenza della legge, ma anche la sua qualità, che deve soddisfare gli *standard* di prevedibilità imposti dalla normativa convenzionale[310]. Gli Stati sono tenuti a prevedere regole precise, chiare e dettagliate che possano essere conosciute e comprese dai cittadini. La legge dovrebbe,

[308] Corte e.d.u., 2 settembre 2010, app. n. 35623/05, Uzun vs Germania.
[309] Corte e.d.u., 2 dicembre 2015, app. n. 47143/06, Zacharov vs Russia.
[310] Si vedano, però, le considerazioni articolate nel capitolo 1, par. 3.1. in merito alla elasticità del parametro in questione che, secondo la costante giurisprudenza della Corte, è suscettibile di essere soddisfatto anche a fronte di una legge non scritta, che normalmente caratterizza i sistemi di *common law*.

dunque, individuare i casi, le circostanze e le condizioni alle quali l'ingerenza è legittima, ma altresì prevedere l'adozione di misure volte a consentire la conservazione della documentazione relativa alle operazioni realizzate, specificando le regole applicabili per la protezione o distruzione della medesima. Al contempo, quanto all'applicazione concreta delle misure, non dovrebbe essere lasciato eccessivo spazio di discrezionalità alle autorità competenti per la loro adozione[311].

Tale presupposto sembra assumere, nella logica ricostruttiva fatta propria dai Giudici di Stasburgo, un rilievo sempre maggiore. In una recente sentenza del 2021[312] la Corte, nell'ambito di un procedimento instaurato con riferimento a una perquisizione in un sistema informatico, ha reputato sussistente la violazione della Convenzione per il carattere non proporzionato della misura in ragione del fatto che si fosse trattato di un'iniziativa estemporanea degli inquirenti e che mancasse una disciplina legislativa chiara in ordine alle concrete modalità di esecuzione della perquisizione e del sequestro informatico per assicurare la pertinenza della misura. Tanto nonostante nel caso di specie fossero state adottate alcune cautele volte a ristringere l'ambito della ricerca e la conseguente intrusione nella vita privata del singolo[313].

Anche in ordine a tale punto la Corte di Strasburgo ha offerto importanti precisazioni, sancendo l'illegittimità dell'apprensione indiscriminata di tutti i dati contenuti in un sistema informatico senza indicazione, nel provvedimento autorizzativo, dell'ambito di applicazione della misura[314]. Come si vedrà *infra*, proprio il requisito della pertinenzialità della misura quale irrinunciabile presupposto della sua proporzionalità è quello che genera maggiori problemi quando si tratti della sua implementazione effettiva.

Preziose indicazioni sono state, poi, fornite dalla Corte anche con riferimento al necessario riscontro – da compiere in concreto sul piano giudiziario – dell'esistenza di indizi sufficienti a carico del soggetto che subisce l'imposizione della misura. Ciò non

---

[311] Per questa e per le precedenti affermazioni, Corte e.d.u., 30 giugno 1998, app. n. 58/1997/842/1048, Valenzuela Contreras vs Spagna.

[312] Corte e.d.u., 16 novembre 2021, app. n. 698/19, Sargava vs Estonia.

[313] In particolare, si trattava di una ricerca operata tramite l'inserimento di parole chiave in un sistema informatico di tipo *smartphone*.

[314] Cfr. Corte e.d.u., 3 luglio 2012, app. n. 30457/2006, Robathin vs Austria; Corte e.d.u., 22 maggio 2008, app. n. 65755/01, Iliya Stefanov vs Bulgaria; Corte e.d.u., 12 febbraio 2015, app. n. 5678/06, Yuditskaya ant others vs Russia; Corte e.d.u., 16 novembre 2021, app. n. 698/19, Sargava vs Estonia. Sul punto, quanto ai principi espressi nell'ordinamento italiano, si vedano le considerazioni del capitolo 3, par. 1.1.

esclude che la misura possa comportare l'incidenza su diritti di soggetti terzi rispetto all'indagine in corso; in tal caso, però, spetta ancora una volta alla legge la definizione dei presupposti in base ai quali una simile evenienza può verificarsi[315].

Perché la normativa interna possa dirsi proporzionata, poi, è necessario che preveda, per lo svolgimento dell'atto investigativo, una durata massima. Principio, questo, che è stato costantemente ribadito dalla Corte di Strasburgo[316] e che, come si vedrà, assume particolare rilievo con riferimento alle misure di sorveglianza continuativa che saranno analizzate nel prossimo capitolo. Sul punto, peraltro, importanti precisazioni sono state fornite anche dalla Corte di Giustizia, come si avrà modo di evidenziare più avanti.

Da ultimo, la legge deve prevedere opportuni rimedi azionabili da parte del cittadino che reputi di aver subito una compressione illegittima del suo diritto alla vita privata da parte delle autorità pubbliche. In un caso relativo a una perquisizione domiciliare, ad esempio, la Corte ha ravvisato una violazione dell'art. 8 della Convenzione in quanto l'interessato non aveva avuto la possibilità di attivare, *ex ante* ovvero *a posteriori*, un controllo giurisdizionale effettivo sulla sussistenza dei presupposti giustificativi del provvedimento. In particolare, secondo la Corte, «ciò implica che le persone interessate possano ottenere un controllo giurisdizionale effettivo, tanto in fatto come in diritto, della misura in questione e dello svolgimento della stessa. Quando un'operazione considerata irregolare ha già avuto luogo, il ricorso o i ricorsi disponibili devono permettere di fornire all'interessato una riparazione adeguata […]. A quest'ultimo riguardo, la Corte rammenta di avere ammesso che, in alcune circostanze, il controllo della misura contraria all'articolo 8 effettuato dai giudici penali fornisce una riparazione adeguata per l'interessato, dal momento che il giudice procede a un controllo effettivo della legittimità e della necessità della misura contestata e, se del caso, esclude dal processo penale gli elementi di prova raccolti»[317].

Sulle medesime linee interpretative appena tracciate si è assestata anche la Corte di Giustizia dell'Unione Europea con riguardo alle misure restrittive incidenti sui diritti di

---

[315] Corte e.d.u., 14 settembre 2009, app. n. 25198/02, Iordachi e altri vs Moldavia.

[316] *Ex multis*, Corte e.d.u., 6 settembre 1978, no. 28, Klass and Others vs Germany; sent. 29 giugno 2006, no. 54934/00, Weber and Saravia vs Germany; sent. 9 giugno 2009, no. 72094/01, Kvasnica vs Slovakia.

[317] Cfr. Corte e.d.u., Sez. I, 27 settembre 2018, n. 57278, Brazi vs Italia; Corte e.d.u., 4 dicembre 2015, app. n. 47143/06, Zakharov vs Russia, per la quale «*personal data in the police sector, which provides that where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced*»; e ancora, Corte e.d.u., 7 giugno 2016, app. n. 19602/06, Cevat Özel c. Turchia.

cui agli articoli 7 e 8 della Carta di Nizza[318]. A differenza dell'art. 8 della Convenzione europea dei diritti dell'uomo, gli artt. 7 e 8 della Carta non prevedono le condizioni alle quali una restrizione dei diritti ivi sanciti è legittima. Tali condizioni sono, però, enucleabili dall'art. 51 del medesimo *corpus* normativo, che dispone che «eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e delle libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui». Trattasi, come si vede, di una clausola in buona misura sovrapponibile a quella sancita dall'art. 8 della Convenzione. Tanto, come già evidenziato, ha fatto sì che la Corte di Giustizia operasse un costante richiamo alla giurisprudenza di Strasburgo nell'analisi della portata e delle possibili restrizioni del diritto alla vita privata sancito dalla Carta, anche in forza la clausola di cui al comma 3 dell'art. 52 della medesima.

Nonostante, però, la sostanziale sovrapponibilità dei percorsi ermeneutici tracciati dalle due Corti, vi sono almeno tre aspetti su cui la giurisprudenza di Lussemburgo ha arricchito le indicazioni provenienti dalla Corte europea dei diritti dell'uomo e, se possibile, tracciato un profilo di garanzie più elevato di quello individuato da quest'ultima. Il riferimento è, anzitutto, alla individuazione di una sorta di nocciolo duro del diritto alla vita privata la cui restrizione impone allo Stato l'adozione del più elevato livello di cautele possibile; in secondo luogo, al legame che avvince la gravità dell'intrusione e quella del reato in relazione al quale si procede ai fini della verifica di proporzionalità della misura; in terzo luogo, all'autorità legittimata ad adottarla.

A offrire ripetutamente alla Corte di Giustizia l'occasione di pronunciarsi in relazione alla legittimità della compressione del diritto alla vita privata e della sua componente relativa al trattamento dei dati personali è stato il perdurante dibattito in merito alla acquisizione, da parte dell'autorità pubblica, dei tabulati relativi al traffico telefonico e telematico con finalità di repressione e accertamento dei reati. Nell'ambito di questa

[318] La Corte di Giustizia suole ricondurre alla medesima matrice, consistente nella protezione della vita privata, i diritti sanciti dai due articoli. Cfr. Corte Giust., 9 novembre 2010, C-92/09, Volker und Markus Schecke and Eifert, in cui si stabilisce che «il rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali» è «riconosciuto dagli artt. 7 e 8 della Carta».

materia, le linee essenziali tracciate dalla Corte a partire, quanto meno, dal 2014[319], hanno trovato piena maturazione nella pronuncia emessa nel marzo 2021[320] su impulso della Corte Suprema estone, che ha deciso un rinvio pregiudiziale sull'interpretazione dell'art. 15, paragrafo 1, della direttiva 2002/58 CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[321].

Le questioni pregiudiziali sollevate dal giudice *a quo* vertevano su due distinti profili della normativa europea, attinenti, per un verso, alla precisa perimetrazione dei presupposti di un'ingerenza nei diritti fondamentali sanciti a livello europeo e, per altro verso, all'individuazione dell'organo competente a esercitare un controllo preventivo sull'ingerenza medesima. Sotto il primo profilo, si sollecitava, dunque, la Corte di Giustizia a pronunciarsi sulla necessaria correlazione tra la gravità dei reati oggetto di accertamento e l'incidenza della misura conservativa e acquisitiva dei tabulati sui diritti fondamentali sanciti dalla Carta, nonché sulla rilevanza del quantitativo di dati acquisiti nella valutazione della gravità dell'ingerenza medesima. Sotto il secondo profilo, invece, la Corte era chiamata a stabilire se potesse o meno considerarsi autorità indipendente il pubblico ministero che dirige il procedimento istruttorio e che rappresenti la pubblica accusa nel procedimento giudiziario.

Ribadendo le conclusioni già parzialmente raggiunte nella giurisprudenza precedente[322], la Corte di Giustizia ha stabilito che la gravità dell'ingerenza nei diritti fondamentali sanciti dalla Carta di Nizza deve essere correlata all'interesse perseguito tramite l'adozione della misura, di modo che intrusioni di particolare gravità possono essere giustificate esclusivamente alla luce dell'esigenza di accertare e reprimere forme particolarmente gravi di criminalità[323]. Dallo sviluppo argomentativo della sentenza

[319] Cfr. Corte Giust., 8 aprile 2014, Digital Rights Ireland vs Minister for Communications e a., C-293/12 e C-594/12; Corte Giust., 21 dicembre 2016, Tele2 Severige e Watson e a., C – 203/15 e C – 698/15; Corte Giust., 2 ottobre 2018, Ministerio Fiscal, C-207/16; Corte Giust., 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18.

[320] Corte Giust., 2 marzo 2021, C-746/18, H.K.

[321] Sul punto, volendo, CASCONE, *La Corte di Giustizia dell'Unione Europea definisce le condizioni per la legittimità delle normative nazionali in materia di acquisizione dei tabulati. Le ripercussioni sull'ordinamento italiano della sentenza del 2 marzo 2021 (c-746/18) nel caso H.K.*, in *Cass. pen.*, 2022, 2, 419 ss.

[322] Il riferimento è alle sentenze *Digital Rights Ireland* e *Ministerio Fiscal*. Vedi nota 285.

[323] Al par. 34, in particolare, la Corte ha precisato che, alla stregua di tale parametro, la conservazione e il trattamento dei dati al solo scopo di identificare l'utente (e non anche al fine di conoscere la data, l'ora, i destinatari, la durata della comunicazione e il luogo in cui la stessa è avvenuta) sono consentiti per il perseguimento dei reati in generale, non potendo simile ingerenza considerarsi grave.

emerge che per ingerenza grave intendersi quella che consente di trarre precise conclusioni sulla vita privata delle persone interessate. Trattasi dell'unico parametro che, secondo la Corte, assume rilievo nel valutare la proporzionalità della misura: la limitazione del provvedimento acquisitivo a certe categorie di dati o a periodi temporali ristretti potrebbe, infatti, incidere sulla proporzionalità del trattamento dei dati, ma tanto il fattore tempo così come quello relativo al quantitativo di dati acquisiti sarebbero, ad ogni modo, del tutto ininfluenti laddove il risultato probatorio conseguito consenta di trarre precise conclusioni sulla vita privata dei soggetti interessati[324].

È, questo, un punto di particolare interesse nella misura in cui viene, con estrema lucidità, messo a fuoco il limite al di là del quale intrusioni nella sfera privata possono giustificarsi solo in virtù della tutela di interessi di estremo rilievo – come la lotta alle forme gravi di criminalità –, individuato nella capacità, insita nell'acquisizione di certe tipologie di dati, di consentire di trarre conclusioni precise, o molto precise, sulla vita privata delle persone i cui dati sono stati conservati. In ciò la sentenza sembra cogliere perfettamente la profondità dell'incidenza delle misure di controllo dei dati prodotti dai singoli tramite l'uso delle tecnologie comunicative e informatiche sui diritti fondamentali dei soggetti interessati, emancipando la tematica dal tema, cui viene tradizionalmente ricondotta, della mera tutela del diritto alla libertà e segretezza delle comunicazioni, piuttosto che dalla mera esigenza di tutela di dati personali o sensibili e illuminando, invece, le sue profonde connessioni con il rispetto della vita privata e con l'interesse di ogni individuo a sottrarsi a forme di controllo continuativo da parte dell'autorità pubblica, indipendentemente dalla natura dei dati acquisiti.

Tanto consente alla Corte di analizzare l'ulteriore questione rimessa alla sua interpretazione, concernente l'autorità legittimata ad adottare la misura limitativa del diritto fondamentale. Perché il principio di proporzionalità possa dirsi effettivamente rispettato, è essenziale che la sussistenza dei presupposti legalmente predeterminati per l'adozione della misura sia vagliata in maniera imparziale da un'autorità indipendente e non può essere ritenuta tale l'ufficio del pubblico ministero, poiché tale organo dirige l'indagine ed esercita l'azione penale[325] e, perciò, non si connota per la sua posizione di neutralità e terzietà nei confronti delle parti del procedimento. In altre parole, il pubblico ministero è una parte pubblica antagonista alla difesa e, per questo, non può

[324] Cfr. parr. 38 e 39.
[325] Cfr. pag. 55.

essere qualificato come autorità imparziale nemmeno quando il suo *status* gli impone di agire esclusivamente alla stregua di quanto stabilito dalla legge e di tenere conto degli elementi a discarico dell'imputato e non solo di quelli a suo carico.

Come visto in precedenza, nel nostro ordinamento il pubblico ministero è stato tradizionalmente considerato legittimato anche all'adozione di atti restrittivi della libertà personale e domiciliare, visto il richiamo dell'art. 13 Cost. all'"autorità giudiziaria", che lo dovrebbe ricomprendere. Il principio espresso dalla Corte di Giustizia, dunque, assume un formidabile rilievo nella misura in cui è suscettibile di impedire che simili soluzioni normative possano essere riproposte. Ciò, se non in virtù della Carta Costituzionale, certamente in virtù dei principi sanciti dalla giurisprudenza di Lussemburgo e per tutto quanto riguarda la normativa statale adottata nell'implementazione del diritto dell'Unione.

4.1.3. (segue) La regolamentazione degli aspetti tecnici.

Passando al piano tecnico, lo stesso assume peculiare rilievo nella regolazione dell'istituto in questione non solo in relazione ad aspetti più puntuali della disciplina, di cui si dirà in seguito, ma anzitutto sul piano della necessaria delimitazione della categoria giuridica oggetto di analisi secondo le coordinate prima tracciate.

Se, come si è visto, la perquisizione e il sequestro *online* dovrebbero consentire esclusivamente la visione e acquisizione di dati già contenuti nel dispositivo informatico e non anche di quelli formati successivamente all'accesso – pena lo sconfinamento in un'attività di *surveillance* le cui caratteristiche suggeriscono la messa a punto di una distinta categoria probatoria – è evidente che perché tale limite sia effettivo bisogna agire anzitutto sul piano tecnico. Ciò implica che una disciplina normativa dell'istituto dovrebbe prevedere, in primo luogo, il necessario ricorso a *software* che consentano, al contempo, di individuare il preciso momento – vale a dire la data e l'ora – di creazione del dato informatico e di limitare la ricerca e l'eventuale acquisizione di dati a quelli preesistenti all'accesso. Naturalmente, il programma informatico utilizzato dovrebbe altresì permettere l'esperimento di una verifica successiva al termine delle operazioni in merito al loro effettivo confinamento ai dati già memorizzati nel sistema al momento dell'intrusione nello stesso; pertanto, dovrebbe essere in grado di salvare le informazioni che consentano il tracciamento delle attività effettivamente svolte e dei

dati sui quali queste sono ricadute. Al contempo, il verbale di documentazione dell'atto in tal modo realizzato dovrebbe indicare, oltre alla data e l'ora esatta dell'accesso, altresì il programma informatico utilizzato e l'avvertimento della facoltà delle difese di accedere ai dati di tracciamento dell'attività svolta. In tal modo, la difesa avrebbe l'opportunità di verificare la legittimità delle operazioni compiute e, eventualmente, azionare i rimedi legalmente previsti per l'espulsione dal fascicolo procedimentale dei dati acquisiti in violazione dei limiti sanciti.

4.2. Le garanzie antecedenti all'esecuzione della misura: presupposti applicativi e autorità competente.

Seguendo il criterio sistematico e quello di proporzione di cui si è parlato nelle pagine precedenti, il primo aspetto da prendere in considerazione ai fini dell'individuazione di precisi limiti regolatori allo svolgimento dell'attività in questione è quello relativo alla platea dei reati per l'accertamento dei quali la misura può essere disposta. All'elevata capacità intrusiva dello strumento investigativo di cui si discorre deve corrispondere un interesse statale particolarmente forte alla repressione di fatti delittuosi caratterizzati da un elevato disvalore sociale, di modo che il sacrificio dei diritti incisi dalla misura non sia superiore ai benefici derivanti dalla sua adozione[326]. Ne consegue che sarebbe del tutto irragionevole e sproporzionata una previsione normativa che consentisse l'impiego dello strumento in questione in relazione a ogni fattispecie di reato, essendo piuttosto necessario limitare il ricorso allo strumento all'accertamento di reati gravi, sulla falsariga dello schema normativo riguardante le intercettazioni di comunicazioni telefoniche o telematiche, ai sensi degli articoli 266 e 266 *bis* c.p.p. D'altronde, se è vero quanto è stato rilevato in relazione al sequestro informatico codicistico in merito al fatto che esso condivide con le intercettazioni l'attitudine ad acquisire nel procedimento enormi quantitativi di dati potenzialmente irrilevanti[327], tanto vale viepiù con riferimento alla misura di cui si discute in questa sede, ben più intrusiva anche del suo, apparente, corrispondente codicistico.

---

[326] Tale criterio, come si è visto nel par. 4.1.2., deve ritenersi operante anche in forza delle delucidazioni fornite dalla giurisprudenza europea in punto di proporzionalità della restrizione del diritto alla vita privata tutelato dalla Convenzione europea dei diritti dell'uomo e dalla Carta di Nizza.

[327] CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. e proc.*, 2009, 4, 481.

Una limitazione rigorosa del novero dei reati in relazione ai quali la misura può essere disposta avrebbe, peraltro, l'effetto di rendere più tollerabile l'introduzione di uno strumento investigativo di tale intrusività alla generalità dei consociati e, auspicabilmente, di evitare il riproporsi dell'inesauribile e risalente dibattito, non solo normativo e dottrinale ma anche – se non prima di tutto – sociale, che ha riguardato e riguarda tutt'ora la disciplina delle intercettazioni, da sempre tacciata di generare un eccessivo sacrificio delle aspettative di riservatezza dei singoli. A questo proposito, anzi, deve evidenziarsi come potrebbe apparire non sufficientemente restrittiva finanche la selezione operata dalle due norme richiamate riguardanti proprio le intercettazioni e ciò su un duplice piano. Per un verso, il limite edittale di cinque anni previsto dall'art. 266 c.p.p. non ha impedito il ricorso a dir poco massiccio allo strumento in questione, che pur dovendo astrattamente rappresentare una misura di carattere, per così dire, eccezionale, costituisce oggi la modalità investigativa largamente privilegiata nel corso delle indagini penali, non solo in dipendenza di prassi applicative eccessivamente disinvolte, ma anche in ragione del fatto che «fattori impeditivi del generalizzato impiego di tale mezzo di ricerca della prova non paiono trovare adeguato riscontro normativo»[328].

Per altro verso, una riproposizione della clausola di estensione dell'ambito applicativo delle intercettazioni telematiche ai reati «commessi mediante l'impiego di tecnologie informatiche o telematiche» non apparirebbe suscettibile di operare una rigorosa selezione delle fattispecie per le quali è ammesso il ricorso alla misura. È, infatti, perfettamente ragionevole una estensione della platea di "fattispecie abilitanti" a determinati reati che, pur non rientrando nei limiti edittali, presentano peculiarità nelle modalità di commissione dei fatti da cui conseguono ovvie difficoltà nel condurre un'indagine basata solo su mezzi di ricerca della prova tradizionali. Nondimeno, quella richiamata dall'art. 266 *bis* c.p.p. è una categoria non solo eccessivamente indeterminata ma, in ogni caso, irragionevolmente ampia.

Indeterminata in quanto dalla formulazione letterale della norma non si comprende se il richiamo è solo i reati informatici introdotti dalla l. n. 547/1993 ovvero anche ai reati

[328] DI BITONTO, *Lungo la strada per la riforma della disciplina delle intercettazioni*, in *Cass. pen*., 2009, 1, 14.

comuni ommessi con l'impiego di mezzi informatici[329]; ampia in quanto, ove anche si accogliesse la tesi più restrittiva per la quale il riferimento sarebbe solo ai reati "informatici" introdotti nel 1993, la realizzazione di indagini dal carattere così spiccatamente intrusivo non apparirebbe ragionevole con riferimento ad alcune fattispecie di disvalore sociale non così elevato e per le quali, di conseguenza, sono previsti limiti edittali piuttosto bassi (si pensi, ad esempio, alle fattispecie di cui agli artt. 615 *quater* e 615 *quinquies* c.p.p.).

Tenendo conto di quanto appena detto, nella definizione della platea di fattispecie per le quali può legittimamente disporsi il ricorso alla misura dovrebbero, anzitutto, individuarsi limiti edittali particolarmente elevati (anche, auspicabilmente, più elevati di quelli previsti dall'art. 266 c.p.p.); in secondo luogo, ove si reputasse – e sarebbe ragionevole – di estendere l'applicabilità della misura a fattispecie non rientranti nei limiti edittali in ragione delle implicazioni tecnologiche della condotta o dell'oggetto su cui la stessa ricade, ciò dovrebbe avvenire in modo da operare una selezione sufficientemente rigorosa, per esempio prevedendo, comunque, che debbano essere oltrepassati determinati limiti edittali, ancorché più bassi rispetto a quelli previsti in via generale.

Definito l'alveo dei reati per i quali è possibile disporre la misura in questione, appare evidente come il solo fatto che si proceda in relazione a tali ipotesi criminose non sia sufficiente per legittimare il ricorso alla ricerca e acquisizione occulta dei dati informatici. L'elevato rango del bene giuridico inciso dalla misura e il grado della sua compressione suggeriscono, infatti, di limitare il ricorso allo strumento al solo caso in cui emergano dagli atti procedimentali non meri sospetti di commissione del reato, ma elementi concreti che lascino desumere l'esistenza di un *fumus delicti* qualificato, parificabile, quanto meno, a quello dei gravi indizi di reato richiesto in materia di intercettazioni[330]. Tale conclusione, in realtà, si impone non solo e non tanto in ragione

[329] Si vedano, per le opposte soluzioni, CAMON, *Le intercettazioni nel processo penale*, Giuffrè, 1996, 67 e FILIPPI, *L'intercettazione di comunicazioni*, Giuffrè, 1997, 83.

[330] Il *fumus* previsto in materia di misure cautelari personali, rappresentato dai gravi indizi di colpevolezza, pare, invece, una garanzia inadeguata nel caso di specie. Non si tratta, infatti, di applicare restrizioni della libertà personale in via preventiva all'adozione di una sentenza definitiva di condanna, ma di ricercare elementi utili per le indagini in stadi poco avanzati delle stesse, nei quali, tendenzialmente, manca un quadro indiziario della solidità di quello necessario in materia cautelare. Sicché richiedere un *fumus delicti* anche soggettivamente connotato appare inopportuno in quanto confinerebbe, probabilmente, l'uso dello strumento a un numero irrisorio di procedimenti. Proprio, anzi,

dell'elevato grado di compressione dei diritti fondamentali connessi all'esecuzione della misura, ma anche per l'esigenza di contenere la tendenza di quest'ultima ad atteggiarsi alla stregua di uno strumento dalle potenzialità fortemente esplorative. La definizione, dunque, di un quadro fattuale e indiziario più preciso possibile consente di limitare la ricerca e l'acquisizione dei dati a quanto sia effettivamente rilevante per l'accertamento in corso, riducendo il rischio di vere e proprie pesche a strascico nella "vita virtuale" del titolare del sistema informatico.

È facile, infatti, immaginare che le potenzialità del mezzo di cui si discute possano indurre gli inquirenti a un accesso indiscriminato a tutti i dispositivi in uso a un determinato soggetto o, comunque, a un'acquisizione massiva di tutto quanto contenuto nel dispositivo bersaglio. In questo modo, scolorirebbe l'aspetto teleologico necessariamente connesso all'adozione di misure impattanti su diritti fondamentali, rappresentato, nel caso di specie, dalla necessità di acquisire elementi utili per l'accertamento di determinati fatti di reato e non dalla messa in opera di controlli a tappeto sulla vita dei consociati. Richiedere, invece, il raggiungimento, quanto meno, della soglia dei gravi indizi di reato, un presupposto che opera a monte dell'applicazione della misura – come quello di cui si discute – può avere effetti "virtuosi" al momento della sua esecuzione, assicurando una maggiore continenza delle operazioni e, così, la loro rispondenza al principio di proporzionalità.

Assume, dunque, in questo contesto particolare rilievo la motivazione del provvedimento autorizzativo, che dovrà altresì contenere precise indicazioni in merito al titolare del dispositivo (che ben potrebbe, dunque, essere una persona diversa da quella sottoposta alle indagini[331]), ai concreti fatti per i quali si procede, al collegamento esistente tra il dispositivo preso di mira e l'indagine in corso (dunque, alle ragioni per cui si ritiene che il sistema informatico bersaglio contenga elementi utili per l'accertamento dei fatti), alle informazioni – sia pur individuate in maniera indiretta o indeterminata – che ci si attende di rinvenire all'esito della ricerca. Solo la presenza di tali indicazioni nel provvedimento che dispone la misura consentirebbe, infatti, di assicurare lo svolgimento, *ex post*, di un controllo di concreta proporzionalità della

---

l'impossibilità di rinvenire *aliunde* le informazioni e gli elementi di prova oggetto della ricerca, necessari a consolidare il quadro investigativo, giustifica, in termini di proporzionalità, il ricorso alla misura.

[331] In questo caso, tuttavia, si dovrebbe quanto meno richiedere che il provvedimento autorizzativo motivi in ordine alle ragioni per le quali il terzo risulta collegato all'indagine in corso.

stessa quanto alla sussistenza *ex ante* dei suoi presupposti applicativi, con particolare riferimento alle esigenze probatorie da soddisfare e, ancor prima, alla pertinenza al reato di dati ricercati e acquisiti.

A quest'ultimo proposito, una soluzione suscettibile di contenere la ricerca e l'apprensione dei dati nei limiti di quanto strettamente necessario – dunque pertinente – per l'indagine potrebbe essere quella di imporre al giudice di individuare l'ambito concreto della ricerca. Vale a dire, cioè, che nel provvedimento applicativo della misura il giudice dovrebbe fornire altresì indicazioni specifiche in ordine a quale sia la tipologia di dati acquisibili e a quali parti del sistema informatico (ad esempio, determinate cartelle o determinati programmi informatici) possono essere sottoposte alla ricerca). Altro *escamotage* tecnico adoperabile per contenere la portata della ricerca e apprensione dei dati potrebbe essere quello di prevedere il ricorso a *software* che consentano di isolare documenti o cartelle informatiche sulla base di una ricerca testuale. Il giudice, quindi, sarebbe onerato di indicare, nel provvedimento autorizzativo, le parole esatte attraverso le quali deve procedersi alla ricerca.

Come si vedrà nell'ultimo capitolo, soluzioni di questo genere sono state adottate dal legislatore spagnolo nella riforma legislativa che, nel 2015, ha disciplinato le investigazioni a carattere tecnologico. Esse, tuttavia, presentano alcuni inconvenienti e la loro effettività sembra, in definitiva, dipendere eccessivamente dalle caratteristiche della singola indagine in corso[332].

Sembra, invece, decisamente da accogliere la proposta avanzata da una parte della dottrina che, in materia di intercettazioni telefoniche, ha evidenziato come sia essenziale effettuare una "funzionalizzazione della restrizione"[333] al fine di evitare che il ricorso al mezzo di ricerca della prova si trasformi in uno strumento meramente esplorativo e che il provvedimento autorizzativo si riduca a una sorta di autorizzazione in bianco[334] in forza della quale gli inquirenti non procedono alla ricerca di elementi utili all'indagine ma, piuttosto, alla sottoposizione del soggetto intercettato a un controllo indiscriminato. Al fine, invece, di non snaturare quello che è pur sempre un mezzo di ricerca della prova e che, come tale, dovrebbe essere adoperato solo laddove si reputi

[332] Si rinvia alla lettura del capitolo 5 per l'illustrazione delle problematiche rilevate in quell'ordinamento in relazione a tale disciplina. Cfr. cap. 5, par. 2.3.1.

[333] DI BITONTO, *Lungo la strada della riforma*, cit., 18.

[334] GREVI, *I requisiti delle intercettazioni e la motivazione del provvedimento autorizzativo*, in *Cass. pen.*, 2009, 9, 3348 ss.

ragionevolmente prevedibile, per il suo tramite, l'acquisizione di elementi di prova pertinenti al reato per cui si procede, si è proposto di imporre al giudice il «dovere di preconizzare in anticipo, al momento di emissione dell'autorizzazione ad intercettare, il risultato probatorio che si intende conseguire, esponendo le ragioni sulla cui base ritenere che le comunicazioni intercettate possano far raggiungere quell'obiettivo agli inquirenti»[335].

Una soluzione di questo tipo potrebbe essere utilmente implementata con riferimento alla misura in discorso. Essa non presenterebbe l'inconveniente di imporre al giudice di procedere, *ex ante*, a una delimitazione del concreto ambito di operatività della misura che potrebbe essere resa del tutto inefficace in ragione, ad esempio, della difficoltà di prevedere la sistemazione dei *files* nel dispositivo informatico prima dell'accesso; o ancora, della impossibilità di predeterminare gli spazi virtuali in cui possono rinvenirsi elementi utili all'indagine in caso questa afferisca a fattispecie di reato strutturate su condotte rispetto alle quali elementi dimostrativi potrebbero essere rinvenuti in qualsivoglia segmento dello spazio virtuale aggredito. Per contro, onerare il giudice dell'obbligo di motivare in ordine alla tipologia di informazioni che ci si attende ragionevolmente di ricavare dallo svolgimento dell'atto investigativo consentirebbe una verifica in merito al fatto che lo stesso non abbia carattere meramente esplorativo. Una verifica, dunque, che andrebbe compiuta *ex ante*, sui cui esiti non inciderebbero i risultati concretamente ottenuti né effettive o supposte criticità nell'operazione di selezione dei dati legittimamente attingibili.

Quale che sia la soluzione prescelta, anche su questo punto occorrono regole chiare, che possano guidare l'operato degli organi deputati all'adozione e all'esecuzione della misura in questione secondo protocolli ben precisi[336].

---

[335] Ancora, DI BITONTO, *Lungo la strada della riforma*, cit., 18. Sul punto, si vedano anche le riflessioni di Grevi, *I requisiti delle intercettazioni*, cit., 3348 ss., che evidenzia come soluzioni di questo tipo siano, invero, già evincibili dal sistema normativo attualmente vigente. La disciplina in materia di intercettazioni, infatti, impone al giudice che emetta il provvedimento autorizzativo di motivare non solo l'esistenza di gravi indizi di reato, ma altresì delle ragioni che rendono indispensabile l'intercettazione per la prosecuzione dell'indagine. Ciò implica che debbano essere indicate, sia pure in forma sintetica, le ragioni per cui è necessario sottoporre taluno a intercettazione e, di conseguenza, che debba essere espresso il «nesso teleologico tra le stesse intercettazioni e gli sviluppi dell'indagine in corso di svolgimento», di modo che si manifesti il collegamento tra le utenze intercettate e i fatti per cui si procede e che lo strumento in questione possa effettivamente dirsi residuale.

[336] In questo senso, come si è visto nel par. 4.1.2., sembra orientata anche la più recente giurisprudenza della Corte europea dei diritti dell'uomo (Corte e.d.u., 16 novembre 2021, app. n. 698/19, Sargava v. Estonia) e della Corte di Giustizia (Corte Giust., 2 marzo 2021, C-746/18, H.K.).

Ciò ancora non basta: perché possa dirsi davvero rispettato il principio di proporzionalità, la misura deve essere non solo idonea allo scopo che si prefigge (dunque, come si è appena concluso di dire, rilevante per l'accertamento dei fatti) ma altresì strettamente necessaria. Vale a dire, cioè, che l'autorità inquirente deve versare in una situazione nella quale l'acquisizione di quei medesimi elementi probatori ricavabili dal dispositivo informatico non sia possibile tramite il ricorso a mezzi meno intrusivi[337]. Anche su questo punto, naturalmente, dovrebbe insistere l'onere motivazionale del soggetto processuale preposto all'adozione dell'atto. Si tratterebbe, in buona sostanza, di introdurre una regola simile a quella prevista dall'art. 267, comma 1, c.p.p. in materia di intercettazione realizzata tramite captatore informatico, per la quale si prevede che il decreto che l'autorizza indichi le ragioni che rendono necessario il ricorso a tale modalità e, dunque, insufficiente l'utilizzo degli strumenti tradizionali. Nel caso di perquisizione e sequestro *online*, una simile regola potrebbe riguardare proprio i rapporti con gli istituti codicistici della perquisizione e del sequestro informatico, in modo da consentire il ricorso allo strumento occulto solo nella misura in cui i suoi corrispondenti palesi si rivelino inidonei a garantire il conseguimento del risultato. In questa maniera, peraltro, potrebbe anche evitarsi un possibile effetto, senz'altro patologico, ma facilmente pronosticabile, dell'introduzione di una disciplina normativa che facoltizzi l'accesso da remoto al dispositivo informatico, ovvero il sostanziale abbandono, da parte delle procure, del ricorso agli strumenti investigativi del sequestro e della perquisizione informatici già attualmente regolati.

Quanto all'autorità competente all'emissione del provvedimento che dispone l'esecuzione della misura, non pare possano esservi dubbi in merito alla necessità di affidare tale compito al giudice e non semplicemente al pubblico ministero, similmente a quanto accade in materia di intercettazioni[338]. Tale conclusione si impone alla luce di quanto si è detto in relazione all'esigenza di subordinare l'applicazione della misura alla verifica della sua proporzionalità, soprattutto per quanto attiene all'esistenza di gravi indizi di reato. Trattasi di una verifica che, già su un piano squisitamente logico, non può essere affidata allo stesso soggetto processuale che – in qualità di *dominus* delle

[337] Corte e.d.u., 2 dicembre 2015, app. n. 47143/06, Zacharov vs Russia. In tal modo, si assicura che le misure non siano disposte in maniera arbitraria.

[338] Ferma restando, ovviamente, l'opportunità di prevedere una disciplina specifica che, per il caso di urgenza, facoltizzi il pubblico ministero a disporre lo svolgimento dell'atto salva successiva convalida del giudice, similmente a quanto accade in materia di intercettazioni.

indagini – è deputato alla raccolta di quegli stessi elementi di prova che costituiscono la base valutativa per l'adozione del provvedimento. Ovvio, dunque, che tale vaglio non possa che essere affidato a un terzo e, segnatamente, al giudice.

Peraltro, una simile soluzione è oggi necessitata, se non alla luce della disciplina costituzionale di cui agli artt. 13 e 14 Cost., certamente in virtù degli ultimi arresti della giurisprudenza europea in relazione a un mezzo di indagine – l'acquisizione dei tabulati telefonici – che ha indubbie assonanze con quello oggetto di analisi in questa sede alla luce della potenzialità, connaturata a entrambi, di consentire l'acquisizione di un'enorme mole di dati riguardanti la vita privata dei soggetti coinvolti[339].

4.2. Le garanzie connesse all'esecuzione della misura.

La fase dell'esecuzione della misura è, tra tutte, quella nella quale gli aspetti tecnici dell'attività investigativa condotta assumono maggiore rilievo[340], in dipendenza delle caratteristiche peculiari dei *software* che consentono di realizzare l'intrusione da remoto.

Su un piano squisitamente operativo, due sono le modalità attraverso le quali potrebbe procedersi alla perquisizione e al sequestro *online*: eseguito l'accesso, gli inquirenti potrebbero effettuare la ricerca dei dati rilevanti per l'accertamento e acquisire (vale a dire, sottoporre a sequestro) solo quelli di interesse. In alternativa, potrebbero effettuare una copia clone del sistema informatico bersaglio per poi eseguire la ricerca in un momento successivo, direttamente sulla copia clone realizzata. Quest'ultima modalità avrebbe un risvolto positivo, quello di limitare nel tempo l'intrusione nel sistema informatico che, altrimenti, dovrebbe perdurare per tutto il protrarsi della ricerca dei dati necessari per l'accertamento. Non v'è dubbio, però, che un simile *modus procedendi*, violando il principio di necessaria pertinenza, risulterebbe senz'altro sproporzionato, comportando la perdita dell'esclusiva disponibilità, da parte del titolare del dispositivo, di tutti i dati nello stesso contenuti, che confluirebbero, in massa, nelle mani degli investigatori. Potrebbero, certo, immaginarsi dei correttivi, come quello di prevedere che, concluse le operazioni di selezione dei dati rilevanti, tutti gli altri siano immediatamente cancellati. Tale espediente, però, per un verso si atteggerebbe alla stregua di una soluzione *ex post* a fronte di una lesione già ampiamente perpetrata; per

[339] Il riferimento è a Corte Giust., 2 marzo 2021, C-746/18 caso H.K. Già analizzata nel par. 4.1.2.
[340] In termini, NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 148.

altro verso, non porrebbe rimedio a quello che pare essere il risvolto maggiormente preoccupante di un'acquisizione massiva dei dati, da ravvisarsi nelle ripercussioni che la stessa può avere sul convincimento dei soggetti che intervengono nella dinamica procedimentale e ne scandiscono l'andamento tramite decisioni fondate sugli elementi probatori raccolti. Ciò che si vuole evidenziare, in altre parole, è che l'acquisizione indiscriminata del contenuto di un sistema informatico può facilmente comportare l'ottenimento di dati suscettibili, se non di svelare *tout court* la personalità del suo titolare, di coglierne alcune caratteristiche e di avere uno scorcio significativo delle sue abitudini di vita. Ove anche, poi, gli elementi così raccolti, se irrilevanti, fossero eliminati, non v'è dubbio che la cognizione degli stessi potrebbe pesare sulle valutazioni affidate a quanti siano venuti a loro conoscenza – a partire dal pubblico ministero – spostando gradualmente il fulcro dell'accertamento dal fatto al suo autore. Trattasi di un rischio che non pare affatto teorico e che, anzi, sembra destinato a crescere con l'incrementarsi dell'uso delle nuove tecnologie nell'indagine penale e la conseguente possibilità di acquisizione di masse sempre maggiori di dati riguardanti il soggetto ad esse sottoposto.

Una possibile soluzione, allora, potrebbe essere quella di affidare a un soggetto diverso da quello preposto alle valutazioni in merito all'esercizio dell'azione penale il compito di selezionare il materiale necessario per l'accertamento, provvedendo immediatamente alla cancellazione del restante. Tale soluzione, però, è scarsamente compatibile con l'inquadramento dello stesso pubblico ministero nel nostro sistema alla stregua del *dominus* dell'indagine penale, sicché sarebbe quanto meno complesso giustificare, su un piano sistematico, che gli si impedisca la cognizione di elementi raccolti nel corso di un'investigazione da lui stesso condotta.

Tra le due modalità operative sopra delineate, allora, l'altra appare senz'altro preferibile. Vero è che comporta una permanenza prolungata nel sistema informatico, giustificata dalla necessità di cercare e selezionare i dati rilevanti, per poi procedere alla loro acquisizione. Nondimeno, ben potrebbe – e anzi dovrebbe – prevedersi un limite temporale per l'effettuazione di una simile ricerca. È evidente, infatti, che le caratteristiche tecniche dello strumento in questione consentirebbero, astrattamente, una intrusione nel sistema bersaglio per una durata potenzialmente illimitata. La circostanza che l'accesso avvenga in maniera occulta e in uno spazio virtuale renderebbe tutt'altro

che remoto – al contrario di quanto accade nel mondo fisico – lo scenario di un'attività di ricerca protratta per giorni o addirittura mesi e non rispondente al canone di necessaria continenza che dovrebbe guidare l'investigazione penale. È possibile, però, come detto, prevedere limiti ragionevoli di durata delle operazioni, di modo tale che lo strumento di ricerca della prova in argomento non trasmuti in un mezzo per frugare *ad libitum* nella vita privata degli individui[341].

Altro aspetto da prendere in considerazione, sempre sul piano tecnico, è la necessità di adottare *software* che consentano di assicurare, e di verificare *ex post*, che le operazioni si svolgano in modo tale da garantire la genuinità e la non alterazione dei dati. Trattasi di un'esigenza che il legislatore sembra aver presente, come dimostrato dalle molteplici previsioni, introdotte a seguito della ratifica della già più volte citata Convenzione di Budapest sul *cybercrime*, che in materia di indagini informatiche richiedono l'adozione di misure tecniche che assicurino la conservazione dei dati originali e ne impediscano l'alterazione[342]. La mancata previsione espressa di un'ipotesi di inutilizzabilità connessa al mancato impiego di misure idonee, tuttavia, ha condotto la giurisprudenza a escludere che il ricorso a tecniche non adeguate comporti l'esclusione dalla piattaforma probatoria del materiale raccolto[343], con la conclusione che la mancata adozione di tali modalità operative implica solo la necessità di valutare, in concreto, la sussistenza di eventuali alterazioni dei dati originali e la corrispondenza ad essi di quelli estratti. Trattasi di un profilo di indubbia criticità, in quanto si finisce, in tal modo, per affidare al giudice il compito di svolgere valutazioni, molto complesse sul piano tecnico, in merito alla concreta affidabilità o meno del dato. Sicché, le conclusioni raggiunte in punto di valutabilità e peso probatorio del dato raccolto vengono a dipendere dall'analisi di volta

[341] D'altronde, come visto, anche la giurisprudenza della Corte europea dei diritti dell'uomo, nelle sue pronunce sul tema, ribadisce costantemente l'esigenza di individuare un termine di durata massima delle misure impattanti sui diritti fondamentali. *Ex multis*, Corte e.d.u., 6 settembre 1978, no. 28, Klass and Others vs Germania; Corte e.d.u., 29 giugno 2006, app. n. 54934/00, Weber and Saravia vs Germania; Corte Giust., 9 giugno 2009, n. 72094/01, Kvasnica vs Slovakia.

[342] Nota, a questo proposito, NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 152-153 come, in materia di intercettazioni condotte con il captatore informatico, l'art. 89 disp. att. c.p.p. preveda l'utilizzo di programmi inseriti in apposito decreto ministeriale nonché la documentazione, nel verbale, delle attività tecniche realizzate, che devono essere conformi a quanto previsto nella medesima disposizione. L'autore osserva, tuttavia, criticamente come la norma sia sguarnita di previsioni di inutilizzabilità dei dati raccolti in sua violazione.

[343] *Ex multis*, Sez. V, 3 marzo 2017, n. 22695, in *CED Cass*., n. 270139; Sez. II, 1° luglio 2015, n. 29061, in *CED Cass*., n. 264572.

in volta condotta da un soggetto normalmente sfornito delle competenze informatiche necessarie.

Ciò suggerirebbe l'introduzione di una regola di esclusione probatoria quanto meno con riferimento alle più marchiane violazioni delle regole tecniche di esecuzione delle operazioni[344] e, sicuramente, con riferimento a tutti quei casi in cui, per la mancanza o l'intervenuta alterazione dei metadati relativi al tracciamento delle operazioni compiute, la difesa non sia in grado neppure di interloquire in merito alla correttezza delle tecniche messe in pratica dagli investigatori e alla conseguente genuinità dei dati raccolti. Non deve, infatti, dimenticarsi che il carattere occulto delle operazioni comporta l'impossibilità, per la difesa, di partecipare nel corso del loro svolgimento. Diviene, dunque, essenziale che un "riequilibrio" delle posizioni e delle garanzie difensive avvenga in una fase successiva, proprio tramite la messa a disposizione della difesa di tutti i dati e le informazioni necessarie per verificare la legittimità delle operazioni compiute e la loro correttezza sul piano tecnico.

4.4. Le garanzie successive all'esecuzione della misura: controlli, rimedi e limiti all'utilizzazione dei dati in altri procedimenti.

Alla luce di quanto appena detto, risulta evidente la centralità della disciplina relativa alle fasi successive all'esecuzione della misura, non solo al fine di consentire al soggetto che abbia subito un'invasione del suo domicilio informatico di svolgere un controllo effettivo sulla legittimità della misura adottata, ma anche al fine di ristabilire quella condizione di tendenziale parità tra le parti che l'art. 111, comma 2, Cost. individua quale essenziale presupposto del giusto processo[345].

Sarebbe, però, un errore prospettico ritenere che l'unico piano sul quale viene in rilievo la necessità di apprestare adeguati rimedi a fronte di un'acquisizione illegittima dei dati sia quello processuale: è evidente, infatti, che vi sono interessi anche extraprocessuali che appaiono meritevoli di tutela e, segnatamente, l'interesse dei terzi i cui dati siano stati acquisiti in conseguenza dell'esecuzione della misura. Trattasi di posizioni

[344] Potrebbe, a questo proposito, replicarsi la soluzione di cui all'art. 89 disp. att. c.p.p., tramite la previsione dell'adozione di decreti ministeriali che stabiliscano le modalità tecniche di svolgimento delle operazioni. La norma codicistica, dunque, potrebbe indicare specificamente le regole tecniche alla cui violazione consegue l'inutilizzabilità del risultato probatorio ottenuto.

[345] Si rinvia, sul punto, anche alle considerazioni già articolate nel par. 4.1.2. con riferimento alla posizione assunta in materia dalla giurisprudenza europea.

giuridiche delle quali una disciplina in materia che aspiri a realizzare un adeguato bilanciamento degli interessi in campo non può non tenere conto. È necessaria, però, una precisazione preliminare.

Vi è una netta ed evidente differenza tra la posizione del titolare del domicilio informatico nel quale si realizza l'intrusione e il terzo: mentre la compromissione del diritto del primo risulta del tutto indipendente dalla natura dei dati "violati" (assumendo esclusivo rilievo il fatto che si sia realizzata un'intrusione in un luogo "virtuale" dal quale ha il diritto di escludere altri e nel quale si svolge la sua vita privata), la violazione del diritto del secondo risulta strettamente connessa alla natura dei dati raccolti.

Ciò comporta che di un diritto del terzo a ottenere una restituzione dei dati o una riparazione a fronte di illegittime acquisizioni dei medesimi possa parlarsi solo nei casi in cui si dimostri che trattasi di dati sensibili. L'onere della prova dovrebbe, conseguentemente, ricadere proprio sul terzo che aspiri alla restituzione o alla riparazione, similmente a quanto accade, d'altronde, nell'ambito della disciplina dei sequestri[346], in relazione alla quale il codice di rito prevede, come noto, l'esperibilità del riesame anche a favore del terzo interessato.

In entrambi i casi – cioè sia che si tratti di rimedi predisposti in favore del soggetto (tendenzialmente, si tratterà della persona sottoposta alle indagini) che ha subito l'invasione del domicilio informatico, sia che si tratti di terzi i cui dati sono stati acquisiti in virtù dell'esecuzione della misura – risulta evidente come l'effettività del diritto a effettuare un controllo sulla legittimità delle operazioni e a esperire eventuali rimedi non può prescindere dalla conoscenza dell'atto. Il tema dei controlli e dei rimedi successivi all'applicazione della misura, dunque, è strettamente legato a quello degli oneri informativi dell'autorità procedente.

La questione è particolarmente complessa, atteso che, trattandosi di una misura il cui aspetto qualificante risiede nel carattere occulto, appare arduo ipotizzare l'esistenza di un onere, per l'autorità procedente, di informare i soggetti interessati dello svolgimento dell'atto immediatamente dopo il termine delle operazioni. Ciò potrebbe, infatti, vanificare la stessa utilità della misura e mettere a repentaglio lo svolgimento delle indagini.

[346] Cfr. artt. 257 e 322 e 324 c.p.p.

Dal canto suo, la stessa giurisprudenza della Corte europea dei diritti dell'uomo non ritiene che la notificazione agli interessati dell'esecuzione di misure occulte incidenti sulle prerogative di cui all'art. 8 della Convenzione sia condizione essenziale per la legittimità della disciplina nazionale, ma si limita a reputare auspicabile l'informativa dopo la cessazione delle misure, «appena è possibile effettuare la notificazione senza compromettere la finalità della restrizione»[347].

Un ragionevole contemperamento dei contrapposti interessi in campo potrebbe rinvenirsi nella istituzione di una regola che, in via generale, obblighi il pubblico ministero al deposito degli atti relativi all'esecuzione della misura in un termine non eccessivamente lungo – che potrebbe essere quello di cinque giorni attualmente previsto in materia di intercettazioni dall'art. 268, comma 4, c.p.p. – con conseguente onere di notificare al soggetto che ha subito l'intrusione domiciliare e ai terzi interessati i cui dati sensibili siano stati acquisiti l'avvenuto deposito dei verbali e degli atti relativi all'esecuzione della misura (ivi inclusi, naturalmente, la richiesta di autorizzazione della stessa e il provvedimento autorizzativo adottato dal giudice), con facoltà di prendere visione degli atti ed estrarne copia.

A questo punto, potrebbe ipotizzarsi una procedura che consenta agli aventi diritto di ottenere l'immediata restituzione dei dati raccolti e la loro espulsione dal fascicolo procedimentale, sulla falsariga della procedura di riesame prevista dall'art. 324 c.p.p.[348]. L'aspetto positivo di una simile previsione sarebbe, senz'altro, da rinvenirsi nella possibilità, per il soggetto le cui prerogative siano state violate dall'esecuzione della misura, di ottenere immediatamente una reintegrazione del suo diritto senza dover necessariamente attendere una declaratoria di inutilizzabilità del risultato probatorio acquisito, le cui tempistiche verrebbero a dipendere, sostanzialmente, dalla decisione del pubblico ministero di porre i dati raccolti alla base di una qualsivoglia richiesta (ad esempio, di applicazione della misura cautelare) rivolta al giudice che procede. Si è già detto[349], invece, che la comminatoria di inutilizzabilità del risultato probatorio non elide la violazione delle prerogative costituzionali violate dall'esecuzione della misura, che si

[347] Cfr. Corte e.d.u., 4 dicembre 2015, Zakharov vs Russia, app. n. 47143/06.

[348] Trattasi di una soluzione, quella che fa leva sul meccanismo del riesame, che non pare peregrina alla luce di quanto si è osservato precedentemente (cfr. par. 1.1.) circa il fatto che deve ormai reputarsi pacifico che il soggetto che subisce un sequestro di dati informatici potrebbe avere un interesse concreto e attuale alla esclusiva disponibilità dei dati stessi, il che giustificherebbe la percorribilità di un rimedio che consenta un'immediata reintegrazione nel suo diritto.

[349] Cfr. par. 3.2.

pone su un piano diverso e anteriore, e che l'utilizzo procedimentale di quel materiale ha, piuttosto, l'effetto di approfondire una lesione già perfezionata o di comportare l'insorgenza di una nuova violazione.

Se, però, la regola generale dovrebbe essere quella di una *discovery* del materiale raccolto, non v'è dubbio che essa dovrebbe subire eccezioni in tutti i casi in cui possano derivarne pregiudizi per le indagini. Per tale eventualità, naturalmente, sarebbe preferibile prevedere una procedura che imponga al pubblico ministero di chiedere al giudice l'autorizzazione a ritardare il deposito degli atti, adeguatamente motivata con l'esposizione degli elementi concreti sulla base dei quali si ritiene che una *discovery* possa pregiudicare l'esito delle investigazioni.

Naturalmente, anche a fronte di un simile atto autorizzativo, l'obbligo di integrale *discovery* dovrebbe comunque conseguire, in tutti i casi in cui la legge stessa lo preveda, all'utilizzo degli atti in questione nell'ambito del procedimento. Sicché, ad esempio, ove il pubblico ministero decidesse di utilizzare il materiale raccolto a fondamento di una richiesta di applicazione di una misura cautelare e la stessa fosse concessa, i relativi atti dovrebbero essere, secondo le regole generali, depositati integralmente nella cancelleria del giudice per le indagini preliminari[350].

Ai controlli e ai rimedi esperibili ad opera dei soggetti interessati in seguito alla conoscenza della misura dovrebbero, poi, senz'altro corrispondere precisi poteri, in capo al giudice, di esclusione dalla piattaforma probatoria dei materiali acquisiti illegittimamente. Si tratta, dunque, di integrare il "catalogo" delle inutilizzabilità probatorie inserendovi le ipotesi di violazione delle regole relative all'autorizzazione e all'esecuzione della misura, con l'avvertenza che se un utile modello a tal fine potrebbe essere rappresentato dall'art. 271 c.p.p. in tema di intercettazioni, le ipotesi di violazione cui consegue l'inutilizzabilità dovrebbero essere integrate con l'indicazione – sulla scorta di quanto si è detto nel precedente paragrafo – delle violazioni più gravi delle regole tecniche previste per l'esecuzione delle operazioni. Nell'impossibilità, in questa sede, di prevedere una precisa casistica – operazione che presupporrebbe, per

[350] Ovviamente, in tal caso, le scansioni peculiari della procedura cautelare renderebbero altamente probabile che sia il giudice della cautela a pronunciarsi per primo sull'utilizzabilità o meno di tali atti. Ciò, comunque, non dovrebbe impedire ai soggetti interessati di azionare la procedura di riesame nel termine previsto dalla legge, che dovrebbe decorrere, in via generale, dalla notifica del deposito degli atti relativi alla misura e, ove questa manchi, dal giorno della conoscenza della stessa, come avviene in caso di riesame avverso il decreto di sequestro ex art. 324 c.p.p.

l'appunto, la previa individuazione delle regole tecniche di esecuzione della misura – può evidenziarsi nondimeno come tali violazioni potrebbero essere ricondotte a due categorie: per un verso, quelle che, incidendo irrimediabilmente sulla genuinità del dato acquisito, comportino l'inaffidabilità dell'elemento probatorio e la conseguente impossibilità di basare sullo stesso qualsivoglia valutazione processuale; per altro verso, le violazioni che incidano sul diritto della difesa di essere posta nelle condizioni di verificare la conformità delle operazioni condotte alla legge (ad esempio, tramite la messa a disposizione, in forma intellegibile, dei *file* concernenti i metadati delle operazioni compiute, eventualmente anche in vista dell'affidamento a un esperto della loro analisi).

Da ultimo, fondamentale risulta l'inserimento di una regola che, similmente a quella prevista in materia di intercettazioni dall'art. 270 c.p.p., stabilisca limiti alla circolazione della prova in altri procedimenti, subordinandone l'ammissibilità a requisiti più stringenti di quelli previsti, in via generale, dall'art. 238 c.p.p. È evidente, infatti, come ricorrano, anche nel caso di specie, le ragioni che, con riferimento alla disciplina delle intercettazioni, hanno condotto all'adozione di una disciplina speciale in materia di utilizzazione in altri procedimenti, da ravvisarsi nella necessità di non vanificare in un momento successivo all'acquisizione dell'elemento probatorio tutte le garanzie operanti nel momento antecedente e, segnatamente, al momento dell'autorizzazione dell'atto.

Con riferimento al divieto previsto dall'art. 270 c.p.p., dottrina e giurisprudenza hanno ben chiarito come, essendo il provvedimento autorizzativo basato su una motivazione individualizzata – contenente la predeterminazione dei soggetti da sottoporre a controllo e dei fatti di reato per i quali in concreto si procede – occorre impedire che esso trasfiguri in una sorta di autorizzazione in bianco[351]. Trattasi di una *ratio* ben ravvisabile nel caso di specie, alla luce non solo di quanto si è detto nelle pagine precedenti circa i contenuti minimi che il provvedimento autorizzativo della perquisizione e del sequestro *online* dovrebbe avere, ma altresì dell'ingente quantitativo di dati – si badi, anche di natura comunicativa – acquisibili tramite il ricorso allo strumento in questione. Un approccio rigoroso ed effettivo alla tutela dei diritti

[351] Corte Cost. 23 luglio 1991, n. 366; Corte Cost. 24 febbraio 1994, n. 63. In dottrina, così, BALDUCCI, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Giuffrè, 2002, 174; CAMON, *Le intercettazioni nel processo penale*, cit., 275; FILIPPI, *L'intercettazione di comunicazioni*, cit., 184; GREVI, *La nuova disciplina delle intercettazioni telefoniche*, Giuffrè, 1982, 66.

fondamentali – soprattutto quando, come nel caso di specie, li si comprime in maniera tanto incisiva – impone di rendere eccezionale l'ipotesi di una spendita del materiale probatorio ottenuto in virtù di tale compressione al di fuori del contesto processuale ove essa è stata disposta.

Non può farsi a meno di notare, tuttavia, come simili preoccupazioni appaiano recessive, almeno nell'attuale momento storico, per il legislatore: lo dimostra proprio il contenuto della recente modifica dell'art. 270 c.p.p. ad opera della L. 28 febbraio 2020, n. 7 (che ha convertito con modificazioni il d.l. 30 dicembre 2019, n. 161) che, in netta controtendenza rispetto alle esigenze di innalzamento della tutela della libertà e segretezza delle comunicazioni segnalate dalla comunità scientifica ormai da anni, hanno sostanzialmente sterilizzato il divieto di circolazione delle intercettazioni di cui all'originaria formulazione della norma[352]. Trattasi di una tendenza che non può che essere stigmatizzata, soprattutto alla luce delle accresciute potenzialità di controllo che sono connaturate alle più avanzate tecnologie informatiche. Oltre a consentire una perpetrazione della restrizione del diritto fondamentale inciso dalla misura sostanzialmente *ad libitum*, una circolazione dei risultati probatori ottenuti slegata da qualsiasi limite concreto ed effettivo rischierebbe di incoraggiare, anziché disincentivare, prassi degenerative improntate alla raccolta di un numero quanto più possibile elevato di dati da sfruttare, eventualmente, anche in altri procedimenti.

---

[352] Come noto, l'originaria formulazione della norma stabiliva che «i risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza». Su tale formulazione erano intervenute, nel 2019, le Sezioni unite (Sez. un. 28 novembre 2019, n. 51, Cavallo, in *CED Cass.*, n. 277395), con l'intento di dirimere i contrasti insorti in merito alla locuzione "procedimenti diversi" adoperata nella disposizione. Con la pronuncia in questione, la Corte aveva chiarito che una medesimezza dei procedimenti – con la conseguente inoperatività dei limiti alla circolazione probatoria previsti dalla norma – poteva riscontrarsi solo in presenza di una connessione ai sensi dell'art. 12 c.p.p. A seguito della modifica del 2020, le maglie della fattispecie si sono a tal punto slargate che non pare eccessivo concludere che la stessa abbia, attualmente, un'incidenza pressoché nulla quanto alla limitazione effettiva della circolazione delle intercettazioni tra procedimenti diversi. Secondo l'attuale formulazione normativa «i risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza e dei reati di cui all'articolo 266, comma 1», sicché, in buona sostanza, le captazioni potrebbero essere utilizzate in qualsivoglia altro procedimento – pur in mancanza di connessione sul piano sostanziale tra i fatti oggetto di accertamento – purché esso abbia ad oggetto l'accertamento di fatti integranti fattispecie di reato rientranti tra quelle richiamate dall'art. 266 c.p.p. Per una posizione critica sulla novella, si veda GALLUCCIO MEZIO, *"Intercettazioni - corpo del reato" e altre insidiose suggestioni*, in *Dir. pen. e proc.*, 2021, 3, 387 ss. Si vedano anche DIDDI, *Il regime dell'utilizzabilità*, in Diddi, Filippi e Marandola, *La nuova disciplina delle intercettazioni*, Pacini Editore, 2020, 128; NATALI, *Sezioni unite e "legge Bonafede": nuove regole per l'uso trasversale delle intercettazioni*, in *Cass. pen.*, 2020, 5, 1914.

Appare, conseguentemente, imprescindibile la messa a punto di limiti rigorosi alla circolazione probatoria degli elementi di prova ottenuti, che non si sostanzino nella mera previsione della possibilità di un loro utilizzo in un altro procedimento sol che si proceda, nello stesso, per ipotesi di reato per le quali si sarebbe potuta originariamente disporre la misura.

A questo fine, può essere utile richiamare quanto si è prima evidenziato in tema di previsioni suscettibili di assicurare la necessaria proporzionalità della misura nella fase antecedente alla sua esecuzione, tramite l'individuazione del contenuto minimo del provvedimento autorizzativo che, come detto, deve lumeggiare la specifica connessione esistente tra il dispositivo oggetto di investigazione e i (gravi) fatti di reato per il cui accertamento si procede. È evidente, in altre parole, come la circolazione indiscriminata del risultato probatorio acquisito avrebbe l'effetto di vanificare del tutto una simile garanzia.

Una soluzione potrebbe, allora, essere rappresentata proprio dalla predisposizione di una regola che consenta l'utilizzo della prova in altri procedimenti (e sempre purché in questi ultimi si proceda in relazione a ipotesi di reato che avrebbero consentito *ab origine* l'applicazione della misura) solo laddove tra questi e quello di provenienza sia ravvisabile una forma di connessione. Tanto sulla scorta di quanto le stesse Sezioni unite – nella precedente sentenza *Cavallo* prima menzionata – avevano stabilito in materia di intercettazioni. Mentre, però, in quel caso la connessione aveva l'effetto di determinare la medesimezza del procedimento, con la conseguente inoperatività dei limiti previsti dall'art. 270 c.p.p., in questo caso dovrebbe rappresentare il presupposto imprescindibile per l'utilizzo della prova per l'accertamento di reati diversi da quello per il quale la misura venne autorizzata[353].

[353] Le considerazioni spese in questa sede con riferimento alla circolazione della prova tra procedimenti penali lasciano, ovviamente, impregiudicate le perduranti esigenze di una sistematizzazione adeguata della materia con riferimento al riversamento delle prove acquisite nel processo penale in procedimenti di altro tipo. Come noto, trattasi di una questione risalente in ordine alla quale la giurisprudenza appare piuttosto compatta nel ritenere la spendibilità delle prove acquisite nel procedimento penale in sede extra-penale anche al di là dei limiti previsti con riferimento a determinate prove, come accade, significativamente, in materia di intercettazioni (cfr. Sez. un. civ., 12 giugno 2017, n. 14552, con riferimento ai procedimenti disciplinari a carico di magistrati; Sez. V, 7 febbraio 2013, n. 2916, con riguardo ai procedimenti tributari; CNF, 18 giugno 2020, n. 69, con riferimento al procedimento disciplinare forense). Tanto, peraltro, non senza le critiche di attenta dottrina, che evidenzia come, in tal modo, si finisca per aggirare i limiti previsti dall'art. 15 Cost. nonostante l'assenza di una specifica disciplina in materia nell'ambito dei procedimenti in cui i risultati delle intercettazioni vengono riversate. Sul punto, si vedano le considerazioni critiche di NAPPI, *Sull'utilizzazione extrapenale dei risultati delle*

Capitolo IV

ONLINE SURVEILLANCE FRA SCENARI ATTUALI E FUTURIBILI

Sommario: 1. Lineamenti generali dell'*online surveillance*; 2. La non riconducibilità dell'*online surveillance* all'intercettazione di flussi disciplinata nell'art. 266 *bis* c.p.p.; 3. L'intercettazione, l'acquisizione di *e-mail* dalla casella di posta elettronica e di altre forme di messaggistica; 4. La localizzazione *online*; 5. L'acquisizione di video-riprese; 6. Il *key logging* e le altre attività di controllo del dispositivo informatico; 7. Il possibile ricorso a un'attività indiscriminata di sorveglianza: impatto sulle prerogative costituzionali e conseguenze processuali; 8. L'*online surveillance* come categoria probatoria: una proposta *de iure condendo*; 9. Le garanzie antecedenti, contestuali e successive all'esecuzione della misura.

1. Lineamenti generali dell'*online surveillance*.

Se nel capitolo antecedente ci si è soffermati sugli strumenti di indagine tecnologica che permettono l'acquisizione da remoto e in maniera occulta di dati immagazzinati in un dispositivo informatico e preesistenti all'accesso al dispositivo medesimo (*online search*), scopo del presente capitolo è condurre uno studio sulle attività investigative condotte sempre da remoto e occultamente, ma finalizzate alla sottoposizione del dispositivo bersaglio a una vera e propria sorveglianza continuativa, con acquisizione, oltre che – eventualmente – di dati già salvati nella memoria dello strumento informatico, anche di dati e informazioni futuri.

Come si è avuto modo di osservare, l'opportunità di distinguere le due attività, tanto in un'ottica *de iure condito* che in un'ottica *de iure condendo*, si spiega già sotto un punto di vista puramente intuitivo con la ontologica differenza esistente tra una intrusione avente carattere "istantaneo" – sia pur invasiva in quanto suscettibile di condurre

---

intercettazioni, in *Cass. pen.*, 2014, 1, 388 ss., basate sul condivisibile presupposto che «i limiti imposti dall'art. 270 c.p.p. non sono destinati a tutelare l'imputato nella formazione della prova, ma a garantire la libertà e segretezza delle comunicazioni di persone anche estranee al procedimento penale. E questo diritto è comunque inviolabile, quale che sia la natura del procedimento nel quale i risultati delle intercettazioni vengono utilizzati […] L'esigenza di precludere la divulgazione del contenuto di comunicazioni telefoniche non pertinenti attiene alla garanzia anche extraprocessuale di qualsiasi persona».

all'acquisizione di un numero elevatissimo di dati e informazioni – e una avente carattere continuativo[354].

Ci si riferisce, dunque, in questa sede all'utilizzo di quegli strumenti informatici[355] che consentono di captare in tempo reale e per un arco temporale più o meno esteso il flusso informatico intercorrente tra il micro-processore e le periferiche dello strumento digitale oggetto dell'attività investigativa, così realizzando un monitoraggio costante di tutto quanto viene realizzato sopra o attraverso lo stesso[356]. Trattasi, dunque, di tipologie investigative non riducibili ai classici concetti di perquisizione, ispezione o sequestro non solo in ragione del carattere occulto dell'attività svolta, ma anche perché questi ultimi «devono concludersi nel tempo strettamente necessario a verificare la presenza o l'assenza della fonte di prova nel luogo o sulla persona indicata nel decreto autorizzativo, ed eventualmente ad apprenderla. Non può così rientrare nel concetto di perquisizione l'introduzione e la permanenza a oltranza di un programma spia all'interno di un computer dell'indagato, al fine di copiare e sequestrare indistintamente tutti i file e i dati elaborati in un arco di tempo indefinito»[357].

Le potenzialità operative dello strumento informatico in questione con riferimento all'apprensione di dati in tempo reale sono state ben descritte nella pronuncia delle Sezioni unite della Corte di cassazione resa nel caso *Scurato*[358], avente ad oggetto, come visto precedentemente[359], la questione relativa all'impiego del captatore per la realizzazione delle intercettazioni tra presenti. In quell'occasione la Corte, pur non soffermandosi sugli impieghi del captatore ulteriori rispetto a quello precipuamente oggetto di analisi, ne mise in luce le potenzialità, evidenziando la possibilità, tramite il ricorso allo strumento in questione, «di captare tutto il traffico dati in arrivo o in

---

[354] Cfr., sul punto, le considerazioni già articolate nel par. 2.1. del cap. 1. Per tutti, sulla maggiore invasività di un'attività di sorveglianza avente carattere continuativo, NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Un tentativo di sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Cedam, 2020, 90 ss.

[355] Come si è visto nel capitolo 1, allo stato della tecnica lo strumento tecnologico in questione è quello noto come captatore informatico, ma le considerazioni che seguono sono perfettamente spendibili in ordine a qualsiasi altro ritrovato tecnologico che consenta lo svolgimento di attività investigative del tipo di quelle descritte di seguito.

[356] Per ulteriori riferimenti bibliografici rinvia al cap. 1, par. 2.1.

[357] TROGU, *Intrusioni segrete nel domicilio informatico*, in AA.VV., *Le indagini atipiche*, a cura di Scalfati, Giappichelli, 2019, 577.

[358] Sez. un., 28 aprile 2016, n. 26889, Scurato, in *Arch. nuova proc. pen.*, 2017, 76 e ss. con nota di CAMON, *Cavalli di troia in Cassazione* e in *Cass. pen*. 2016, 2274, con nota di BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*.

[359] Cfr. par. 2, cap. 1.

partenza dal dispositivo "infettato" (navigazione e posta elettronica, sia *web mail*, che *out look*); di attivare il microfono e, dunque, di apprendere per tale via i colloqui che si svolgono nello spazio che circonda il soggetto che ha la disponibilità materiale del dispositivo, ovunque egli si trovi; di mettere in funzione la *web* camera, permettendo di carpire le immagini; di perquisire l'*hard disk* e di fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira; di decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (*screenshot*); di sfuggire agli antivirus in commercio. I dati raccolti sono trasmessi, per mezzo della rete *internet*, in tempo reale o a intervalli prestabiliti ad altro sistema informatico in uso agli investigatori».

La mancanza di una normativa specifica sul punto impone di analizzare distintamente le singole attività realizzabili con tali strumenti tecnologici al fine di verificarne la riconducibilità alle categorie legali esistenti[360]. Come già si è già anticipato nel primo capitolo[361], infatti, l'analisi delle singole attività realizzabili con tale strumento appare, *de iure condito*, l'unica via percorribile per ricostruire il trattamento processuale dei risultati di simili attività investigative[362]. Per questa ragione si procederà, nelle pagine a seguire, nel senso appena delineato. Ciò equivale a porsi, almeno momentaneamente, nell'ottica di quanti – seguendo l'esempio delle Sezioni unite appena citate – hanno sostenuto la teoria della cd. "neutralità dello strumento tecnologico", a indicare il principio per il quale l'applicabilità o meno di una data disciplina in materia di protezione dati personali non dovrebbe dipendere dalle caratteristiche tecniche della tecnologia utilizzata, sulla scorta dell'osservazione secondo la quale «il rispetto della doppia riserva di legge e di giurisdizione richiesta dalla Costituzione per ogni tipo di intrusione nelle libertà fondamentali poste a tutela del domicilio privato e delle comunicazioni non si estende – nel quadro normativo vigente – anche alla necessità di avere una specifica previsione legislativa per ogni tipologia di strumento captativo utilizzabile»[363].

---

[360] FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma,* in *Proc. pen. e giust.*, 2016, 5, 124.

[361] Cfr, par. 3.2.

[362] Cfr. TORRE, *Il captatore informatico tra riforma Orlando e sistema processuale,* in *Giur. ita*., 2018, 7, 1774 ss.

[363] Ad esempio, LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *Dir. pen. cont.,* 7 ottobre 2016, 11 ss.

Alla base di una simile ricostruzione sta la comprensibile preoccupazione che una normativa eccessivamente dettagliata anche sul piano tecnico, tarata sulle specifiche caratteristiche operative del singolo strumento tecnologico, si esponga inesorabilmente al rischio di una rapida obsolescenza. Se ciò è vero, però, occorre tenere presente che proprio le caratteristiche tecniche dei nuovi ritrovati tecnologici sono suscettibili di incidere sull'inquadramento delle attività che consentono di realizzare non solo in senso qualitativo ma anche quantitativo[364] e ciò è esattamente quanto accade nel caso di specie. La "scomposizione" – sia pur a fini meramente classificatori – delle specifiche attività astrattamente riconducibili alla categoria dell'*online surveillance* va incontro alla facile obiezione per la quale la realizzazione congiunta delle attività di controllo del dispositivo sopra delineate è non solo quanto è destinato ad affermarsi nella prassi in ragione dell'ovvio potenziale investigativo dello strumento, ma altresì un'evenienza suscettibile di mutare in termini qualitativi la tipologia di controllo realizzato, incidendo, altresì, sul bene giuridico inciso dal ricorso alla misura[365]. Detto altrimenti, è evidente come di vera e propria "neutralità" dello strumento non possa parlarsi laddove le attività di controllo e acquisizione dei dati astrattamente realizzabili siano combinate, con la conseguente realizzazione di una vera e propria attività di sorveglianza "a tappeto" dell'utilizzatore del sistema informatico e l'esponenziale incremento della intensità della lesione dei diritti fondamentali di quest'ultimo.

Ne consegue, come si vedrà, che in un'ottica *de iure condendo* la creazione di un'unica categoria giuridica suscettibile di ricomprendere l'insieme delle attività di *surveillance* astrattamente esercitabili appare l'opzione più adeguata, anche al fine di mettere a punto una normativa improntata a livelli di tutela proporzionati all'incremento della intensità della lesione delle prerogative costituzionali incise[366].

---

[364] Cfr. cap. 1, par. 2 ss.

[365] Cfr., sul punto, il par. 8. Si vedano anche le considerazioni di CAPRIOLI, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, in AA.VV., *Dimensione tecnologica e prova penale*, Giappichelli, a cura di Luparia, Marafioti e Paolozzi, 2019, 51, che evidenzia come l'operazione di scomposizione delle singole attività realizzabili con il captatore informatico al fine di verificarne la riconducibilità alle categorie esistenti rischi di porsi in contrasto con il principio di legalità processuale. Ne deriva, secondo l'autore, che i nuovi strumenti tecnologici, nella misura in cui siano suscettibili di comportare nuove compressioni dei diritti costituzionalmente tutelati, richiedono la messa a punto di nuove garanzie. Tanto, peraltro, senza considerare come una classificazione separata delle singole attività appaia inadeguata anche in ragione del fatto che alcune di esse non risultano nettamente riconducibili all'una o all'altra categoria ma hanno carattere, in qualche misura, ibrido. Sul punto, PARLATO, *Problemi insoluti: le perquisizioni on-line*, in AA.VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra e Orlandi, Giappichelli, 2018, 308 ss.

[366] Cfr. par. 8.

2. La non riconducibilità dell'*online surveillance* all'intercettazione di flussi disciplinata nell'art. 266 *bis* c.p.p.

Prima di passare all'analisi delle singole attività realizzabili per il tramite del ricorso al captatore informatico, pare opportuno sgomberare il campo da un equivoco. Il riferimento è alla possibilità di ricorrere all'istituto di cui all'art. 266 *bis* c.p.p. per l'inquadramento delle attività di acquisizione dei dati informatici in forma occulta e in tempo reale.

Come si è già avuto modo di anticipare nel terzo capitolo[367], una simile soluzione parrebbe consentita dalla formulazione piuttosto ampia della norma in discorso, che fa riferimento a «l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi». Si è visto, sempre in quella sede, che tanto ha condotto parte della giurisprudenza a interpretare la disposizione nel senso che per il suo tramite si consentisse l'acquisizione di qualsivoglia dato (o meglio, *bit*) "in transito" su un sistema informatico, indipendentemente dal fatto che lo stesso si inserisca nell'ambito di un'attività di comunicazione in senso stretto tra due o più soggetti che fanno uso del sistema – o dei sistemi – telematici o informatici[368].

È evidente come l'accoglimento di una simile tesi, di fatto, condurrebbe alla conclusione della riconducibilità, *de iure condito*, di qualsiasi attività di *surveillance* avente di mira l'acquisizione di dati in corso di formazione sul dispositivo informatico all'intercettazione telematica di cui all'art. 266 *bis* c.p.p.

Tale soluzione, suscettibile di aprire la strada a un'indiscriminata attività di vigilanza occulta del soggetto sottoposto alle indagini impattante sulle sue prerogative costituzionali, è stata, peraltro, recentemente avallata dalla Corte di cassazione in una pronuncia[369] relativa a un ricorso per violazione di norma processuale, ai sensi dell'art. 606, lett. c), c.p.p., in relazione all'estrazione tramite *screenshot* di un *file excel* dal *personal computer* dell'imputato tramite il captatore informatico. La Corte, nel caso di specie, ha reputato l'attività in questione perfettamente legittima, estendendo, di fatto, le

[367] Cfr. cap. 3, par. 1.2.

[368] Sez. un., 13 luglio 1998, n. 21, Gallieri, in *Foro it.*, 1999, 2, 87; Sez. IV, 28 giugno 2016, n. 40903, Grassi, in *CED Cass*. n. 268228.

[369] Trattasi di Sez. I, 7 ottobre 2021, n. 3591, Romeo, in *CED. Cass.*, n. 282495. In termini critici, PROCACCINO, *Piccoli equivoci senza importanza: tra intercettazioni di flussi telematici, perquisizioni e prove atipiche*, in *Cass. pen.*, 2022, 9, 3120 ss.

sue considerazioni a qualsiasi attività di "mera constatazione" da remoto di dati informatici in corso di formazione che, «pur non costituendo una "comunicazione" in senso stretto, costituisce certamente, invece, un comportamento cd. comunicativo, del quale è ammessa la captazione – previo provvedimento autorizzativo dell'AG - nonché la videoregistrazione, dunque anche la fotografia, nel caso di specie mediante screen shot della schermata». Trattasi di un'impostazione che non può essere condivisa e che rappresenta il mero *escamotage* per aggirare il patente vuoto normativo che si riscontra nella materia.

Che l'art. 266 *bis* c.p.p. possa essere interpretato nel senso che esso legittimi qualsivoglia acquisizione di dati informatici da remoto pur in mancanza di una comunicazione tra due o più soggetti è cosa di cui è lecito dubitare per vari ordini di ragioni.

È noto che uno dei nodi interpretativi tradizionalmente riguardanti la definizione la disciplina delle intercettazioni è quello relazionato alla necessità di definire cosa rientri e cosa non rientri nel concetto di comunicazione. In mancanza di una definizione legale, la giurisprudenza di legittimità è orientata nel senso dell'accoglimento di un'interpretazione piuttosto ampia, per la quale può definirsi comunicazione pressoché qualsiasi forma di trasmissione, da un soggetto a un altro soggetto, del contenuto di un pensiero tramite l'uso della parola o mediante altri atteggiamenti idonei a manifestarlo[370]. Si tratta, come si vede, di un concetto piuttosto elastico, in cui sono suscettibili di rientrare molteplici estrinsecazioni del modo di ciascun individuo di relazionarsi con altri soggetti. Quanto, però, è certo, è che caratteristica strutturale del concetto di "comunicazione" sia quella della sua natura relazionale, vale a dire che non v'è comunicazione – comunque la si voglia intendere – senza un atto volontario di trasmissione di un pensiero tra soggetti. Non v'è dubbio, peraltro, che proprio questo tipo di condotta sia quella a cui l'art. 15 Cost. accorda tutela, escludendo che la pubblica autorità possa intromettersi – se non con le garanzie previste dalla legge e per effetto di un atto motivato dell'autorità giudiziaria – nelle comunicazioni riservate tra individui.

La lettura giurisprudenziale cui si è fatto riferimento antecedentemente pretenderebbe di ampliare il concetto di comunicazione fino a farvi rientrare quanto dovrebbe restarne

[370] Così la giurisprudenza di legittimità consolidata. Si vedano, *ex multis*, Sez. III, 7 luglio 2010, n. 37197, in *CED Cass.*, n. 248563; Sez. V, 17 novembre 2015, n. 11419, in *Cass. pen.*, 2017, 2, 717; Sez. III, 21 novembre 2019, n. 15206, in *CED Cass.*, n. 279067.

ontologicamente escluso, vale a dire la captazione di flussi di dati interni al circuito informatico aggredito che non sono espressione di alcuna forma di trasmissione del pensiero tra soggetti ma del normale funzionamento di qualunque sistema digitale che si basi sulla circolazione di impulsi elettro-magnetici noti come *bit*. Proprio per questo, è senz'altro condivisibile quell'orientamento giurisprudenziale che, con riguardo al tentativo esegetico di slabbrare oltre il suo confine naturale il concetto di intercettazione, ha ribadito che «per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro […] non potendo ritenersi sufficiente l'elaborazione del pensiero e l'esternazione, anziché mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura ed in tal modo memorizzato», trovandosi altrimenti al cospetto «non [di] un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma […] [di] "un flusso unidirezionale di dati" confinato all'interno dei circuiti del personal computer»[371].

A sostegno di una simile conclusione militano sia elementi letterali che sistematici. Anzitutto, per quanto l'art. 266 *bis* c.p.p. si riferisca, ambiguamente, al "flusso" interno al sistema informatico o intercorrente tra più sistemi, non offre alcun tipo di spunto per ritenere che del termine "comunicativo" adoperato nella disposizione possa essere offerta una lettura tanto discordante da quella invalsa, da decenni, in tema di intercettazioni. D'altro canto, la stessa disposizione, sia nella rubrica che nel testo, richiama il concetto di intercettazione, al quale è connaturata, secondo un granitico e ancora attuale indirizzo giurisprudenziale, oltre che l'esistenza di una comunicazione nel senso appena descritto, anche la caratteristica della terzietà dell'intercettante rispetto ai comunicanti. Né può ritenersi che i comunicanti, nel caso di specie, siano i terminali elettrici su cui viaggiano i *bit* o, addirittura, l'utilizzatore del sistema informatico e il sistema medesimo. Sul piano sistematico, la soluzione ermeneutica in commento condurrebbe a un singolare scollamento tra l'attività di intercettazione e la prerogativa costituzionale alla quale essa è stata, da sempre, collegata e dalla quale promana, ovvero quella di cui all'art. 15 Cost. Tale norma tutela le comunicazioni tra persone, non tra terminali elettronici di un dispositivo informatico.

[371] Sez. V, 14 ottobre 2009, n. 16556, Virruso, in *CED Cass.*, n. 246954.

Tanto, peraltro, senza tralasciare gli esiti aberranti dell'assetto che deriverebbe dall'accoglimento di una simile ricostruzione, cioè il vero e proprio sdoganamento di qualsivoglia attività di vigilanza occulta e da remoto su dispositivi informatici, rispetto alla quale la mera disciplina delle intercettazioni sembra del tutto sproporzionata per difetto.

È evidente, dunque, che la disposizione deve, più pianamente, essere interpretata nel senso che il suo ambito applicativo riguardi non già qualsivoglia "flusso comunicativo di *bit*" – lettura che, peraltro, avrebbe scarso o nullo significato dal punto di informatico – quanto, piuttosto, una comunicazione, pur sempre tra più soggetti, che però si svolge non in forma analogica, come accade nel caso di una "tradizionale" chiamata telefonica, ma tramite una tecnologia che sfrutta impulsi elettrici non percepibili immediatamente e che devono essere, dunque, decodificati[372].

3. L'intercettazione, l'acquisizione di *e-mail* dalla casella di posta elettronica e di altre forme di messaggistica.

Una delle attività di *online surveillance* realizzabili tramite l'utilizzo del captatore informatico è quella consistente nell'acquisizione dei contenuti comunicativi delle conversazioni intrattenute dall'utilizzatore del dispositivo infettato. Tale attività, suscettibile di incidere – quanto meno – sulla prerogativa costituzionale di cui all'art. 15 Cost., può concretamente realizzarsi attraverso varie modalità, delle quali non tutte sono apparse riconducibili al concetto di intercettazione precisato dalla giurisprudenza di legittimità[373] nel senso di una captazione occulta, contestuale e ad opera di un terzo di una comunicazione o conversazione riservata tra più soggetti. Mentre, infatti, appare del

[372] DI BITONTO, *La captazione di flussi telematici*, in AA.VV., *L'intercettazione di comunicazioni*, a cura di Bene, Cacucci Editori, 2018, 86. Nel senso che, per il resto, l'intercettazione telematica o informatica conserva tutte le altre caratteristiche strutturali di un'intercettazione tradizionale, CUOMO, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, a cura di Lupària, Cedam, 2022, 656, il quale evidenzia che «le operazioni, come accade per ogni tipologia di intercettazione, devono presentare le caratteristiche della terzietà di colui che capta il flusso delle informazioni e il carattere riservato della comunicazione, senza impedirne la prosecuzione e senza che gli interlocutori siano a conoscenza dell'attivazione del servizio […] La comunicazione informatica tra due o più soggetti può avvenire tramite il tradizionale scambio di messaggi di posta elettronica o per mezzo delle più svariate applicazioni che consentono l'interazione tra gli interlocutori in tempo reale o differito (servizi di messaggistica o chat)». Deve segnalarsi, però, come lo stesso autore sembri parzialmente contraddirsi laddove, a pag. 661, afferma che «possono essere oggetto di intercettazione anche gli scambi di dati intercorrenti tra un elaboratore e le sue periferiche, che ricevono dati digitali per essere elaborati sotto forma di scritti, immagini o suoni».

[373] Sez. un., 28 maggio 2003, n. 6747, Torcasio, in *CED Cass.*, n. 225465-468.

tutto pacifico che integri un'attività di intercettazione[374] – nella specie, di intercettazione ambientale – la captazione di dialoghi avvenuti nei pressi del sistema informatico bersaglio per mezzo dell'attivazione del microfono, diversi dubbi interpretativi sono sorti con riguardo alle altre tipologie di intrusioni realizzabili. Il riferimento è, in particolar modo, all'acquisizione delle *e-mail* contenute nella casella di posta elettronica e delle conversazioni salvate in altri strumenti di messaggistica in dotazione alla pressoché totalità dei dispositivi informatici di uso comune. La riconducibilità di tali attività investigative alle categorie codicistiche già esistenti è questione tutt'altro che definitivamente risolta, in ordine alla quale diverse oscillazioni si sono registrate non solo in dottrina, ma altresì in giurisprudenza. Il nodo interpretativo attiene, in particolare, all'istituto al quale simili attività andrebbero ricondotte, non essendo chiaro se si tratti di una attività di intercettazione (eventualmente telematica, ai sensi dell'art. 266 *bis* c.p.p.), di un sequestro di corrispondenza ai sensi dell'art. 254 *bis* c.p.p. o, piuttosto, di un sequestro "tradizionale"[375]. Tali difficoltà di inquadramento dipendono, in buona misura, dalle caratteristiche tecniche e operative dei programmi di messaggistica e di scambio di *e-mail* diffusi tra gli utenti.

A differenza di quanto accade in un'intercettazione tradizionale – nella quale l'intrusione nella conversazione riservata e la sua captazione non possono che essere contestuali alla stessa – l'apprensione del contenuto della comunicazione via *e-mail* o attraverso altri applicativi di messaggistica può avvenire in diversi stadi della trasmissione del messaggio: è possibile, così, che l'accesso nel sistema informatico con acquisizione delle conversazioni in chiaro intervenute tra il titolare del dispositivo e un terzo si realizzi non contestualmente alla sua verificazione, ma in un momento successivo, in cui i messaggi di posta elettronica o di altro tipo sono già stati spediti e sono pervenuti nel sistema del destinatario, ivi rimanendo conservati negli appositi spazi di memoria degli applicativi utilizzati. In questo secondo caso, il concetto di intercettazione, per come delineato dalla giurisprudenza di legittimità, appare non

[374] Come si è già spiegato nel cap. 1, tale specifico impiego del captatore non è oggetto di approfondimento in questa sede data l'esistenza di una disciplina specifica sul punto.

[375] Si veda, ad esempio, BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* in *Riv. it. scienze giur*., 2017, 8, 348, che segnala come sia «difficile stabilire la riconducibilità a fattispecie di attività normativamente tipizzate: emblematico è l'ipotesi della captazione delle e-mail già inviate o ricevute, non riconducibili al classico concetto di intercettazione per l'assenza del requisito della contestualità tra comunicazioni e atto acquisitivo, delle mail mai spedite ma parcheggiate nella cartella 'bozze', per le quali, in mancanza di un invio, è ancora più difficile individuare una "comunicazione"».

adeguato a ricomprendere il fenomeno in ragione della mancanza del carattere di contestualità della captazione.

Altro delicato problema di inquadramento si è posto, come si vedrà tra un momento, con riferimento alla questione relativa alle *e-mail* conservate nella casella "bozze" del sistema di posta elettronica utilizzato dall'utente alla luce del ricorso, ad opera dei membri di alcune associazioni per delinquere, a *escamotages* finalizzati proprio a eludere eventuali attività di intercettazione, tra i quali quello di comunicare esclusivamente tramite la creazione di bozze di *e-mail* in uno stesso *account* di posta elettronica cui tutti i membri dell'associazione hanno accesso. In un simile caso, è altresì il mancato inoltro del messaggio a determinare le anzidette difficoltà di inquadramento[376], essendosi registrato in giurisprudenza il dubbio se una simile attività sia assimilabile al concetto comunicazione – con la conseguente, possibile applicabilità della disciplina delle intercettazioni – o meno.

Anticipando le conclusioni cui si addiverrà terminata la trattazione di questo tema, pare il caso di segnalare fin da subito che simili dubbi interpretativi sembrano dipendere non solo da questioni – come quelle appena segnalate – di carattere squisitamente tecnico, ma anche dalla percezione diffusa che l'applicazione delle classificazioni giurisprudenziali e dottrinali in tema di intercettazione alle nuove forme di messaggistica sia insoddisfacente dal punto di vista della tutela dei diritti fondamentali e, in qualche misura, arbitraria. Detto altrimenti, non è semplice, se si ragiona sul piano delle garanzie, comprendere per quale ragione all'apprensione ripetuta dei contenuti delle *chat* presenti sul sistema informatico tramite il monitoraggio costante del dispositivo e la periodica acquisizione delle conversazioni debba corrispondere un regime giuridico improntato a rigore inferiore rispetto a quello che sarebbe applicabile nel caso di captazione in tempo reale del flusso comunicativo. È evidente, infatti, come il grado di lesione della libertà e segretezza delle comunicazioni ad opera di simili misure appare quanto meno paragonabile, sicché una diversa modulazione delle garanzie applicabili operata sulla base della distinzione tra captazioni contestuali e non contestuali, se appariva ragionevole con riferimento alle tradizionali tecniche di esecuzione delle intercettazioni, sembra conservare scarso significato dinanzi a tecnologie che permettono in via sistematica il recupero delle conversazioni pregresse.

[376] Per entrambe le questioni, si veda, *ex multis*, PARLATO, *Problemi insoluti: le perquisizioni on-line*, cit., 308 ss.

Proprio tale consapevolezza pare sottesa a una pronuncia del 2016[377] della quarta sezione penale della Suprema Corte, che ha ricondotto l'acquisizione di messaggi di posta elettronica già ricevuti o spediti e conservati nelle rispettive caselle di posta in entrata e in uscita, indipendentemente dal sistema intrusivo adottato dagli inquirenti – accesso diretto al computer o inserimento di un programma spia –, a un'attività di intercettazione telematica, con la conseguente operatività delle garanzie di cui agli artt. 266 *bis* c.p.p. In particolare, secondo la pronuncia, il criterio in base al quale occorre distinguere l'intercettazione dal sequestro della posta elettronica non è quello dell'attualità della comunicazione rispetto all'atto acquisitivo. Tale soluzione, infatti, farebbe residuare alcuni dubbi interpretativi a fronte di situazioni ricorrenti come quella del ritardo nella consegna del messaggio dal *server* del mittente a quello del destinatario. Alla luce di ciò, il discrimine tra la disciplina delle intercettazioni e quella del sequestro sarebbe rinvenibile nell'avvenuto inoltro dell'*e-mail* da parte del mittente. Si tratta di una soluzione ermeneutica che – ponendosi, sia pure con argomenti in parte contraddittori[378], in netta controtendenza rispetto all'orientamento assolutamente dominante in materia di intercettazioni – lascia trapelare le difficoltà connesse al ricorso ai paradigmi e alle classificazioni – spesso improntate a criteri eccessivamente restrittivi – invalse nella giurisprudenza di legittimità a fronte di fenomeni nuovi.

Quanto, invece, ai messaggi di posta elettronica non inviati dall'utente, ma salvati nella cartella bozze del proprio *account* o in appositi spazi virtuali (ad esempio Dropbox o Google Drive), essi, secondo la Corte, costituirebbero dei semplici documenti informatici ai sensi dell'art. 234 c.p.p.

Tali conclusioni sono state in buona parte ribaltate da pronunce più recenti[379] che, aderendo all'orientamento inaugurato dalle Sezioni unite *Torcasio* in tema di definizione del concetto di intercettazione, hanno optato per la natura documentale, ai

[377] Sez. IV, 28 giugno 2016, n. 40903, Grassi, cit.

[378] Nelle pagine successive della pronuncia è la stessa Corte, infatti, a escludere che le *e-mail* già spedite e ricevute, che pure sarebbero inquadrabili alla stregua di un "flusso informatico o telematico", rientrino nel concetto di corrispondenza, precisando altresì che la stessa conclusione si imporrebbe con riferimento ai «messaggi WhatsApp ed SMS rinvenuti in un telefono cellulare sottoposto a sequestro, in quanto questi testi, non costituendo il diretto obiettivo del vincolo, non rientrano neppure nel concetto di "corrispondenza", la cui nozione implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito».

[379] Si veda Sez. III, 16 aprile 2019, n. 29426, in *Guida dir*., 2019, 38, 102. Conformi, Sez. V, 21 novembre 2017, n. 1822, in *Guida dir.*, 2018, 15, 96 e Sez. VI, 6 febbraio 2020, n. 12975, in *Cass. pen.*, 2020, 12, 4664.

sensi dell'art. 234 c.p.p.[380], dei dati informatici di carattere comunicativo archiviati sulla memoria del dispositivo informatico (quali *e-mail*, sms e messaggi *whatsapp*). Tanto con la conseguenza che tali dati, reputati estranei al concetto di "corrispondenza", ben potrebbero essere acquisiti attraverso lo strumento del sequestro[381], senza necessità di adottare la disciplina stabilita dall'art. 254 c.p.p. Diverso ragionamento dovrebbe farsi, invece, per la vera intercettazione di *e-mail* o altri messaggi similari[382], la quale si caratterizza per la contestualità tra la captazione dei messaggi e la loro trasmissione[383] e, quindi, ha ad oggetto un flusso comunicativo in atto che giustifica l'applicazione del regime di intercettazione telematica.

Come già anticipato, una simile ricostruzione, se appare maggiormente coerente con i criteri ermeneutici da tempo dettati dalla Corte di cassazione in materia di intercettazione, è suscettibile, soprattutto se trasposta nel campo delle investigazioni occulte da remoto, di lasciare scoperti i nervi delle garanzie dei titolari dei sistemi informatici bersaglio. Si è vero, infatti, che gli ultimi ritrovati tecnologici consentono di sottoporre il dispositivo *target* a una sorveglianza perdurante, è facilmente immaginabile che gli inquirenti, anziché avviare le lunghe e complesse procedure necessarie per l'esecuzione dell'attività di intercettazione telematica, si limitino a monitorare il sistema informatico di riferimento scaricando, man mano, le conversazioni che avvengono tramite lo stesso. Tanto senza considerare come, con riferimento ai sistemi di messaggistica istantanea (come *whatsapp, Telegram* etc.), questo sistema consenta altresì di aggirare con estrema facilità l'ostacolo rappresentato dalla criptatura delle comunicazioni ad opera dei *providers* del servizio.

---

[380] Medesima soluzione, in dottrina, per CERQUA, *Tra comunicazioni telematiche e rito, il sequestro della corrispondenza elettronica*, in *Dimensione tecnologica e prova penale*, Giappichelli, 2019, 97 ss.

[381] Per questa soluzione in dottrina, KOSTORIS, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in AA.VV., *Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, a cura di Ruggieri e Picotti, Giappichelli, 2011, 179; LUPÁRIA, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, (diretto da) Spangher, vol. VII, a cura di Garuti, Utet giuridica, 2011 387; ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, 1, 135.

[382] In dottrina, per un'analisi delle modalità tecniche di esecuzione delle intercettazioni telematiche, si vedano VACIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, 2012, 80 ss.; TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, Cedam, 2014; PITTIRUTI, Digital evidence e *procedimento penale*, Giappichelli, 2017, 63.

[383] Specifica la Corte che di solito tale tipologia di intercettazione si attua attraverso la clonazione dell'*account* di posta elettronica dell'indagato e immediata trasmissione dei dati presso una postazione di decodifica.

Dinanzi a uno scenario di questo tipo, continuare a fondare la distinzione tra un'attività di mero sequestro e una di intercettazione sul solo carattere contestuale o meno della captazione conduce a risultati paradossali, con il rischio di incorrere in un sistematico abbassamento dei livelli di tutela connessi alle misure restrittive del diritto di cui all'art. 15 Cost. Non possono, sul punto, non condividersi le considerazioni di chi ha evidenziato che «in virtù di una simile qualificazione, viene meno ogni ragione di una tutela rafforzata e non è richiesta l'adozione delle garanzie che sorreggono l'attività di intercettazione telematica ex art. 266 *bis* c.p.p. in termini di presupposti ed autorizzazione giurisdizionale […] Al di fuori delle ipotesi sinora richiamate, ovvero quella della captazione contestuale di un flusso comunicativo di dati connotato da dinamicità e attualità e quella dell'apprensione di contenuti di posta elettronica nella disponibilità del fornitore del servizio, residua la casistica dell'acquisizione di *e-mail* rinvenute in seguito all'ispezione o alla perquisizione di un supporto informatico di proprietà dell'utente. Simili attività investigative evidenziano la tensione esistente tra la legalità processuale, preordinata a garantire sia la certezza giuridica della legittimità delle operazioni sia la tenuta dibattimentale dei risultati d'indagine, e la tutela in concreto delle garanzie»[384].

Proprio l'esempio delle bozze di *e-mail* adoperate per scambiare informazioni senza inoltro del messaggio dimostra come i tradizionali criteri ricostruttivi ed ermeneutici sostenuti dalla giurisprudenza di legittimità siano eccessivamente rigidi e insuscettibili di apprestare uno statuto di tutele adeguato[385]. In un simile caso, pur a fronte dell'evidente finalità comunicativa del salvataggio delle bozze nella casella *e-mail*, l'esclusione della applicabilità della disciplina delle intercettazioni viene fatta dipendere da un dato meramente tecnico-formale come quello dell'effettivo inoltro del messaggio e appare, pertanto, del tutto irragionevole.

Simili frizioni con le guarentigie costituzionali e con il principio di legalità si esacerbano nel caso di monitoraggio occulto e continuativo della casella di posta

[384] PADUA, *L'accesso alla casella e-mail e l'acquisizione dei contenuti: un delicato inquadramento normativo*, in *Proc. pen. e giust.*, 2018, 3, 595-596.

[385] Si vedano, sul punto, anche le considerazioni di PARLATO, *Problemi insoluti: le perquisizioni on-line*, cit., 295: «la Suprema Corte si destreggiava tra le varie attività limitrofe, qualificando l'intercettazione "captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti". L'evolversi sia degli strumenti captativi, sia delle comunicazioni stesse che ne sono oggetto, ha messo ora in crisi diversi capisaldi di tale definizione: tra essi, la necessaria concomitanza tra attività captativa segreta ed interlocuzione tra i soggetti coinvolti nella comunicazione/conversazione, nonché l'inquadramento di quest'ultima».

elettronica o degli applicativi di messaggistica istantanea: è evidente, in questo caso, come la trasposizione delle categorizzazioni a oggi invalse nella giurisprudenza di legittimità comporti l'applicazione livelli di tutela del tutto insufficienti a fronteggiare le gravi compressioni dei diritti fondamentali dei singoli. Non è mancato, d'altronde, chi ha evidenziato come l'impiego del captatore informatico al fine di acquisire le comunicazioni pregresse memorizzate sul dispositivo sia illegittimo e comporti, pertanto, l'inutilizzabilità del risultato probatorio raggiunto[386].

4. La localizzazione *online.*

Un'ulteriore attività investigativa resa possibile dal ricorso al captatore informatico consiste nella localizzazione dello strumento digitale bersaglio. Trattasi di un mezzo investigativo assimilabile al pedinamento elettronico o tramite sistema GPS[387], entrambi da tempo sotto il mirino di una parte della dottrina che non ha mancato di evidenziare le criticità e le frizioni con i principi costituzionali della ricostruzione operata in materia dalla giurisprudenza di legittimità. Con indirizzo granitico, infatti, se ne ammette il ricorso nell'indagine penale oltre che l'utilizzo dei risultati conoscitivi ottenuti in ragione della irripetibilità dell'atto[388]. Come noto, infatti, manca nel codice di rito qualsivoglia previsione normativa che regoli tale forma di pedinamento[389] e, in presenza di un simile vuoto legislativo, la giurisprudenza è compatta nel ritenere che la localizzazione e il monitoraggio degli spostamenti di un soggetto altro non siano che modalità tecnologicamente avanzate di pedinamento che, come tale, rientrerebbero – al pari del pedinamento "tradizionale" – nelle attività atipiche di controllo e accertamento demandate alla polizia giudiziaria ai sensi degli artt. 55, 347 e 370 c.p.p., senza che sia necessaria alcuna autorizzazione giudiziale[390].

---

[386] Così, PADUA*, L'accesso alla casella e-mail*, cit., 599.

[387] Sul punto, da ultimo, si veda la trattazione sistematica di FANUELE, *La localizzazione satellitare nelle investigazioni penali*, Cedam, 2019, 205, anche per gli ampi riferimenti bibliografici.

[388] Addirittura, secondo Sez. III, 2 aprile 2019, n. 36364, «la perdita, per un disguido tecnico, del supporto informatico contenente i dati trasmessi e rilevati dal GPS istallato sul veicolo dell'imputato non preclude che tali informazioni possano comunque essere acquisite nel dibattimento per mezzo delle deposizioni della polizia giudiziaria che ha proceduto alla loro analisi ed alla loro annotazione nelle relazioni di servizio».

[389] BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali*, in AA.VV., *Le indagini atipiche*, a cura di Scalfati, Giappichelli, 2019, 443.

[390] *Ex multis*, Sez. II, 4 aprile 2019, n. 23172 in *CED Cass.*, n. 276966; Sez. III, 27 febbraio 2015, n. 32699, inedita; Sez. I, 10 gennaio; 2012, n. 14529, inedita; Sez. V, 10 marzo 2010, n. 9667, in *Dir. pen. proc.*, 2010, p. 1464; Id., Sez. IV, 29 gennaio 2007, n. 8871, in *Cass. pen.*, 2008, p. 1137; Sez. V, 27 febbraio 2002, Bresciani, in *Foro it.*, 2002, II, c. 635.

Tuttavia, le criticità evidenziate dalla dottrina con riferimento alle operazioni di pedinamento elettronico e a quelle operate a mezzo di sistemi GPS si ripropongono in maniera non dissimile nel caso di pedinamento effettuato tramite l'inoculazione di un *virus* con la conseguente acquisizione del controllo sul dispositivo infettato e dei dati di localizzazione presenti nel medesimo. Non pare, infatti, che il ricorso a simile modalità operativa abbia caratteristiche che consentano di tracciare una distinzione significativa rispetto agli equivalenti – pur tecnologicamente meno avanzati – del pedinamento elettronico o tramite GPS[391], quanto a dati e informazioni acquisibili o diritti fondamentali incisi. Anche in questo caso, infatti, come nel pedinamento elettronico "tradizionale", l'attività investigativa si sostanzia in un monitoraggio continuo degli spostamenti del soggetto attenzionato dall'indagine, non *in toto* assimilabile al pedinamento "classico" operato personalmente e fisicamente dall'agente di polizia giudiziaria.

Nonostante, dunque, il ricorso al *virus* non comporti alcuna significativa differenza rispetto all'uso del GPS o al pedinamento elettronico, pare, nondimeno, opportuno, per ragioni di completezza, soffermarsi brevemente sul tema, quanto meno al fine di portare a emersione le criticità connesse al ricorso a tale strumento investigativo.

Secondo la giurisprudenza di legittimità, la non necessità di un provvedimento autorizzativo dell'autorità giudiziaria si spiega in ragione del mancato impatto della misura su diritti costituzionalmente tutelati. Si legge, ad esempio, in una delle pronunce più recenti sul tema[392] che il rilevamento satellitare «non si risolve in una interferenza con il diritto alla riservatezza delle comunicazioni né in una lesione dell'inviolabilità del

[391] Sul punto si vedano, però, le osservazioni di NOCERINO, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0,* in *Dir. pen. e proc*., 8, 2021, 1026, che rileva il differente grado di intrusività connesso all'utilizzo di sistemi informatici (come il captatore informatico) che consentono il controllo costante della posizione del soggetto in quanto aventi ad oggetto il monitoraggio di uno strumento digitale che egli generalmente porta sempre con sé, rispetto a sistemi di rilevazione GPS posizionati, normalmente, sui veicoli. L'autrice evidenzia come «la dirompenza di simili strumenti non consente tuttavia di assimilare tout court le attività de quibus al "mero" pedinamento satellitare tradizionale che, nella maggior parte dei casi, deriva dal posizionamento di un GPS satellitare sulle autovetture. In effetti, la peculiarità di queste *species* di geolocalizzazione è l'osservazione in tempo reale del movimento del soggetto "monitorato": in questi casi, è sufficiente che la persona da monitorare porti con sé, nei suoi spostamenti, lo smarthphone o il tablet dotato di connessione mobile affinché gli investigatori possano conoscere i movimenti del soggetto senza limiti spazio-temporali. In altri termini, pur ritenendo che il pedinamento elettronico possa pacificamente essere ricompreso nel genus dei mezzi di ricerca della prova atipici, non si può non evidenziare il maggiore grado di incisività rispetto ai diritti fondamentali allorquando l'attività de qua venga condotta mediante strumenti tecnici di indagine, dal momento che, in tal modo, vengono rilevati tutti gli spostamento dell'individuo anche quando entra in luoghi privati, all'interno dei quali non potrebbe estendersi il pedinamento elettronico tradizionale».

[392] Sez. II, 4 aprile 2019, n. 23172, in *CED Cass.*, n. 276966.

domicilio», con la conseguente possibilità, per la polizia giudiziaria, di effettuarlo di sua iniziativa senza necessità di un'autorizzazione preventiva né di una successiva convalida.

La dottrina che si è occupata del tema ha compattamente criticato una simile ricostruzione sul presupposto che la stessa, oltre a non considerare una serie di parametri costituzionali che ben potrebbero venire in rilievo nel caso di specie[393], non terrebbe in minima considerazione le indicazioni derivanti dalla giurisprudenza della Corte europea dei diritti dell'uomo che, ormai da più di un decennio, reputa che l'uso del GPS per monitorare gli spostamenti di un soggetto interferisca con il diritto alla vita privata di cui all'art. 8 della Convenzione[394] e che, pertanto, debbano trovare piena applicazione le condizioni di legittimità dell'atto descritte dal medesimo articolo, nell'interpretazione fornitane dalla stessa Corte: anzitutto, deve trattarsi di una misura necessaria in una società democratica ad assicurare il soddisfacimento degli interessi ivi enumerati; è necessario, poi, che la stessa abbia una base legale e che siano previste specifiche garanzie a tutela degli individui contro ingerenze illegittime o arbitrarie. Requisiti, questi ultimi, che non appaiono adeguatamente soddisfatti nel nostro ordinamento, tanto che una parte della dottrina italiana ha evidenziato come non vi sia

[393] Si vedano, ad esempio, le riflessioni di ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della privacy e onde eversive,* in *Arch. pen*., 2015, 3, 924 ss., che evidenzia come, oltre alla restrizione del diritto alla *privacy* e del diritto a spostarsi liberamente sul territorio senza subire forme di controllo occulto – riconducibile alla libertà di circolazione di cui all'art. 16 Cost. –, potrebbe venire in rilievo anche l'inviolabilità del domicilio tutte le volte che il pedinamento elettronico, dopo essersi svolto in luoghi pubblici, prosegua negli spazi di cui all'art. 14 Cost.

[394] Corte e.d.u., 2 settembre 2010, app. n. 35623/05, Uzun vs Germania e Corte e.d.u., 8 febbraio 2018, app. n. 31446/12, Ben Faiza vs Francia. Nelle pronunce in questione, la Corte ha evidenziato come nel concetto di "vita privata" ricada anche «la zona di interazione di un individuo con un altro, anche in un contesto pubblico», trattandosi di un aspetto suscettibile di incidere sullo sviluppo della personalità umana. Conseguentemente, misure comportanti la registrazione sistematica o permanente di dati concernenti una persona, ancorché gli stessi siano "esposti" al pubblico, può comportare una lesione del diritto alla vita privata.

altra via percorribile se non quella dell'inammissibilità[395] o inutilizzabilità[396] dei risultati ottenuti[397].

Il caso del pedinamento elettronico o tramite captatore informatico rappresenta un ulteriore punto di emersione della inadeguatezza dell'attuale costruzione dogmatica in tema di prova e investigazioni atipiche. Dinanzi alla sistematica tensione fra tutela dei diritti fondamentali e le esigenze di accertamento del fatto, ingenerata dai nuovi strumenti tecnologici di investigazione atipica, non pare rinviabile una seria riflessione sulla perdurante inadeguatezza dell'interpretazione giurisprudenziale per lo più propensa a ritenere integrati i presupposti per l'ammissione della prova in relazione agli esiti conoscitivi raccolti attraverso le nuove modalità tecnologiche di localizzazione.

5. L'acquisizione di video-riprese.

Altro applicativo del captatore informatico è quello che consente l'acquisizione del controllo sulla telecamera del dispositivo, che può, dunque, essere attivata e disattivata (anche congiuntamente al microfono) dagli investigatori in qualsiasi momento, consentendo la captazione di immagini all'insaputa del soggetto che utilizza lo strumento *target*.

Prima di soffermarsi sulla disciplina eventualmente applicabile, *de iure condito*, a una simile attività, occorre sgomberare il campo dal possibile equivoco di riconnettere allo svolgimento di tale attività una lesione dell'inviolabilità del domicilio informatico a prescindere dal luogo fisico nel quale vengono captate le immagini. Il che, volendo fare applicazione dei principi di diritto espressi proprio in materia di video-riprese nella

[395] MARCOLINI, *Le cosiddette perquisizioni* online (*o perquisizioni elettroniche*), in *Cass. pen*., 2010, 7-8 2867.

[396] In questo senso, FANUELE, *La localizzazione satellitare*, cit., 205, secondo la quale i risultati ottenuti con il pedinamento satellitare non possono reputarsi utilizzabili neppure a fini endo-processuali, ostando a ciò la regola di cui all'art. 191, comma 1, c.p.p. Per una diversa soluzione, si veda IOVENE, *Pedinamento satellitare e diritti fondamentali della* persona, in *Cass. pen.*, 2012, 10, 3564, secondo la quale dovrebbe sollevarsi una questione di legittimità costituzionale per contrasto con gli artt. 8 della Convenzione europea dei diritti dell'uomo e 117 Cost. del diritto vivente, laddove interpreta gli artt. 55, 347, 370 e 189 c.p.p. nel senso che essi rendano ammissibile il pedinamento elettronico alla stregua di un mezzo atipico di ricerca della prova, in quanto tale lasciato all'iniziativa della polizia giudiziaria.

[397] Nel senso, invece, che dovrebbe sollevarsi una questione di legittimità costituzionale per contrasto con l'art. 117 Cost. degli artt. 55, 348 o 189 c.p.p. per l'interpretazione fornitane dal diritto vivente, SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. ita. dir. e proc. pen.*, 2012, 2, 607.

pronuncia a Sezioni unite *Prisco*[398], avrebbe la conseguenza della radicale inammissibilità dei risultati probatori ottenuti stante la assenza di qualsivoglia disciplina normativa sul punto. Oggetto della ripresa e, dunque, dell'intrusione investigativa è, in questo caso, non quanto accade all'interno del dispositivo informatico, ma quanto si verifica intorno al medesimo. A ciò consegue che, astrattamente, possa trasporsi in questo campo la ricostruzione contenuta nella pronuncia sopra citata[399], fondata sulla natura – di domicilio, di luogo pubblico o di luogo coperto da un'aspettativa di riservatezza – dello spazio oggetto di videoripresa[400].

Che questa sia, nondimeno, una soluzione regolatoria adeguata a fronteggiare la grave intrusione realizzabile per mezzo del ricorso a tale tecnica investigativa nel caso di specie è conclusione della quale pare lecito dubitare, ancora una volta, in ragione delle caratteristiche tecniche dello strumento oggetto di analisi.

Si fa riferimento, in particolare, al carattere itinerante del medesimo che, inoculato nel dispositivo informatico, segue ogni spostamento del suo utilizzatore e consente un monitoraggio costante dello stesso. Proprio una simile capacità intrusiva sta alla base della inevitabile constatazione della difficoltà – da un punto di vista della necessaria tutela dei diritti fondamentali dei soggetti coinvolti – di reputare *sic et simpliciter* trasponibile nel caso di specie la distinzione fatta propria dal diritto vivente relativamente alla natura dei luoghi nei quali la video-ripresa viene ad essere realizzata. Alla base di tale affermazione stanno almeno due ordini di ragioni.

In primo luogo, la circostanza che lo strumento in questione consenta una sorveglianza non statica (come quella che si realizzerebbe nel caso di una video-camera che gli inquirenti decidessero di installare in un dato luogo) ma dinamica rende infinitamente maggiore la lesione dell'aspettativa di riservatezza dell'utilizzatore del dispositivo informatico, indipendentemente dalla natura – domiciliare, privata o pubblica – del luogo video-ripreso. A fronte di ciò, la soluzione regolatoria immaginata dalla pronuncia *Prisco* – in forza della quale sarebbe consentita la video-ripresa nei luoghi pubblici in assenza di qualsivoglia autorizzazione giudiziaria e quella realizzata nei

[398] Sez. un., 28 marzo 2006, n. 26795, Prisco, in *Cass. pen.*, 2006, 4344 ss., con note di RUGGERI, *Riprese visive e inammissibilità della prova* e di DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni unite*.

[399] Cfr. cap. 2, par. 3.1.

[400] In tal senso, CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo,* in *Dir pen e proc*., 2018, 9, 1219.

luoghi coperti da un'aspettativa di *privacy* in forza di una mera autorizzazione del pubblico ministero – appare inadeguata per difetto[401]. In altre parole, sarebbe miope non riconoscere che la sfera privata giuridicamente rilevante, «con il dilatarsi dello spazio di interazione della persona con il mondo esterno indotto dal progresso tecnologico, non può più farsi coincidere con quello coperto dagli artt. 14 e 15 Cost.»[402]. Sicché, se appare insufficiente la garanzia del mero provvedimento motivato del pubblico ministero per l'acquisizione di immagini in luoghi coperti da un'aspettativa di *privacy*, sembra una vera e propria aberrazione che una intrusione di tale entità nella sfera di riservatezza del singolo realizzata per mezzo di una video-ripresa costante e itinerante – sia pure in luoghi pubblici – possa reputarsi legittima in assenza di qualsivoglia provvedimento giudiziario autorizzativo e di qualsivoglia esplicitazione delle ragioni che giustificano il ricorso a un simile mezzo istruttorio nel caso di specie. Nella nota pronuncia *Uzun vs Germania* del 2010[403], d'altronde, la Corte europea dei diritti dell'uomo ha evidenziato come «*article 8 protects,* inter alia*, a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"* […] *A person walking along the street will inevitably be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character* […] *Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain*».

Appare più che mai urgente la presa d'atto, soprattutto da parte del legislatore, del rinnovato assetto della mappatura dei diritti fondamentali dei singoli in conseguenza del dirompere delle nuove tecnologie, non dissimilmente da quanto sta accadendo in altri

[401] Valgono viepiù, nel caso di specie, le considerazioni di ANDOLINA, *L'ammissibilità degli strumenti di* captazione, cit., 929 che, con riferimento alla disciplina enucleata dalla pronuncia in questione, rileva come l'impostazione alla medesima sottesa sia anacronistica in quanto l'esistenza di un provvedimento giudiziario autorizzativo nel caso di video-ripresa in luoghi coperti da un'aspettativa di *privacy* rappresenta una cautela insufficiente, anche in ragione dell'efficacia, nel nostro ordinamento, degli artt. 8 della Convenzione europea dei diritti dell'uomo e 8 della Carta dei diritti fondamentali dell'unione europea, che prevedono espressamente una riserva di legge per la compressione delle prerogative ivi riconosciute ai singoli.

[402] Ancora, ANDOLINA, *L'ammissibilità degli strumenti di captazione*, cit., 929.

[403] Corte e.d.u., 2 settembre 2010, app. n. 35623/05, Uzun vs Germania.

ordinamenti nei quali alcune pronunce, anche molto risalenti, danno testimonianza di un approccio non meramente formalistico alla tutela dei diritti, fondato su un'interpretazione delle categorie giuridiche esistenti che, a costo di più o meno evidenti disallineamenti dal dato testuale, accorda la massima tutela possibile alle prerogative individuali. Tra gli esempi più celebri, non può non citarsi la nota decisione Katz v. United States[404] del 1967, nella quale la Corte Suprema, pronunciandosi sulla legittimità dei risultati della registrazione realizzata, per il tramite dell'installazione di un dispositivo elettronico all'esterno di una cabina telefonica, senza una previa autorizzazione giudiziale, ha precisato l'ovvio, ovvero che «*what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection […] But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected*». Ciò, d'altronde, non è tanto diverso da quanto sostenuto anche da una parte della dottrina italiana in merito alla necessità di riconoscere la «presenza di aree di pertinenza dell'individuo, ovvero di "spazi virtuali" di manifestazione della sua personalità, che vanno oltre l'interesse alla tutela del segreto e della *privacy* e che sono propriamente riconducibili a uno *spatium operandi et deliberandi* del titolare dello *jus excludendi alios*»[405].

6. Il *key logging* e le altre attività di controllo del dispositivo informatico.

Nel tentare di offrire una visione di insieme dell'attività d'indagine realizzabile tramite il captatore informatico, si è efficacemente evidenziato come il *software* installato possa, tra l'altro, «servire da vero e proprio specchio, idoneo a riflettere – in tempo pressoché reale – le attività che sono compiute all'interno del sistema, consentendo la graduale acquisizione di ciò che nel tempo si somma al dato già acquisito»[406]. In questa particolare funzionalità del captatore confluiscono, in via, per così dire, residuale, le attività denominate di *keylogging* e tutte le ulteriori attività di controllo del dispositivo

[404] Supreme Court, Katz v. United States, 389 U.S. 347 (1967). Nella dottrina statunitense si è efficacemente parlato di un "*right to public anonimity*", il quale dovrebbe garantire che «*when in public, one will remain nameless–unremarked, part of the undifferentiated crowd–as far as the government is concerned*», Slobogin, *Public privacy: camera surveillance of public places and the right to anonymity*, in *Mississippi Law Journal*, 2002, 72, 235. Per un'analisi della giurisprudenza statunitense in tema di sorveglianza elettronica, si rinvia alla lettura di DI PAOLO, *Tecnologie del controllo e prova penale*, Cedam, 2008, 88 ss.

[405] FLOR, *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente*, in *Riv. ita. dir. e proc. pen*., 2007, 2-3, 941.

[406] MANCUSO, *La perquisizione* on line, in *Jusonline*, 2017, 3, 415.

informatico che appaiono insuscettibili di essere ricondotte alle tipologie investigative finora analizzate.

In particolare, tramite il sistema di *keylogging* è possibile ottenere il controllo della tastiera del dispositivo infettato, con la conseguente possibilità di decifrare e visualizzare tutto viene digitato tramite la stessa. Trattasi, come è intuibile, di attività tanto intrusiva quanto potenzialmente utilissima su un piano investigativo (si pensi, ad esempio, alla semplicità con la quale possono, in tal modo, acquisirsi le chiavi di accesso a sistemi di uso riservato dell'utente, come quello bancario, assicurativo e così via).

Altra funzione degna di nota è quella denominata *screenshot*[407], attraverso la quale è possibile ottenere istantanee dello schermo del dispositivo bersaglio, così visualizzando e mantenendo traccia di qualsivoglia attività vi si svolga. Simile a questa attività è, poi, quella di *screencast*, che però concerne l'acquisizione di video anziché di semplici istantanee.

Tentare di offrire una definizione complessiva ed esaustiva di simili attività è arduo almeno quanto tentare di ricondurle ad una qualche categoria giuridica esistente. Effettivamente, simili accertamenti sembrano rappresentare, anche nel panorama delle investigazioni digitali, un *novum* dalle connotate quanto mai eccentriche rispetto alle categorie investigative note.

Ogni tentativo di ricondurre tali acquisizioni di dati alle categorie tradizionali dei mezzi di ricerca della prova è destinato a fallire. Così, alcuni hanno evidenziato come tali attività siano sovrapponibili a una sorta di «atipica ispezione online»[408], ma il paragone non sembra calzante perché mentre l'ispezione è diretta all'accertamento delle tracce e degli effetti materiali del reato, tali attività non sono limiate a questo circoscritto oggetto, né per le finalità (spiccatamente esplorative) che le connotano né, tanto meno,

---

[407] Si veda la esaustiva definizione di ATERNO, *La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante screen shot,* in *Dir. pen. e proc*. 2018, 8, 1069, che evidenzia come tramite la «modalità "screen shot" si acquisisce in chiaro (parte di) ciò che è cifrato e che appare sullo schermo dello smartphone o di un personal computer nel momento in cui l'utente utilizza lo strumento informatico. Con delle vere e proprie fotografie dello schermo effettuate dal software posto all'interno dello smartphone/pc, il malware acquisisce - o può comunque acquisire - le informazioni più svariate sia dei contenuti comunicativi sia di quelli non comunicativi. Non si tratta di intercettazione ambientale con l'uso del microfono; non si tratta di captare da remoto tutti i files e contenuti del supporto; bensì soltanto di fare una "foto" di ciò che appare a video ovvero di ciò che l'utente del telefono sta facendo».

[408] FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale*, cit., 131.

per le caratteristiche proprie dello strumento su cui l'attività di ricerca si dipana, specie con riferimento all'incredibile eterogeneità di contenuti.

Al contempo, non sembra possa farsi riferimento alla categoria del sequestro, atteso che l'intrusione di cui si discute consente l'apprensione anche di dati non preesistenti rispetto all'atto acquisitivo. Per la stessa ragione va, poi, esclusa la riconducibilità all'istituto della perquisizione, che presuppone lo svolgimento di un'attività di ricerca mirata all'apprensione di qualcosa che già esiste e non alla realizzazione di una sorveglianza in tempo reale di un luogo, fisico o informatico che sia. Trattasi, in altre parole, di un'attività di acquisizione di dati in tempo reale, in quanto tale più simile a un'attività di intercettazione, rispetto alla quale, però, manca il carattere necessariamente comunicativo del dato acquisito[409].

A complicare qualsivoglia tentativo di inquadramento giuridico delle attività in oggetto contribuiscono i confini, per così dire, "mobili" delle stesse sotto un profilo squisitamente tecnico. A prima vista, infatti, le modalità di esecuzione delle operazioni sembrerebbero poter influire sulla riconducibilità o meno a certe specifiche categorie esistenti di mezzi di ricerca della prova. Così, se l'acquisizione di un di fermo immagine, o comunque di un numero circoscritto di istantanee, non sembra di per sé convincentemente riconducibile ad alcuna categoria esistente, laddove si verificasse un'acquisizione a intervalli ravvicinati di istantanee di tutto quanto accade sullo schermo, con la conseguente captazione di una conversazione *medio tempore* intrattenuta dall'utilizzatore del sistema, si potrebbe pensare di essere dinanzi a un'attività di intercettazione. Anticipandosi la conclusione cui si giungerà al termine del paragrafo, però, una sistematizzazione di questo tipo – cioè fondata sulla natura del dato acquisito – è caratterizzata non solo da evidenti margini di incertezza, ma altresì da una certa dose di "casualità". Nell'esempio appena fatto, la scoperta e la captazione di contenuti comunicativi vengono e a collocarsi alla stregua di meri "accidenti", non essendo possibile pronosticare quale uso dello strumento digitale farà il suo titolare – e, dunque, quale sarà la tipologia dei dati prodotti – prima dell'inizio delle operazioni.

Alla difficoltà di un inquadramento nelle categorie esistenti si accompagnano pericoli inediti per le prerogative individuali. Per quanto le attività appena descritte possano apparire, a primo acchito, meno intrusive di altre analizzate finora, una simile

[409] Cfr. par. 2.

conclusione sarebbe affrettata e poco convincente. Per avvedersi di ciò, basta riflettere sul fatto che tramite lo svolgimento di tali accertamenti è talvolta possibile acquisire quanto non si sarebbe potuto registrare neppure con un'intercettazione telematica. Si pensi, ad esempio, a un messaggio digitato sulla tastiera in vista dell'invio a un contatto presente sulla rubrica che non venga, però, spedito in ragione di un ripensamento. E ancora, si pensi alla possibilità di captare riflessioni, appunti o note registrati sul dispositivo informatico, dunque estrinsecazioni in forma intellegibile dei pensieri dell'utilizzatore del sistema non destinati alla condivisione con chicchessia. Sotto questo punto di vista, simili attività sembrerebbero suscettibili di impattare su prerogative di rango ben più elevato rispetto a quella tutelata dall'art. 15 Cost.

Quanto alla giurisprudenza, nella radicale assenza di una presa di posizione compatta sul punto, si registra uno sparuto numero di pronunce, peraltro fondate su soluzioni ermeneutiche difficilmente condivisibili. In una sentenza del 2017, ad esempio, la Sezione quinta della Corte di cassazione[410] ha ricondotto l'acquisizione di *screenshot* dal dispositivo informatico infettato dal captatore a una semplice attività di intercettazione telematica di cui all'art. 266 *bis* c.p.p. Di conseguenza, ha considerato utilizzabili gli esiti investigativi raccolti sul presupposto che la limitazione, precedentemente operata dalle Sezioni unite *Scurato*[411], dell'uso del captatore ai soli procedimenti di criminalità organizzata fosse stata dal Massimo Collegio operata solo con riferimento all'attività di intercettazione tra presenti, con la conseguenza che «non sono da intendersi escluse le ulteriori forme di intercettazione, tra cui quelle telematiche ex art. 266 *bis* c.p.p. che non sono intercettazioni caratterizzate dal doppio requisito di essere sia comunicative che tra presenti».

È evidente, però, anche alla luce di quanto si è detto in apertura del capitolo in merito alla necessità di distinguere simili attività da quella di cui all'art. 266 *bis* c.p.p., la fallacia di un simile modo di ragionare, riconducibile alla già segnalata tendenza ad ampliare a dismisura i confini del concetto di intercettazione al fine di impedire la dispersione di elementi conoscitivi reputati fondamentali nel compendio investigativo o probatorio del singolo processo.

---

[410] Sez. V, 30 maggio 2017, n. 48370, in *CED. Cass.*, n. 271412. Soluzione da ultimo ribadita da Sez. I, 7 ottobre 2021, n. 3591, Romeo, in *CED. Cass.*, n. 282495.

[411] Sez. un., 28 aprile 2016, n. 26889, Scurato, in *Arch. nuova proc. pen.*, 2017, 76 e ss. con nota di CAMON, *Cavalli di troia in Cassazione* e in *Cass. pen*. 2016, 2274, con nota di BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*.

Nell'impossibilità di ricondurre lo svolgimento di simili attività a categorie giuridiche esistenti, sembra inevitabile l'esito dell'inammissibilità – seguendo l'impostazione fatta propria dalle Sezioni unite *Prisco*[412] – o dell'inutilizzabilità – aderendo alla teoria della prova incostituzionale – dei risultati probatori ottenuti. Pare, infatti, difficilmente revocabile in dubbio che simili attività impattino, quanto meno, sull'inviolabilità del domicilio informatico, la cui restrizione è subordinata, in base al dettato costituzionale, alla riserva di legge.

Né pare opportuno, come si è già anticipato, tentare una sistematizzazione delle operazioni investigative esperibili tramite le funzionalità tecniche in commento in base alla tipologia di dati raccolti. Come si è lucidamente evidenziato, «un'interpretazione più sensibile alla tutela dei diritti fondamentali dalle subdole aggressioni cui essi sono sottoposti nell'era digitale porta a prescindere dal tipo di dato captato e ad attribuire carattere determinante all'invasività dell'attività captativa, anche in ragione della considerazione che, a fronte di strumenti di tal genere, una distinzione sul tipo di dato si potrebbe ragionevolmente effettuare soltanto *ex post* […] A ben vedere, infatti, la videoregistrazione della successione delle schermate di un computer o lo spionaggio della digitazione sulla tastiera giungono ad un livello di invasività tale da aggredire il foro interno della persona, la vera e propria inviolabilità della psiche, tanto da poter indurre a profilare un limite assoluto rispetto all'attività captativa»[413].

7. Il possibile ricorso a un'attività indiscriminata di sorveglianza: impatto sulle prerogative costituzionali e conseguenze processuali.

Come si è già evidenziato, la scomposizione finora operata delle singole attività esperibili tramite il controllo da remoto del dispositivo informatico risponde alla sola esigenza di ricavare, *de iure condito*, il trattamento processuale applicabile alle singole acquisizioni di dati realizzabili. Tanto nell'evidente impossibilità di individuare un istituto che possa reputarsi un convincente succedaneo di quello che, invece, pare essere l'utilizzo fisiologico dello strumento in questione, da rinvenirsi proprio nel contestuale svolgimento delle attività finora analizzate, con la realizzazione di una vera e propria sorveglianza "a tappeto" del dispositivo infettato e del suo utilizzatore.

[412] Sez. un., 28 marzo 2006, n. 26795, Prisco, cit.
[413] CONTI, *Sicurezza e riservatezza*, in *Dir. pen. e proc*., 2019, 11,1584.

Siamo in un campo, dunque, in cui l'impatto sulle prerogative costituzionali degli individui si colloca – quanto meno per quanto concerne l'ambito delle investigazioni da remoto – sul livello massimo possibile. L'attività in tal modo realizzata non è minimamente assimilabile, sul piano dell'incidenza sulle aspettative di riservatezza connesse all'uso della tecnologia informatica, neppure alle tradizionali attività – comunemente inserite tra i mezzi di ricerca della prova maggiormente invasivi – comportanti una sorveglianza contestuale del soggetto, quali l'intercettazione o lo svolgimento di video-riprese. Tanto in quanto lo strumento in questione non si limita a consentire la captazione di quanto accade intorno al dispositivo ma, come visto, lo sonda nella sua interezza, consentendo di accedere – nella totale inconsapevolezza di chi subisce l'intrusione – in «spazi teoricamente inviolabili che rappresentano le estensioni digitali della personalità degli individui, dove vengono riversate informazioni riservate di ogni genere»[414]. Non è nuova la costatazione per la quale, a fronte di attività suscettibili di assurgere a simili livelli di intrusività, la compressione della intimità individuale sarebbe tale da ingenerare una vera e propria violazione della psiche[415].

Non sembra, in definitiva, possano esservi dubbi sulla conclusione per la quale, laddove le potenzialità esplorative dello strumento informatico in questione siano esperite contestualmente, con la realizzazione di una forma di subdola e occulta sorveglianza del dispositivo, si sia dinanzi a una marchiana lesione di quel nuovo bene di rilevanza costituzionale che, in chiusura del primo capitolo, è stato indicato come diritto alla riservatezza e all'autodeterminazione nell'uso delle tecnologie informatiche. Prerogativa che, trovando la sua matrice costituzionale nel combinarsi dei diritti discendenti dagli artt. 13 e 14 Cost., è certamente coperta da una riserva di legge e di giurisdizione e non può che essere destinataria di uno statuto di tutele improntato al massimo rigore, proporzionalmente alla gravità della sua restrizione[416]. Come si vedrà, peraltro, trattando delle difficoltà connesse a una regolamentazione futura dello

[414] DANIELE, *Contrasto al terrorismo e captatori informatici*, in *Riv. dir. proc*., 2017, 2, 402.

[415] BRONZO, *L'impiego del trojan horse informatico*, cit., 303 e CONTI, *Prova informatica e diritti fondamentali*, cit., 1220.

[416] In termini, BRONZO, *L'impiego del trojan horse informatico*, cit., 350, che evidenzia come «queste attività investigative realizzate attraverso i virus spia incidano insomma su beni la cui lesione esige – in ogni caso – una previa determinazione, da parte del legislatore ordinario, dei «casi» e dei «modi» di aggressione. Per i quali è necessario, cioè, che vengano predeterminati, all'esito di un delicato e complesso bilanciamento di vari interessi, i reati per cui quella certa modalità investigativa è possibile; la legittimazione soggettiva (giudice, pubblico ministero, polizia giudiziaria); la descrizione del tipo di attività e la sua durata; le sanzioni per il caso di inosservanza delle regole».

strumento in questione, la necessità di approntare un reticolo di garanzie di estremo rigore dipende altresì dalla esigenza di rendere il ricorso a un simile strumento da parte delle autorità pubbliche preposte alla repressione dei reati "accettabile" da parte della popolazione, costantemente esposta al rischio di finire nel mirino di simili pratiche investigative. La realizzazione di una sorveglianza continuativa degli atteggiamenti e dei pensieri più intimi del singolo, infatti, incide sulla sua libertà psichica non solo nel senso, appena precisato, di rendere possibile un'intrusione negli aspetti più reconditi della sua personalità, di cui il dispositivo informatico è spesso un formidabile *medium*; ma altresì nel senso di ingenerare dei riflessi comportamentali che sono la diretta conseguenza della consapevolezza della possibilità di essere sottoposti a controllo[417]. Detto altrimenti, chi sa di poter essere sorvegliato tende ad agire in maniera differente. Evidente, dunque, che anche in questo senso tali strumenti possono avere riflessi sulla libertà di autodeterminazione[418].

Finché una regolamentazione dello dell'attività in questione non sarà approntata, sembra scontato l'esito dell'inammissibilità o inutilizzabilità della prova così ottenuta[419].

Appare, pertanto, utile e necessario interrogarsi sulle difficoltà – sia tecniche che di natura politico-normativa – connesse a una auspicabile regolamentazione complessiva dell'attività di *online surveillance*, nella consapevolezza che la comminatoria dell'inutilizzabilità non è sufficiente a riparare alla violazione alle prerogative dei

---

[417] *Ex multis*, REIMAN, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, Santa Clara computer & high tech. L. J., 27, 38, 1995, che evidenzia che «*to the extent that a person experiences himself as subject to public observation, he naturally experiences himself as subject to public review. As a consequence, he will tend to act in ways that are publicly acceptable*». Ciò accade in quanto, quando sa di essere osservato, l'individuo sviluppa una sorta di "doppia visione", per la quale tende a identificarsi con il punto di vista dell'osservatore, che si affianca a quello proprio. Per la osservazione, poi, per la quale lo sviluppo di tale "doppia visione" laddove la sorveglianza involga non solo l'osservazione ma anche la registrazione dei comportamenti del singolo, si veda SLOBOGIN, *Public privacy*, cit., 239. Si veda anche Nicolicchia, *I controlli occulti e continuativi come categoria probatoria*, cit., 81.

[418] Una plastica dimostrazione di ciò si rinviene nella miriade di esempi che la stessa quotidianità ci offre. Basti pensare all'abitudine, ormai diffusissima tra gli utilizzatori di sistemi informatici dotati di videocamera, di coprire l'"occhio" della camera quando non è in uso.

[419] In tal senso è compatta la dottrina. Si vedano, *ex multis*, ANDOLINA, *L'ammissibilità degli strumenti di captazione*, cit., 923; TORRE, *Il captatore informatico*, cit., 1781; FILIPPI, *L'ispe-perqui-intercettazione "itinerante: le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, in *Arch. pen.*, 2016, 2, 352; GRIFFO, *Perquisizione informatica… e dintorni,* in *Giur. pen. web*, 2019, 5, 3; MARCOLINI, *Le cosiddette perquisizioni* online, cit., 2866; TONINI e CONTI, *Il diritto delle prove penali*, Giuffrè, 2014, 392 ss.

singoli causato dal ricorso a tale strumento[420] e che è, piuttosto, necessario approntare una cornice normativa adeguata.

8. L'*online surveillance* come categoria probatoria: una proposta *de iure condendo.*

Al fine di stabilire le coordinate essenziali di un intervento legislativo finalizzato a regolare lo svolgimento di attività di *online surveillance* pare opportuno prendere le mosse proprio dalla cornice normativa già ipotizzata con riferimento all'attività di *online search*[421]. Le due tipologie probatorie, infatti, presentano alcuni importanti tratti comuni sia sotto il profilo tecnico (il riferimento è, anzitutto, al tipo di tecnologia utilizzata e alla congerie dei possibili bersagli dell'attività intrusiva) sia sotto il profilo dei beni giuridici incisi (da un lato, il domicilio informatico; dall'altro, il diritto all'autodeterminazione nell'uso delle tecnologie informatiche) che, pur essendo certamente distinti, sono nondimeno contigui.

Nel delineare, dunque, gli elementi essenziali dello statuto normativo dell'attività di *online surveillance*, anche al fine di evitare sterili ripetizioni, si richiamerà ampiamente la disciplina già abbozzata con riferimento all'attività di *online search*, con l'indicazione, però, di volta in volta, di quelle che dovrebbero essere le divergenze maggiormente significative rispetto a quest'ultima.

Come si vedrà, infatti, il più elevato rango della prerogativa costituzionale incisa nel caso di *online surveillance*[422] e la maggiore intrusività della violazione determinano, oltre a ovvie criticità della regolamentazione su un piano squisitamente politico-normativo, anche alcune significative divergenze in termini di proporzionalità del bilanciamento di interessi sotteso al possibile assetto normativo della materia. Ciò impedisce un richiamo integrale *sic et simpliciter* alle già delineate condizioni di ammissibilità delle attività di *search* e *seizure* da remoto e, anzi, impone l'individuazione di correttivi finalizzati a creare uno statuto di guarentigie maggiormente rigoroso, al fine di rendere del tutto eccezionale l'impiego a fini investigativi di pratiche altamente lesive dei diritti di libertà.

---

[420] CAPRIOLI, *Intercettazioni e tutela della privacy nella cornice costituzionale*, in *Cass. pen.*, 2021, 4, 1144.

[421] Si veda cap. 3, par. 4 ss.

[422] Come si è già visto, viene in gioco anche la libertà morale.

Sotto il profilo tecnico-normativo, la principale difficoltà connessa alla regolamentazione della *online surveillance* è diretta conseguenza di una peculiare caratteristica tecnica dello strumento in questione, da rinvenirsi nel suo carattere promiscuo. Come emerso nei paragrafi precedenti, la versatilità del congegno tecnologico di cui si discute è tale da consentire la realizzazione di una vasta gamma di attività di ricerca e acquisizione dei dati. Peraltro, se già in una prospettiva attuale tali attività appaiono difficilmente tipizzabili (si pensi alle difficoltà, prima segnalate, di tracciare con esattezza i confini e le caratteristiche di attività come quelle di *keylogging* o di *screenshot*), in una prospettiva futura le criticità di una dettagliata classificazione sono destinate ad aumentare alla luce dell'imprevedibilità degli sviluppi tecnologici, che ben potrebbero consentire ulteriori inedite forme di intrusione. Perciò occorre evitare che la disciplina normativa adottata in materia si esponga a una inesorabile e rapida obsolescenza[423].

In dottrina, la costatazione di simili problematiche ha condotto al delinearsi di differenti prospettive nell'approccio regolativo da seguire *de iure condendo*.

Secondo un primo orientamento – che parrebbe fondarsi proprio sulla constatazione della difficoltà di tipizzazione di tutti i possibili usi del captatore (così come di qualsivoglia altro strumento di controllo remoto che l'avanzamento tecnologico consentirà di sviluppare) – sarebbe opportuno individuare un'unica categoria probatoria, tramite la messa a punto di regole specifiche da seguire ogniqualvolta si proceda a un'attività di sorveglianza occulta e continuativa da remoto, indipendentemente dallo strumento tecnologico adoperato[424].

Secondo una proposta particolarmente suggestiva, invece, si potrebbe prendere a modello lo statuto della prova atipica di cui all'art. 189 c.p.p. al fine di introdurre una disciplina per l'atto d'investigazione atipico, con la contestuale individuazione di

[423] In termini, NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 59. Si vedano anche le considerazioni di DANIELE, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen. e giust.*, 2018, 5.

[424] In questo senso, MANCUSO, *La perquisizione* on line, cit., 433, che individua altresì alcune coordinate essenziali del possibile intervento normativo. In termini, BARROCU, *Il captatore informatico: un virus per tutte le stagioni*, in *Dir. pen. e proc*., 2017, 3, 386. Per un approccio estremamente rigoroso ed esaustivo, si vedano le dettagliate considerazioni di NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 57 ss., che ipotizza la messa a punto di una categoria probatoria avente ad oggetto lo svolgimento di controlli contrassegnati dal carattere occulto e continuativo.

specifiche garanzie operanti a tutela dei diritti fondamentali lesi dalla misura[425]. Andrebbe, dunque, introdotto un divieto generale di ingerenza sui diritti fondamentali attraverso atti investigativi non disciplinati dalla legge, con la previsione della eccezionale possibilità di ricorrervi in alcuni specifici e ben circoscritti casi (coincidenti con l'accertamento dei più gravi reati di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p.) e con l'operatività di peculiari garanzie, tra le quali il necessario intervento del giudice.

Tale soluzione presenta il non trascurabile vantaggio di essere sufficientemente elastica da attagliarsi anche a nuovi strumenti investigativi che il progresso tecnologico dovesse porre a disposizione degli inquirenti nel prossimo futuro. Essa, tuttavia, potrebbe prestare il fianco a un'obiezione correlata al modello di disciplina dettato dal codice in materia di prova atipica. Quest'ultimo, infatti, comporterebbe che le modalità specifiche di esecuzione dell'atto non siano determinate fin dal principio, ma vadano individuate, in prima battuta, dal pubblico ministero, per poi essere convalidate dal giudice all'emissione del provvedimento autorizzativo[426].

Di conseguenza, potrebbe rimanerne frustrata l'esigenza costituzionale di predeterminazione, ad opera della legge, non solo i "casi" ma anche i "modi" dell'intrusione. Ciò comporterebbe un'implementazione solo parziale della riserva di legge ed esporrebbe la nuova disciplina al rischio di una declaratoria di illegittimità costituzionale.

Secondo un'altra posizione, sarebbe da scartare l'approccio fondato sulla individuazione di un'unica categoria probatoria, per procedere ad «elaborare discipline differenziate a seconda della specifica intrusione che si intenda effettuare, con garanzie tendenzialmente modellate sulla falsariga di quelle previste oggi per le intercettazioni

---

[425] MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta,* in *Cass. pen*., 2015, 2, 767 ss. Quanto all'individuazione dei confini della categoria investigativa in argomento, l'autore specifica, inoltre, che vengono in rilievo i soli atti che, attraverso l'uso della tecnologia, non «si limitano a potenziare le ordinarie capacità percettive degli operanti (*sense-enhancing technologies*), bensì quelli che attribuiscono loro facoltà estranee alla dimensione umana (*sense-replacing technologies*)». In secondo luogo, dovrebbe trattarsi di atti che, secondo una valutazione *ex ante*, possano fornire informazioni utili alla conduzione o prosecuzione dell'indagine. Infine, deve trattarsi di atti che incidano sui diritti fondamentali dei singoli.

[426] Secondo la proposta in argomento, infatti, la richiesta del pubblico ministero dovrebbe contenere «la descrizione dettagliata dell'atto che si intende espletare e delle relative modalità di svolgimento». Nel provvedimento autorizzativo, poi, il giudice potrebbe «modificare le modalità di svolgimento dell'atto descritte dal pubblico ministero o prescriverne di ulteriori meno gravose per le limitazioni del diritto fondamentale ma ugualmente efficaci ai fini dell'accertamento». Cfr. MARCOLINI, *Le indagini atipiche a contenuto tecnologico,* cit., 791.

telefoniche, che presentano lo *standard* più elevato»[427]. Anche tale ricostruzione, tuttavia, si espone ad alcuni rilievi critici.

Non solo, come si è evidenziato, un approccio di questo tipo esporrebbe la disciplina normativa al rischio di una veloce obsolescenza, data l'impossibilità di prevedere gli sviluppi futuri delle tecnologie informatiche di controllo remoto, che potrebbero consentire lo svolgimento di attività intrusive nuove. Oltre a ciò – e questo pare l'argomento risolutivo – la parcellizzazione delle singole tipologie di attività esperibili non consentirebbe di cogliere appieno la capacità intrusiva dello strumento in questione, la cui gravità – in termini di impatto sui diritti fondamentali coinvolti – ben si intuisce solo se si guarda all'operatività congiunta di tutti gli applicativi di controllo a disposizione dello stesso. Sotto questo punto di vista, è peraltro da dubitare che il livello di garanzie assicurato in materia di intercettazioni telefoniche costituisca uno *standard* adeguato e proporzionato in relazione ad atti investigativi la cui invasività e di gran lunga superiore a quella della intrusione in una conversazione da parte dell'autorità procedente. In altre parole, rischierebbe di sfumare la percezione dell'elevatissimo pregiudizio sui diritti fondamentali implicato in queste nuove forme di sorveglianza e ciò rischierebbe di indebolire, anziché di incrementare, il sistema di tutele a garanzia dei medesimi, in conseguenza di una fallace comprensione delle potenzialità intrusive dell'atto. Facile pronosticare, a questo punto, un appiattimento verso il basso – cioè a discapito delle garanzie – dell'equilibrio da raggiungere in punto di bilanciamento dei contrapposti interessi in ballo.

Per tutte le ragioni appena esposte, appare preferibile l'opzione a favore della individuazione di un'unica categoria probatoria, con la messa a punto di un reticolo di garanzie improntate al massimo rigore possibile e, soprattutto, alla regola per la quale il ricorso a simili tecniche di sorveglianza deve in generale ritenersi vietata, essendo eccezionalmente consentito esclusivamente in alcuni ristretti e ben determinati casi.

Ciò precisato sul piano tecnico-normativo, il maggiore ostacolo alla predisposizione di una simile disciplina pare essere, tuttavia, quello di natura ideologico-politica.

Nella naturale contrapposizione tra le esigenze securitarie, sempre più avvertite, e la tutela dei diritti – soprattutto dei diritti di riservatezza – «mafia, terrorismo internazionale, pedofilia, tratta di esseri umani, sono le attuali parole d'ordine che, sulla

[427] BRONZO, *L'impiego del* trojan horse *informatico*, cit., 353.

linea del bilanciamento, giustificano – presso l'opinione pubblica – spostamenti del cursore a vantaggio dell'esigenza repressiva, con sacrificio dei diritti di libertà»[428]. In un simile scenario, è quasi fisiologica la tendenza dei cittadini a cedere al potere pubblico una fetta delle loro legittime aspettative di riservatezza, in cambio di quella sicurezza di cui hanno bisogno per il migliore sviluppo delle lor relazioni[429]. Lo Stato diviene così parte integrante di quella cerchia di soggetti in possesso degli strumenti tecnologici funzionali a realizzare forme più o meno aggressive di sorveglianza.

Secondo una percezione piuttosto comune, ciò non dovrebbe destare particolare allarme visto che la sorveglianza da parte delle autorità pubbliche serve a garantire l'ordine e la sicurezza. Sembra, invece, che forme più o meno larvate di vigilanza destino più diffusa inquietudine e preoccupazione laddove a porle in essere siano soggetti privati. È questo, però, un approccio "ingenuo" se non insipiente sulla questione, per la banale ragione che lo Stato è titolare del monopolio della forza, che non è nella disponibilità di aziende o altri soggetti privati. Pertanto, le conseguenze di eventuali abusi dei poteri di sorveglianza e di controllo nelle mani dello Stato sono suscettibili di essere percepite in maniera più disruptiva.

È essenzialmente questa la ragione per la quale, nonostante l'allarme diffuso e, apparentemente, perdurante che contrassegna la nostra epoca dinanzi alle forme più gravi di criminalità, non si assiste a una generalizzata rinuncia, da parte dei cittadini, alle loro esigenze di *privacy*, rispetto alle quali, anzi, vengono reclamate garanzie di tutela sempre più intense, di pari passo con la crescente capacità intrusiva degli strumenti tecnologici del controllo.

In tale contesto, sembrano soprattutto le Corti europee, per il momento, le principali custodi dei diritti in questo campo: si è parlato in questo senso della progressiva definizione di vero e proprio statuto dei diritti sulla rete[430], testimoniata dalle molte

---

[428] ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.*, 2014, 3, 1155-1156.

[429] FANUELE, *La localizzazione satellitare*, cit., 5.

[430] In tal senso, si veda SPILLER, *La sentenza Tele2 Sverige: verso una* digital rule of law *europea?*, in *IANUS Dir. e fin.*, dic. 2017, 280 ss., la quale mette in luce il ruolo di *human rights adjudicator* svolto dalla Corte di Giustizia in materia di diritti sulla rete. Nello stesso senso, sia pur con accenti critici, POLLICINO, *Diritto all'oblio e conservazione dei dati. La Corte di Giustizia a piedi uniti: verso un* digital right to privacy, in *Giur. cost.*, 2014, 3, 2956. Sul punto, si vedano, altresì, le considerazioni di RAFARACI, *Verso una* law of evidence *dei dati*, in *Dir. pen. proc.*, 2021, 7, 855. Da ultimo, sull'evoluzione della giurisprudenza della Corte di Giustizia in tema di *data retention*, si veda MARCOLINI, *La giurisprudenza della Corte di giustizia dell'Unione europea sulla data retention: il baluardo dei diritti fondamentali in Europa* in Flor e Marcolini, *La tutela dei diritti fondamentali quale*

pronunce adottate dai Giudici di Lussemburgo nell'ultimo decennio sulle questioni attinenti ai diritti scaturenti dall'uso delle nuove tecnologie digitali e al trattamento dei dati degli utilizzatori di tali tecnologie[431]. Attraverso tali decisioni, si è intrapresa la via di un di progressivo e sempre più rigoroso riconoscimento dei diritti connessi all'uso delle nuove tecnologie – grazie anche al ruolo di vero e proprio parametro "costituzionale" assunta dalla Carta di Nizza[432], in un ambito nel quale si registra, invece, una certa inerzia degli Stati membri che, stretti nella morsa tra esigenze securitarie e protezione dei diritti, appaiono sempre più attenti al soddisfacimento delle prime e sempre meno risoluti nella tutela dei secondi[433].

Proprio in quest'ottica va inquadrata, d'altronde, l'altrimenti incomprensibile scelta del legislatore italiano di astenersi da qualsivoglia serio tentativo di regolamentazione della materia della quale si discute, in relazione alla quale è ormai evidente l'urgenza di porre dei limiti all'indiscriminato assoggettamento dei cittadini a forme più o meno intense di vigilanza occulta.

Da un lato, la mancanza di vincoli di qualunque tipo alla realizzazione di pratiche investigative massimamente incidenti sui diritti fondamentali non impedisce – anzi sembra incentivarlo – il ricorso a simili attività, che rimangono sbrigliate da qualsiasi criterio[434]. Dall'altro, «si evita di introdurre uno strumento investigativo così pericoloso per la *privacy* per non perdere il consenso dell'opinione pubblica»[435]. In questo modo, si

---

limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale, Giappichelli, 2022, 5 ss.

[431] Vedi le già citate Corte Giust., 8 aprile 2014, Digital Rights Ireland vs Minister for Communications e a., C-293/12 e C-594/12; Corte Giust., 13 maggio 2014, Google Spain SL e Google Inc. vs Agencia Española de Protección de Datos (AEPD), C-131/12; Corte Giust., 6 ottobre 2015 Schrems vs Data Protection Commissioner, C-362/14; Corte Giust., 21 dicembre 2016, Tele2 Severige e Watson e a., C – 203/15 e C – 698/15; Corte Giust., 2 ottobre 2018, Ministerio Fiscal, C-207/16; Corte Giust., 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18.

[432] In tal senso, BRONZINI, *La Carta dei diritti dell'Unione europea come strumento di rafforzamento e protezione dello Stato di diritto*, in *Pol. dir.*, 2016, 1-2, 16 ss. Si veda anche BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della* privacy, in *Giur. cost.*, 2016, 1, 299, che evidenzia l'attenzione dell'ordinamento dell'Unione Europea al tema della tutela dei dati personali e il rilievo assunto dalla Carta di Nizza nelle decisioni relativa alla legittimità della normativa derivata dell'Unione Europea.

[433] Nell'attuale scenario politico, una maggiore attenzione alla tutela dei diritti, con particolare riferimento alla protezione della vita privata, a scapito delle esigenze securitarie apparirebbe impopolare. Da questo punto di vista, per un organo giurisdizionale quale la Corte di Giustizia appare più agevole assumere posizioni di maggiore rigore nella tutela dei diritti, non subendo le ripercussioni politiche cui sono esposti i governi nazionali. Infatti, come osserva BRONZINI, *La Carta dei diritti dell'Unione europea*, cit., 16, la Carta di Nizza opera più sul piano giudiziario che su quello di indirizzo politico.

[434] Complice anche la giurisprudenza che, come si è visto finora, ha assunto posizioni per lo più lassiste in materia. Cfr. par. 2 ss., cap. 3.

[435] DANIELE, *Contrasto al terrorismo e captatori informatici*, in *Riv. dir. proc.*, 2017, 2, 404.

consegue il duplice obiettivo di non limitare in maniera significativa il ricorso a strumenti che, per quanto invasivi, sono caratterizzati da elevatissima efficienza investigativa e, al contempo, di non indisporre l'opinione pubblica, che non sarebbe certamente galvanizzata dalla prospettiva di una potenziale sottoposizione ad attività di controllo e sorveglianza "a tappeto".

Un simile atteggiamento risulta particolarmente criticabile anche in quanto è suscettibile di avere alcune ripercussioni sistemiche negative, tra cui quella di generare un progressivo appiattimento verso il basso della tutela effettiva dei diritti fondamentali. Tanto non dissimilmente da quanto accade con il fenomeno della legislazione emergenziale – che, come è stato rilevato[436], tende poi a stabilizzarsi nel sistema perdendo l'originario carattere di provvisorietà; solo che, singolarmente, in questo caso è proprio l'inerzia del legislatore a regolare la materia – evidentemente determinata da un'ottica di *laissez-faire* del tutto incompatibile con quello che sarebbe il fisiologico approccio alla tematica dei diritti fondamentali – a determinare il preoccupante appiattimento di cui si è detto.

Il quadro è aggravato dalle ripercussioni che tale inerzia è suscettibile di comportare sulla giurisdizione. In conseguenza della mancanza di una cornice regolatoria di certe attività, «questa si è ormai spinta al di fuori del confine del controllo e della moderazione del conflitto sociale, per inoltrarsi nei territori della mediazione e della regolazione di quel conflitto. E per prendere, nella regolazione, sempre più estesamente luogo del legislatore politico; poiché questo a sua volta recede, incapace di decisioni forti, univoche e sufficientemente stabili»[437].

La chiave di volta sembra doversi rinvenire proprio nella fisionomia e nel contenuto dell'auspicabile intervento normativo in materia.

Sono certamente praticabili soluzioni legislative che, perseguendo un adeguato bilanciamento degli interessi in campo, consentano di porre fine alla strisciante violazione dei diritti fondamentali dei singoli e, al contempo, di non ingenerare forme di "rottura sociale" dovute alla non accettazione, da parte dei cittadini, di una normativa

[436] STAIANO, *Diritto alla riservatezza e potere pubblico, in Federalismi.it*, 2017, 17, 4.

[437] Ancora, STAIANO, *Diritto alla riservatezza*, cit., 25, di cui vale la pena riportare testualmente le ulteriori, assolutamente condivisibili, osservazioni per le quali «nessun diritto fondamentale può essere lasciato nelle mani di un'aristocrazia giudiziale – oggi necessariamente multilivello – che decida essa stessa sui confini del proprio potere, sostanzialmente libera da vincoli normativi. E da questa posizione esclusiva decida sul bilanciamento tra libertà e sicurezza. Le politiche, infatti, spettano a coloro sulle cui libertà esse incidono, e alla decisione di chi ne sia investito nei modi della rappresentanza».

che consenta di sottoporli a un controllo tanto penetrante, con la conseguente perdita del consenso politico che ne conseguirebbe.

Si potrebbe finanche scomodare la teoria del contratto sociale[438] per desumerne che la rinuncia, da parte dei cittadini, alle sfere più interne delle loro libertà e dei loro diritti fondamentali (quali sono quelle della riservatezza coincidenti con l'aspettativa a non subire forme di controllo massivo e continuativo ad opera del potere pubblico) non può che fondarsi su una corrispettiva esigenza di tutela di altri diritti a fronte di minacce percepite come estremamente gravi. Ma una simile conclusione si imporrebbe anche in forza del richiamo, oltre che al buon senso, alla proporzione e alla ragionevolezza che dovrebbero ispirare l'azione legislativa ogniqualvolta essa incida su diritti fondamentali. Se così è, non pare peregrino avanzare la proposta che un mezzo di ricerca della prova come quello di cui si discute possa essere adoperato solo a fronte dell'esigenza di accertamento e repressione non già di qualsiasi forma di criminalità grave, ma solo di quelle forme di criminalità gravi suscettibili di scuotere in maniera consistente e particolarmente allarmante l'ordine pubblico e la sicurezza dei cittadini. Ciò in quanto è solo dinanzi a simili pericoli che può ragionevolmente presumersi che un consociato sia disposto a cedere una così ampia "fetta" delle sue libertà e dei suoi diritti fondamentali. In altre parole, intanto uno strumento come quello di cui si discute dovrebbe considerarsi legittimo in quanto il suo uso sia assolutamente eccezionale. In tale caratteristica dovrebbe risiedere il punto di equilibrio di un bilanciamento di interessi che possa dirsi appropriato in un ordinamento democratico.

Tale prospettiva sembra caldeggiata dalla stessa giurisprudenza europea in materia di vigilanza occulta dei cittadini, soprattutto quando a venire in rilievo sia il ricorso a tecniche di sorveglianza dei singoli nell'ambito della giustizia penale. In tale ambito, si impone agli Stati il compimento di uno sforzo proiettato alla ricerca di un equilibrio ragionevole tra le varie istanze coinvolte, viste le incredibili potenzialità intrusive dei nuovi mezzi tecnologici di investigazione penale. Aspetto, quest'ultimo, che la Corte europea dei diritti dell'uomo sembra cogliere perfettamente laddove evidenzia che «*the*

[438] Come noto, la teoria in questione postula che un individuo in una società rinunci ad alcune delle sue libertà e si sottometta all'autorità di un ente di controllo in cambio della protezione dei suoi diritti e della sua sicurezza. Nucleo essenziale di tale paradigma è il consenso individuale. Si vedano, in generale, HOBBES, *Leviathan*, Penguin Classics, 1982; ROUSSEAU, *The basic political writings*, Hackett Publishing Company, 1987; HUME, *Essays, moral, political, and literary*, Eu-gene f. Miller, 1987.

protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests […] The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard»[439].

In buona sostanza, quando si tratta dell'adozione, da parte dello Stato, di misure di sorveglianza segreta dei cittadini nell'ambito delle attività di *law enforcement* i parametri della proporzionalità ricavabili dalla disciplina convenzionale devono essere applicati in maniera quanto mai rigorosa, viste le evidenti ricadute di simili pratiche sull'effettiva tenuta dell'ordine democratico e sulla fiducia che i cittadini ripongono nelle istituzioni quanto a protezione dei diritti afferenti alla loro sfera più intima. Ne deriva che neppure in nome della lotta allo spionaggio o al terrorismo lo Stato è legittimato ad adottare qualsivoglia misura ritenga opportuna, dovendo pur sempre prevedere garanzie adeguate ed effettive contro i possibili abusi: la sorveglianza segreta dei cittadini è tollerabile solo nella misura in cui sia strettamente necessaria alla salvaguardia delle istituzioni democratiche[440].

Sulla base di tale premessa può passarsi all'individuazione dei lineamenti essenziali della categoria giuridica della cui possibile introduzione si discute. Quanto si è appena detto, infatti, ha importanti riflessi sulle garanzie antecedenti allo svolgimento dell'atto investigativo, con particolare riferimento alla selezione delle fattispecie per cui lo stesso può disporsi.

9. Le garanzie antecedenti, contestuali e successive all'esecuzione della misura.

Si è già anticipato che i molteplici punti di contatto esistenti tra l'*online surveillance* e la categoria, delineata nel capitolo precedente, della perquisizione e del sequestro *online* suggeriscono di delineare per la prima un reticolo di garanzie che abbia quale generale impalcatura quella già tracciata con riferimento al succedaneo istituto antecedentemente analizzato. Da un punto di vista tecnico, infatti, coincidono non solo gli strumenti

[439] Corte e.d.u., 4 dicembre 2008, app. n. 30562/04, Marper vs Regno Unito. Cfr. anche Corte e.d.u., 29 giugno 2006, app. n. 54934/00, Weber e Saravia vs Germania.
[440] Corte e.d.u., 6 settembre 1978, app. n 5029/71, Klass e altri vs Germania.

adoperati per la realizzazione dell'una e dell'altra attività, ma anche le operazioni informatiche realizzate sul dispositivo e finalizzate all'acquisizione dei dati in esso contenuti, con l'unica differenza che, nel caso di *online surveillance*, sarà consentito altresì l'accesso alle periferiche dello strumento informatico. Per quanto concerne, poi, il grado di invasività delle attività in questione, la ricognizione precedentemente operata relativamente ai beni giuridici incisi dalle due misure consente di collocarle in un ideale crescendo, senza soluzione di continuità, di intrusione nelle prerogative dei singoli coinvolti nell'attività di ricerca della prova. Conclusione, questa, che non pare contraddetta dal fatto che si sia operata una precisa distinzione in merito ai diritti fondamentali lesi dalle due tipologie di attività, atteso che, come si è visto, la più grave misura dell'*online surveillance* incide su beni giuridici che sono stati ricavati proprio a partire da una lettura aggiornata dei diritti costituzionali incisi anche dalla perquisizione e dal sequestro *online*. Nel delineare il possibile statuto di tutele connesso all'esecuzione della misura, pertanto, si richiameranno molte delle considerazioni già svolte nei precedenti paragrafi 4 e seguenti del capitolo 3 e, ovviamente, devono a maggior ragione intendersi richiamati i principi espressi dalla giurisprudenza europea in materia di misure incidenti sul diritto alla vita privata analizzai nel capitolo precedente[441].

Questo, ovviamente, non significa che non siano opportuni, e, anzi, assolutamente necessari, alcuni adattamenti. Al maggior grado di intrusività dell'attività oggetto di analisi in questa sede deve corrispondere uno statuto di tutele più rigido che – come anticipato – dovrebbe altresì essere improntato al principio della stretta eccezionalità del ricorso alla misura.

A questo proposito, anzi, occorre ulteriormente segnalare come l'adozione e la conseguente trasposizione, sul piano normativo, di tale principio è suggerita non solo dalle argomentazioni di carattere politico-normativo cui si è fatto riferimento nel paragrafo precedente, ma anche dalla stessa fisionomia dello strumento in questione, quanto meno laddove si aspiri alla messa a punto di una disciplina che possa dirsi rispettosa del principio di proporzionalità. Si vuole segnalare, detto altrimenti, che connaturato allo strumento in oggetto è il rischio che lo stesso venga, nella prassi

[441] Cfr. cap. 3, par. 4.1.2.

applicativa, ad essere adoperato in una logica e con modalità meramente esplorative. Tanto in un duplice senso.

Per un verso, tale potente mezzo intrusivo potrebbe essere sfruttato per la ricerca indiscriminata di elementi attinenti a un reato precedentemente commesso pur in assenza di qualsivoglia rapporto pertinenziale tra quest'ultimo, il dispositivo informatico e il suo contenuto. Trattasi di un aspetto che, invero, caratterizza altresì il contiguo strumento analizzato nel capitolo precedente. Nel caso di specie, però, tale rischio si esacerba in ragione del fatto che all'acquisizione di elementi preesistenti all'intrusione del dispositivo si somma l'acquisizione di dati futuri.

Sotto altro profilo, i connotati intrinsecamente esplorativi dell'attività in questione potrebbero manifestarsi altresì nell'impiego dello strumento, oltre che al fine di rinvenire elementi conoscitivi utili per l'indagine in corso e per l'eventuale, futuro processo, anche per l'acquisizione di *notitiae criminis*[442]. Un'attività di questo genere sarebbe senz'altro da reputarsi vietata, ma non v'è dubbio che, nella prassi, il rischio di abusi sia più che concreto.

Ebbene, le criticità appena segnalate, rinvenibili anche nel caso di "mera" perquisizione e sequestro *online*, sono in quel contesto parzialmente attenuate dalla circostanza che la ricerca è caratterizzata dalla istantaneità dell'accesso e dalla limitazione dei dati acquisibili a quelli preesistenti nel dispositivo. Tanto, almeno in alcuni casi, consente di stabilire, pur con le criticità già evidenziate, il nesso di pertinenzialità che dovrebbe intercorrere tra la ricerca effettuata e il reato oggetto di accertamento e di rispettare, conseguentemente, il principio di necessaria proporzionalità della misura. Nel caso di specie, invece, tale nesso è destinato a sfumare fino a quasi scomparire[443], in ragione del fatto che gli elementi acquisiti in conseguenza dello svolgimento di un'attività di sorveglianza perdurante su così ampia scala non sono predeterminabili. Si tratta di un aspetto che avvicina, in qualche modo, la misura in questione alle intercettazioni di comunicazioni. Solo che, in questo caso, i rischi sono esponenzialmente maggiori in

[442] Prassi, quest'ultima, che la Corte di cassazione ha da tempo "bollato" come illegittima tanto con riferimento all'attività di sequestro, quanto con riguardo a quella di perquisizione. Si vedano, in tal senso, Sez. I, 16 febbraio 2007, n. 25755, Pomarici, in *Guida dir*., 2012, 79; Sez. VI, 31 ottobre 2007, n. 40380, Sarzanini, in *Cass. pen.*, 2008, 4276; Sez. IV, 17 aprile 2012, n. 19618, Ryanair, in *Cass. pen*., 2013, 1523.

[443] Nel senso che, nelle indagini informatiche, il test di proporzionalità tradizionalmente inteso non sia replicabile in ragione del fatto che prima si acquisisce il contenuto informatico e solo in un secondo momento lo si analizza, PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale,* in *Proc. pen. e giust*., 2020, 2, 301 ss.

ragione del carattere polifunzionale del controllo acquisito sul dispositivo, finalizzato a sorvegliare ogni singolo aspetto – e non solo quello attinente alle comunicazioni – della vita del suo utilizzatore.

Da questo punto di vista, devono senz'altro richiamarsi le considerazioni già spese nel capitolo precedente a proposito dell'esigenza di introdurre una regola che imponga al giudice che autorizza la misura l'obbligo di esplicitare il risultato probatorio tenuto di mira[444]; al contempo, però, non può omettersi di rilevare il rischio che anche una simile soluzione si riveli strutturalmente insufficiente a garantire un adeguato livello di tutela dei diritti fondamentali coinvolti e, in definitiva, la concreta proporzionalità della misura. La circostanza che il giudice debba indicare il risultato probatorio atteso dal suo svolgimento non toglie che, per le sue stesse caratteristiche operative, la misura in questione consentirà di apprendere e riversare nel procedimento una quantità potenzialmente sterminata di informazioni sull'utilizzatore del dispositivo bersaglio, molte delle quali del tutto impertinenti all'indagine in corso.

Allo stesso tempo, soluzioni come quella di imporre al giudice l'obbligo di procedere alla previa individuazione del concreto ambito applicativo della misura – come quella invalsa nel sistema spagnolo, che sarà oggetto di analisi critica nel prossimo capitolo – sembrano anch'esse insuscettibili di risolvere in maniera strutturale il problema della fisiologica tendenza di strumenti investigativi come quello in argomento a operare alla stregua di vere e proprie reti di pesca a strascico nella vita dei soggetti incisi da tali misure. Tanto si sostiene non solo in forza delle considerazioni critiche che saranno articolate in quella sede e che devono intendersi in questa richiamate[445]; ma altresì in ragione del fatto che, stanti le potenzialità operative dello strumento in questione, c'è da dubitare che le procure improntino la loro azione a un pur auspicabile *self-restraint*. Il dibattito che da anni imperversa nel nostro ordinamento in ordine all'eccessivo ricorso alle intercettazioni nel corso delle investigazioni penali lo dimostra.

Ne consegue che anche per tali ragioni – oltre a quelle di carattere più squisitamente politico-normativo cui si è fatto prima riferimento – assume peculiare rilievo la selezione delle fattispecie di reato per l'accertamento delle quali è possibile autorizzarne

[444] Il riferimento è alla già precedentemente commentata funzionalizzazione della restrizione, caldeggiata da DI BITONTO, *Lungo la strada della riforma della disciplina delle intercettazioni*, in *Cass. pen.*, 2009, 1, 18.

[445] Cfr. cap. 5, par. 2.3.1.

il compimento. Tali fattispecie devono essere limitate a una cerchia molto ristretta di delitti suscettibili di squassare in maniera significativa l'ordine pubblico o la sicurezza pubblica, come quelli connessi al terrorismo o le forme più gravi di criminalità organizzata[446]. Tanto, però, con l'avvertenza, con riferimento a quest'ultima formula, che basilari esigenze di legalità imporrebbero una selezione ed elencazione accurata delle fattispecie associative rilevanti, essendo esclusa la possibilità di procedere a una enunciazione del precetto in termini generali. In altre parole, non può mutuarsi la nozione di "criminalità organizzata" elaborata dalla giurisprudenza di legittimità, ad esempio, in materia di ricorso al captatore informatico per la realizzazione delle intercettazioni tra presenti[447], anche perché trattasi di una nozione tanto vaga che è concreto il rischio che finisca per inglobare qualsivoglia reato associativo.

Per quanto concerne, invece, l'aspetto relativo al *fumus* che deve reputarsi sussistente – e adeguatamente motivarsi – per l'autorizzazione della misura, possono richiamarsi le considerazioni già svolte nel precedente par. 4.2. del cap. 3, ove si è evidenziato che lo stesso dovrebbe coincidere, quanto meno, con i gravi indizi di reato richiesti in materia di intercettazioni. Sul punto, però, non sembra peregrino osservare che la esponenzialmente maggiore intrusività della misura – unita alle difficoltà, già segnalate, nell'accertamento del nesso di pertinenzialità tra l'attività di ricerca eseguita e il reato oggetto di accertamento – suggerirebbero di ricomprendere tra i possibili bersagli della stessa i soli soggetti sospettati della commissione del reato, con l'esclusione, dunque, dei terzi.

Ancora in materia di garanzie antecedenti, anche in questo caso il ricorso allo strumento in questione dovrebbe essere limitato ai soli casi in cui sia assolutamente necessario per la prosecuzione delle indagini o per l'accertamento dei fatti. Ciò significa che la adozione della misura di sorveglianza non potrebbe dipendere da mere opzioni strategiche della procura, ma dovrebbe essere subordinata alla costatazione dell'inutilità

---

[446] Per l'osservazione secondo la quale «per quanto l'adozione delle garanzie previste dagli artt. 266 s. c.p.p. sarebbe apprezzabile, risulterebbe però irragionevole permettere le perquisizioni on-line in relazione agli stessi reati in merito ai quali sono consentite le intercettazioni telematiche: ovvero i reati elencati dall'art. 266 c.p.p., nonché «i reati commessi mediante l'impiego di tecnologie informatiche o telematiche». È un insieme eterogeneo di illeciti di diversa natura e gravità, in rapporto a molti dei quali le perquisizioni on-line risulterebbero uno strumento sproporzionato» DANIELE, *Contrasto al terrorismo*, cit., 403, con la precisazione che con il termine "perquisizione online", l'autore fa riferimento anche alle forme di sorveglianza in tempo reale.

[447] Sez. un., 28 aprile 2016, n. 26889, Scurato, cit.

o della non sufficienza degli altri mezzi a disposizione per il raggiungimento delle legittime finalità della medesima.

Da ultimo, per quanto concerne l'autorità competente all'adozione dell'atto, è evidente come le ragioni che, con riferimento alla perquisizione e al sequestro *online*, hanno militato per l'esigenza di affidare al giudice il controllo previo all'esecuzione dell'atto siano ancora più forti nel caso di specie. Non possono, pertanto, che richiamarsi le considerazioni già svolte precedentemente.

Per quanto riguarda le garanzie connesse all'esecuzione della misura valgono i rilievi già svolti con riferimento allo statuto della perquisizione e del sequestro *online*[448]. Non v'è dubbio, pertanto, che la legittimità dell'atto realizzato e la spendibilità processuale dei relativi risultati conoscitivi vada subordinata alla stretta osservanza delle regole tecniche di esecuzione delle operazioni, a partire da quella per la quale è necessario il ricorso a *software* che consentano di tracciare in maniera precisa le operazioni compiute e, dunque, di verificare *ex post* l'affidabilità del risultato probatorio ottenuto.

Qualche considerazione ulteriore, invece, merita la necessaria individuazione di un limite temporale dell'attività di sorveglianza in tal modo realizzata. Stante l'alto valore degli interessi in gioco, l'elevato rischio di abuso della misura per il perseguimento di finalità meramente esplorative e il forte impatto della stessa sui diritti fondamentali coinvolti, il rispetto del principio di proporzionalità imporrebbe di individuare limiti temporali contingentati[449], oltre che l'esclusione radicale di un sistema – simile a quello ora vigente in materia di intercettazioni – di proroghe sostanzialmente *ad libitum*[450]. Tanto, peraltro, senza considerare come il contingentamento della durata massima della misura avrebbe l'indiretto effetto di limitare il quantitativo di dati – potenzialmente ingentissimo – acquisibili tramite la sua messa in atto, con la conseguenza, positiva, non solo di contenere l'intrusione nella sfera privata del singolo, ma altresì di non comprimere eccessivamente l'esercizio del diritto di difesa che, nella materia che occupa, poggia anche sulla effettiva possibilità di analizzare l'intera congerie dei dati

[448] Cfr. par. 4.3., cap. 3.

[449] In termini, NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 148.

[450] Da questo punto di vista, la giurisprudenza della Corte europea dei diritti dell'uomo sembra assestata su posizioni eccessivamente blande, come quella secondo la quale la questione della complessiva durata delle misure di intercettazione può essere lasciata alla discrezione delle autorità competenti a emettere e prorogare i decreti di intercettazione, purché siano previste adeguate garanzie, quali la chiara indicazione nel diritto interno del termine del decreto di intercettazione, delle condizioni che consentono di prorogarlo e delle circostanze in cui deve essere revocato, cfr. Corte e.d.u., 4 dicembre 2015, Zakharov c. Russia, app. no. 47143/06.

raccolti nei tempi – talvolta molto ristretti – utili per l'esplicazione delle varie scelte processuali che caratterizzano l'incedere del procedimento.

Proprio a questo proposito, e passando al tema delle garanzie successive all'esecuzione della misura, occorre evidenziare che, se possono senz'altro richiamarsi, anche in questo caso, le considerazioni già spese nel precedente par. 4.4. del cap. 3 in merito all'istituto della *online search*[451], pare invece indispensabile mettere a punto una disciplina specifica in materia di termini difensivi per l'analisi del materiale raccolto[452]. Come noto, l'attuale disciplina codicistica non prevede alcuna regola volta a parametrare tali tempistiche alla mole dei dati riversati nel procedimento per effetto di alcuni mezzi di ricerca della prova. L'esempio più lampante è dato dalla disciplina delle intercettazioni, suscettibile di ingenerare eccessive compressioni del diritto di difesa in tutti quei casi in cui, a fronte del riversamento, nel fascicolo procedimentale, di un numero talvolta smisurato di captazioni, la difesa si trovi nella sostanziale impossibilità di procedere all'analisi dell'intero compendio delle medesime in ragione della ristrettezza dei tempi entro i quali, a pena di decadenza, è necessario operare determinate scelte processuali[453]. Neppure potrebbe ovviarsi al problema con meccanismi di selezione del materiale raccolto, in vista della sua successiva messa a disposizione del giudice, da parte dell'organo inquirente. Non solo in quanto lo stesso avrebbe, comunque, l'obbligo di far confluire nel fascicolo procedimentale tutti i risultati delle indagini compiute, ma altresì in quanto sarebbe fin troppo facile obiettare a una soluzione di questo tipo che tra i materiali "scartati" ben potrebbero trovarsi elementi favorevoli alla difesa.

A fronte di ciò, l'unica soluzione praticabile pare essere quella, poc'anzi evidenziata, di parametrare i termini difensivi per l'analisi del materiale raccolto alla quantità del medesimo, con l'avvertenza che perché un simile parametro sia obiettivo, dovrebbe essere direttamente relazionato alla durata dell'attività di sorveglianza. Sicché,

---

[451] Il riferimento è, in particolare, alla messa a punto di specifici obblighi informativi, oltre che al sistema dei controlli attivabili a seguito dell'esecuzione della misura e, naturalmente, alla introduzione di specifiche fattispecie di inutilizzabilità per le più gravi violazioni della normativa processuale relativa all'istituto.

[452] Sul punto, cfr. anche le considerazioni di NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, cit., 160.

[453] È il caso, ad esempio, della disciplina vigente in materia di giudizio immediato. Capita fin troppo spesso che, ricevuto il decreto che dispone il giudizio immediato, la difesa si trovi nell'impossibilità analizzare l'intero compendio captativo nel ristrettissimo termine di quindici giorni previsto per la scelta di un rito alternativo.

all'aumentare del tempo del controllo dovrebbero incrementarsi, proporzionalmente, i tempi difensivi per lo studio della documentazione conseguente allo stesso.

Una soluzione di questo tipo, ad esempio, è stata implementata dal legislatore spagnolo nell'ambito della disciplina delle intercettazioni, ove si prevede che, terminate le operazioni, le registrazioni siano messe a disposizione delle parti e che alle stesse sia attribuito un termine al fine di analizzarle e chiedere l'incorporazione alla causa delle intercettazioni di interesse. La legge prevede espressamente che il termine in questione sia stabilito dal giudice in base al volume delle intercettazioni medesime[454].

[454] Art. 588 *ter* i Lecrim.

Capitolo V

UNO SGUARDO COMPARATIVO: LA NORMATIVA SPAGNOLA IN MATERIA DI PERQUISIZIONE E SEQUESTRO DI SISTEMI INFORMATICI DA REMOTO

Sommario: 1. La Ley Organica 13/2015 del 5 ottobre 2015; 1.1. Il diritto al rispetto della vita privata nella Costituzione spagnola (art. 18 CE); 1.2. Principio di legalità e principio di proporzionalità: la necessità di una base legale sufficiente; 2. Le disposizioni comuni in materia di ricorso a mezzi di investigazione tecnologicamente avanzati; 2.1. La riserva di giurisdizione; 2.2. Il principio di specialità; 2.3. Il principio di proporzionalità e la sua trasposizione nel procedimento applicativo della misura; 2.3.1. Pertinenza della misura come necessario presupposto della proporzionalità della stessa: aspetti critici; 2.4. Limiti alla circolazione indiscriminata dei dati: garanzie relative all'utilizzo della prova in altri procedimenti e distruzione dei dati; 3. Il *registro remoto*; 3.1. I beni costituzionali incisi; 3.2. Presupposti applicativi; 3.3. Il procedimento applicativo della misura; 3.4. Dubbi interpretativi; 4. L'agente informatico sotto copertura; 5. Riflessioni conclusive sulla possibile introduzione di istituti di *remote searching* e *remote surveillance* nell'ordinamento italiano.

1. La Ley Organica 13/2015 del 5 ottobre 2015.

Con l'approvazione della Ley Organica 13/2015, del 5 ottobre 2015, il legislatore spagnolo ha introdotto un *corpus* normativo appositamente dedicato alla disciplina dell'insieme delle misure investigative a carattere tecnologico, incidenti su diritti fondamentali costituzionalmente presidiati, suscettibili di essere adottate nel corso delle indagini. Le disposizioni in argomento (corrispondenti agli artt. 588 *bis* a e ss. *Ley de enjuiciamiento criminal*[455]) sono confluite nei Capitoli da IV a X del titolo VIII del Libro II[456] della Lecrim, titolo dedicato alle "Misure di investigazione limitative dei

[455] Trattasi del testo legislativo disciplinante lo svolgimento del processo penale, ovvero del sostanziale corrispettivo del Codice di procedura penale italiano. D'ora in poi, anche "Lecrim".
[456] Il Libro II è dedicato alla fase delle indagini preliminari.

diritti riconosciuti nell'art. 18 della Costituzione"[457] che, come si vedrà più avanti, tutela il diritto al rispetto della vita privata, nelle sue varie accezioni.

L'ampia riforma è stata determinata dalla necessità di adeguare la disciplina processuale penale alle nuove forme di intrusione nella intimità dei singoli rese possibili dall'avanzamento tecnologico, a fronte di una normativa che, risalente al 1882, anno di introduzione della Lecrim, risultava obsoleta e, dunque, inadeguata allo scopo[458]. Oltre a ciò, la novella ha rappresentato l'occasione per riformare la disciplina delle intercettazioni, che – a causa del suo carattere ampiamente indeterminato – aveva condotto alla condanna dello Stato da parte della Corte europea dei diritti dell'uomo in ragione della violazione dell'art. 8 della Convenzione europea dei diritti dell'uomo[459].

Il vecchio art. 579[460] Lecrim, infatti, si limitava ad ammettere il ricorso all'intercettazione delle comunicazioni, con risoluzione motivata del giudice, in presenza di indizi tali da far supporre che in tal modo fosse possibile scoprire o comprovare fatti o circostanze importanti per la causa. Non erano, per contro, previste limitazioni in relazione alle fattispecie per le quali potesse ricorrersi alla misura né, tanto meno, limiti di durata della stessa. Allo stesso modo, non si prevedevano norme

---

[457] Il titolo, dunque, comprende anche la disciplina relativa a misure investigative a carattere non tecnologico, come la perquisizione e il sequestro nel domicilio e l'acquisizione e l'apertura della corrispondenza scritta e telematica (cfr. artt. 545 ss. Lecrim).

[458] BALLESTEROS, *Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la LO 13/2015,* in *Anuario Jurídico y Económico Escurialense,* LII, 2019, 181. Ciò, peraltro, a detta della dottrina, non aveva impedito certe interpretazioni "largheggianti" della giurisprudenza, tendenti a ricondurre agli istituti tradizionali nuove tipologie investigative a carattere tecnologico, sfruttando il carattere particolarmente ampio delle relative formulazioni normative. Si vedano, con riferimento alla perquisizione e sequestro informatici, le considerazioni di CABEZUDO RODRÍGUEZ, *Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal,* in *Las reformas del proceso penal, I Jornada del Boletín del Ministerio de Justicia*, LXX, n. 2186, febbraio 2016, 39 ss., che evidenzia come, in alcune sentenze, la legittimità di perquisizioni e sequestri informatici era stata affermata sulla scorta del richiamo alla disciplina relativa all'accesso e all'apprensione di documenti, di cui agli artt. 573 ss. Lecrim; in termini, HUETE NOGUERAS, *La regulación de las medidas de investigación tecnológica. Análisis de los aspectos referentes a la incorporación al proceso de datos electrónicos de tráfico o asociados*, in *Revista del Ministerio Fiscal*, n. 2, 2016, 59.

[459] Cfr. Corte e.d.u., 30 luglio 1998, Valenzuela Contreras contro Spagna, app n. 27671/95; Corte e.d.u., 18 febbraio 2003, app. n. 12218/09, Prado Bugallo contro Spagna. Per una esaustiva ricostruzione delle pronounce della Corte di Strasburgo sulla legittimità convenzionale della disciplina spagnola, si veda BACHMAIER WINTER, *Telephone tapping in the Spanish Criminal Procedure: An Analysis from the European Court of Human Right's Perspective*, JURA, 2007/2 (University of Pécs), 7-15.

[460] In particolare, la norma prevedeva che fosse possibile «*la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa*», aggiungendo che «*de igual forma, el juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogables por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos*».

relative al procedimento di trascrizione delle conversazioni intercettate, alle precauzioni da osservare per assicurare l'integrità e la completezza delle registrazioni effettuate, al diritto di accesso ai relativi atti da parte della difesa, alle condizioni e alle finalità del controllo della difesa medesima e del giudice in merito alla legittimità della misura e del risultato conoscitivo ottenuto. La disciplina nazionale in materia, dunque, risultava strutturalmente inadeguata al soddisfacimento del requisito della proporzionalità della restrizione del diritto fondamentale richiesto dalla disciplina convenzionale.

Anche i tentativi della giurisprudenza costituzionale, che era più volte intervenuta al fine di colmare tale vuoto legislativo, erano risultati sostanzialmente vani e insuscettibili di assicurare all'ordinamento spagnolo il livello minimo di conformità alla Convenzione europea dei diritti dell'uomo tale da impedire la condanna dello Stato da parte della relativa Corte.

A partire dal 1999, infatti, il Tribunale Costituzionale spagnolo[461] aveva sposato una linea interpretativa fortemente creativa[462], tracciando esso stesso i presupposti essenziali perché una misura restrittiva del diritto al segreto delle comunicazioni potesse reputarsi corrispondente al canone della proporzione. Tanto sul presupposto che, nonostante la mancanza di una base legale sufficiente, fosse precipuo compito del medesimo Tribunale quello di supplire alle insufficienze della disciplina nazionale[463] finché non fosse intervenuta una riforma legislativa[464].

La giurisprudenza costituzionale aveva così avviato un'operazione pretoria di progressiva messa a punto dello statuto di garanzie da rispettare per la legittimità di una misura restrittiva di uno dei diritti tutelati dall'art. 18 Cost., individuando essa stessa le regole che sarebbero state, sedici anni dopo, recepite dal legislatore con la riforma del

---

[461] STC, 5 aprile 1999, n. 49; in termini, STC, 30 gennaio 2006, n. 26.

[462] CABEZUDO RODRÍGUEZ, *Ciberdelincuencia e investigación criminal*, cit., 24. Cfr. anche HUETE NOGUERAS, *La regulación de las medidas de investigación tecnológica*, cit., 59.

[463] Lo stesso punto III del Preambolo alla Ley Organica 13/2015 riconosce espressamente tale *deficit* normativo. In esso si legge che «*por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias supranacionales han recordado*».

[464] Si legge nella pronuncia, infatti, che la costatazione di un patente vuoto normativo «*no resuelve por sí sola la cuestión planteada ni conduce indefectiblemente a la declaración de la lesión del derecho* […] *no puede afirmarse que el Derecho interno no respete las exigencias derivadas del art. 8 CEDH, sino, por el contrario, que en ese nuevo escenario de determinaciones jurisprudenciales le corresponderá a este Tribunal suplir las insuficiencias apreciadas en el precepto legal citado hasta que se produzca la necesaria intervención del legislador*».

2015. Come si vedrà più avanti, infatti, le disposizioni comuni alle misure investigative di carattere tecnologico incidenti sul diritto alla vita privata contengono regole e principi sostanzialmente sovrapponibili a quelli enucleati nella traiettoria giurisprudenziale tracciata a partire dalla fine degli anni '90.

Nella pronuncia del 1999, il Tribunale Costituzionale evidenziava come qualsivoglia intrusione in un diritto fondamentale presupponga l'esistenza di una base legale, nel senso che la legge dovrebbe individuare ciascuno dei presupposti e delle condizioni per l'adozione della misura restrittiva. Cionondimeno, evidenziava – non senza una certa dose di contraddittorietà – come, pur in assenza di una base legale, l'intercettazione potesse reputarsi legittima se concretamente disposta nel rispetto di alcuni requisiti minimi suscettibili di assicurarne l'adeguatezza e la proporzionalità, indicati nel provvedimento autorizzativo emesso dal giudice[465].

In tale scenario, il Tribunale Supremo, pur allineandosi alla giurisprudenza del Tribunale Costituzionale, non aveva mancato, in varie pronunce, di rimarcare l'urgenza di una riforma legislativa suscettibile di porre fine allo stato di incertezza giuridica determinato dalla indeterminatezza della disciplina nazionale[466]. Un'accelerazione in tal senso è, con ogni probabilità, derivata da una sentenza del 2014 del Tribunale Costituzionale[467] con la quale si dichiarò vulnerato il diritto al segreto delle comunicazioni in un caso di intercettazione, pur giudizialmente autorizzata, di conversazioni orali di un detenuto, sul presupposto che, nel caso di specie, la carenza di una base legale non fosse colmabile neppure tramite la verifica concreta della sussistenza dei requisiti di proporzione e adeguatezza, mancando *tout court* una

[465] Come si vedrà, trattasi essenzialmente dei medesimi presupposti oggi previsti dalla normativa in materia, a seguito della riforma del 2015, per qualsiasi intrusione con mezzi tecnologici nel diritto al rispetto della vita privata, nelle sue varie componenti. Sinteticamente, si richiedeva all'organo giudiziario di esternare, nella motivazione, i dati o i fatti oggettivi suscettibili di assurgere a indizi dell'esistenza del reato e del collegamento della persona o delle persone indagate con esso, oltre che di determinare con precisione: il numero o i numeri di telefono e le persone sottoposte a intercettazione, la durata della captazione, il soggetto incaricato di eseguirla, le modalità e le tempistiche con le quali il giudice doveva essere informato degli sviluppi dell'attività captativa. Tali requisiti motivazionali si estendevano, inoltre, anche alla eventuale proroga, precisandosi che, prima di concederla, il giudice doveva conoscere gli esiti dell'attività intercettiva già realizzata, spiegando le ragioni che legittimavano la continuazione dell'intervento.

[466] Vedi STS, 29 de maggio 2007, n. 487, che, in termini decisamente aspri, metteva in evidenzia come né le condanne della Corte europea dei diritti dell'uomo né i reiterati appelli delle corti nazionali avevano, infine, sortito l'effetto sperato di un intervento legislativo suscettibile di porre termine alla carenza legale in materia.

[467] STC, 22 settembre 2014, n. 145.

previsione normativa dalla quale fosse possibile desumere la ammissibilità di un'intercettazione di comunicazioni di un soggetto detenuto[468].

La gestazione, pur decisamente lunga, della riforma ha condotto all'approvazione di un apparato normativo complesso e, almeno nelle intenzioni del legislatore[469], completo in materia di misure investigative di carattere tecnologico.

Tale *corpus normativo* è strutturato in maniera peculiare: a una prima parte (corrispondente al Capitolo IV del Titolo VIII del Libro II della Lecrim) in cui si prevedono le disposizioni comuni alle misure di investigazione tecnologica impattanti sui diritti fondamentali di cui all'art. 18 Cost. ("*Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos*"), corrisponde una seconda parte (Capitoli da V a IX) in cui sono previste, per ciascuna delle misure investigative applicabili, regole specifiche che vanno ad aggiungersi alla disciplina generale.

La *ratio* sottesa alla messa appunto di una simile struttura normativa può rinvenirsi nell'intuizione della assimilabilità delle misure tecnologiche di indagine quanto a impatto sui diritti fondamentali, che conduce alla logica conseguenza della necessità di un'impalcatura di garanzie minime che devono essere applicate a prescindere dalle peculiarità e dal grado di invasività più o meno maggiore delle singole misure.

Così, come si diceva, il Capitolo IV è dedicato alle disposizioni comuni[470], contenenti, anzitutto, quelli che vengono denominati "principi rettori" (art. 588 *bis* s Lecrim), tra cui spicca, *in primis*, la riserva di giurisdizione, con la conseguenza della necessaria autorizzazione giudiziale previa all'esecuzione della misura, salve alcune specifiche

[468] Nella sentenza si precisava, in particolare, che la logica fatta propria dalla giurisprudenza costituzionale e di legittimità a partire dal 1999 – in virtù della quale la mancanza dei presupposti legali per disporre l'intercettazione veniva colmata da una verifica di adeguatezza e proporzione svolta caso per caso sulla base dell'apparato motivazionale del provvedimento autorizzativo – non era replicabile nel caso in questione attesa l'inesistenza di una norma che regolasse – ammettendola – l'intercettazione delle conversazioni tra detenuti all'interno della struttura detentiva.

[469] Come si vedrà, in realtà, proprio la disciplina relativa all'accesso, occulto e da remoto, in dispositivi informatici è quella che pone i maggiori dubbi quanto a effettivo ambito applicativo e limiti dell'ingerenza realizzata.

[470] La disciplina in questione sarà specificamente analizzata nei par. 2 ss.

disposizioni che, in relazione ad alcune misure, legittimano il pubblico ministero e la polizia giudiziaria ad agire in via d'urgenza, salvo la necessaria convalida successiva del giudice[471].

Oltre alla riserva di giurisdizione, acquisisce particolare rilievo l'esplicito richiamo ai principi di specialità, idoneità, necessità e proporzione della misura, tutti convergenti nel senso del carattere strettamente eccezionale delle restrizioni previste dagli articoli seguenti.

Chiudono le disposizioni comuni le norme relative al procedimento applicativo delle misure – a partire dal contenuto minimo della richiesta di applicazione della misura (avanzata dal pubblico ministero o dalla polizia giudiziaria) e della risoluzione giudiziale autorizzativa – che rappresentano effettiva concretizzazione dei principi generali sopra richiamati. Si prevedono, quindi, norme comuni in materia sottoposizione a segreto dell'attività svolta, di durata, cessazione e proroga delle misure, di controllo da parte del giudice, di impatto sui diritti dei terzi, di utilizzazione dei risultati acquisiti in altri procedimenti e, infine, di distruzione del materiale probatorio acquisito quando la sua conservazione non sia più necessaria. Ancorché, poi, la disposizione sia stata inserita a valle delle norme relative alle singole misure investigative, rientra tra le regole di generale applicazione anche quella di cui all'art. 588 *octies* Lecrim, che prevede il cosiddetto ordine di conservazione dei dati. In base a tale norma, il pubblico ministero e la polizia giudiziaria possono richiedere a qualunque persona fisica o giuridica la conservazione e la protezione, per un periodo massimo di novanta giorni prorogabili una sola volta, di dati e informazioni concrete inclusi in un sistema informatico di cui abbiano la disponibilità fino all'ottenimento dell'autorizzazione giudiziale necessaria per la loro acquisizione.

I Capitoli successivi al IV, invece, sono dedicati alle singole misure investigative a carattere tecnologico[472], a partire dalla disciplina relativa alle intercettazioni telefoniche

[471] Ad esempio, in materia di pedinamento e localizzazione, l'art. 588 *quinquies* b Lecrim autorizza la polizia giudiziaria ad intervenire pur in mancanza della previa autorizzazione del giudice quando sussistono ragioni di urgenza che facciano ragionevolmente temere per il buon esito delle indagini ove non sia immediatamente collocato il dispositivo di geolocalizzazione. Peculiare, poi, la disciplina relativa all'intercettazione di intercettazioni: l'art. 588 *ter* d Lecrim consente al Ministro dell'interno e al Segretario di Stato per la Sicurezza, nelle indagini relative ai delitti di banda armata o di terrorismo, di ordinare in via d'urgenza l'esecuzione della misura, salva la successiva convalida da parte del giudice nei tempi contingentati indicati dalla medesima disposizione.

[472] Per una trattazione più approfondita delle singole misure investigative adottabili, si rinvia alla lettura di BALLESTEROS, *Medidas de investigación tecnológica en el proceso penal*, cit., 180 ss.; BUENO DE MATA,

e telematiche[473] (Capitolo V), nell'ambito della quale si attribuisce altresì al giudice la possibilità di autorizzare, oltre che l'acquisizione del contenuto della comunicazione, anche quella dei dati relativi al traffico telefonico e telematico, indipendentemente dal fatto che siano o meno associati a una comunicazione concreta[474]. L'acquisizione dei cosiddetti tabulati telefonici, dunque, può anche rappresentare una misura di carattere, per così dire, accessorio rispetto all'intercettazione, fermo restando che ad essa si può ricorrere anche singolarmente, secondo il disposto dell'art. 588 *ter* j Lecrim. Si prevede, infatti, una specifica normativa in tema di acquisizione di dati conservati da prestatori di servizi[475], oltre che di accesso ai dati necessari per l'identificazione di usuari, terminali e dispositivi di connessione (artt. 588 *ter* k ss. Lecrim)[476].

A seguire, viene delineata la disciplina relativa alla captazione e registrazione di comunicazioni orali ambientali mediante dispositivi elettronici (art. 588 *quater* a ss.

Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, in *Diario La Ley, Nº 8627, Sección Doctrina*, 19 ottobre 2015; CABEZUDO RODRIGUEZ, *Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal*, in AA.VV., *Nuevos horizontes del derecho procesal*, J.M. Bosch Editor, 2016, 541 ss.; LANZAROTE MARTINÉZ, *La nueva regulación de las intervenciones telefónicas y telemáticas: algunas cuestiones claves y otras discutibles*, in *Revista del ministerio fiscal*, 2017, 3.

[473] Trattasi di una disciplina (artt. 588 *ter* a ss. Lecrim) ben più articolata di quella antecedente alla riforma, nella quale, anzitutto, si individuano le fattispecie di reato in relazione alle quali è possibile il ricorso alla misura, precisandosi altresì che i dispositivi intercettati possono essere solo quelli abitualmente o occasionalmente utilizzati dall'investigato (mentre l'intercettazione di un dispositivo di un terzo è possibile solo a date condizioni, indicate nell'art. 588 *ter* c Lecrim). Viene indicato il contenuto minimo del provvedimento autorizzativo, che deve dar conto, in base alle caratteristiche del caso di specie, del rispetto dei requisiti di proporzionalità ed eccezionalità della misura. Infine, vengono dettate specifiche norme in tema di durata dell'intercettazione – che non può essere complessivamente superiore a diciotto mesi – e di controllo delle parti e del giudice in merito alla legittimità della stessa.

[474] Pertanto, tramite specifica autorizzazione – che può inserirsi nel medesimo atto con il quale si dispone l'intercettazione – può prevedersi l'acquisizione dei dati esterni alle comunicazioni intrattenute dall'intercettato, così come di quelli non afferenti a singole interlocuzioni.

[475] Ai sensi dell'art. 588 *ter* e Lecrim, i prestatori di servizi di telecomunicazione e, in generale, di servizi relativi alla società dell'informazione, così come ogni altra persona che in qualunque modo contribuisca a facilitare le comunicazioni attraverso il telefono o qualsivoglia altro mezzo, sono tenuti a collaborare con l'autorità giudiziaria prestando assistenza al fine di consentire la realizzazione delle intercettazioni disposte. Tali soggetti sono, poi, obbligati a conservare il segreto in merito alle attività richieste dalle autorità. Entrambe le obbligazioni, ai sensi del terzo comma dell'articolo, sono penalmente presidiate. Tale disciplina, pur dettata specificamente in materia di intercettazioni, viene richiamata anche in relazione ad altre misure, come nel caso della localizzazione e del pedinamento tramite mezzi tecnici (art. 588 *quinquies* b Lecrim). Uno specifico dovere di collaborazione è, poi, previsto in relazione alla misura del *registro remoto sobre equipos informaticos* all'art. 588 *septies* b Lecrim.

[476] Alcune di queste misure possono essere attuate direttamente dalla polizia giudiziaria, senza autorizzazione del giudice, come accade nel caso di ricorso agli artifici tecnici necessari per consentire l'identificazione degli apparati di telecomunicazione, come il numero IMSI o l'IMEI (cfr. art. 588 *ter* l Lecrim). Trattasi di misure, infatti, di carattere squisitamente tecnico, normalmente prodromiche all'individuazione dei dispositivi da sottoporre alle più invasive attività di vigilanza per le quali è, invece, richiesta l'autorizzazione giudiziale.

Lecrim) che, a differenza di quanto accade nel nostro Paese, possono essere disposte solo se vincolate a comunicazioni che possono aver luogo in incontri concreti tra l'investigato e altre persone e a patto che possa ragionevolmente prevedersi che il ricorso alla misura consenta di apportare all'investigazione dati essenziali e di rilievo probatorio per la ricostruzione dei fatti e l'identificazione del loro autore (art. 588 *quater* b Lecrim). Il Capitolo VII è dedicato alla utilizzazione di dispositivi di captazione delle immagini, di pedinamento e localizzazione, con la precisazione, in relazione a questi ultimi, che la misura può avere una durata non eccedente, proroghe comprese, i diciotto mesi.

Per quanto concerne l'accesso a dispositivi elettronici al fine di vagliarne e, eventualmente, acquisirne il contenuto, la relativa disciplina è contenuta negli artt. 588 *sexies* a ss. Lecrim.

La scelta del legislatore spagnolo è stata, opportunamente, quella di distinguere tra l'accesso palese e "in presenza" al dispositivo (artt. 588 *sexies* a-588 *sexies* b Lecrim) e l'accesso occulto e da remoto (588 *septies* a-588 *septies* c Lecrim), misura, quest'ultima, di particolare interesse per l'oggetto del presente lavoro e alla quale, dunque, si dedicheranno molte delle pagine a venire. Come rilevato dalla dottrina[477], trattasi di una misura dal carattere ampiamente innovativo, fino al 2015 non prevista nel sistema spagnolo né, tanto meno, legittimabile sulla base dell'interpretazione estensiva delle norme in materia di intercettazione o di acquisizione di documenti.

1.1. Il diritto al rispetto della vita privata nella Costituzione spagnola (art. 18 CE).

Come evidenziato nel paragrafo precedente, i capi relativi alle misure investigative a carattere tecnologico sono contenuti nel Titolo VIII del Libro II della Lecrim, dedicato alle misure incidenti sui diritti fondamentali di cui all'art. 18[478] della Costituzione spagnola[479]. Trattasi di una circostanza di estremo rilievo in quanto, come si vedrà nel

[477] BACHMAIER WINTER, *Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015*, in *Boletín del Ministerio de Justicia*, n. 2195, 2017, 6.

[478] L'articolo così recita: «*1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*».

[479] D'ora in poi, anche CE.

prossimo paragrafo, la restrizione di diritti fondamentali costituzionalmente presidiati richiede, nell'ordinamento spagnolo, l'esistenza di una esplicita base legale.

Quella di cui all'art. 18 CE è una norma complessa, che riconosce e garantisce una serie di diritti che, pur dovendosi mantenere concettualmente distinti, sono riconducibili a una matrice unitaria, da rinvenirsi nel diritto al rispetto della vita privata[480]. Così, l'inviolabilità del domicilio e delle comunicazioni e il diritto alla protezione dei dati di carattere personale di cui ai commi 2, 3 e 4 dell'art. 18 CE. non rappresentano mere articolazioni del diritto all'intimità, all'onore e alla propria immagine, ma si atteggiano alla stregua di figure autonome, alle quali – con particolare riferimento all'inviolabilità del domicilio e delle comunicazioni, espressamente dichiarati inviolabili – il legislatore costituente ha inteso accordare una tutela massima, funzionale al libero sviluppo della personalità umana[481].

Il carattere esplicito della tutela accordata alla vita privata e alle sue autonome componenti ha contribuito acché il dibattito in merito ai diritti fondamentali ristretti dalle intrusioni statali nelle prerogative dei singoli scaturenti dall'uso delle nuove tecnologie si sia atteggiato, negli anni passati, in maniera parzialmente distinta da quanto accaduto nel nostro ordinamento. L'aspetto che più di ogni altro vale la pena di rimarcare prima di procedere a una disamina, sia pur sintetica, delle componenti dell'articolo in argomento di maggiore interesse per il presente lavoro è la mancanza di una riflessione dottrinale e giurisprudenziale in merito alla necessità di una lettura evolutiva del domicilio.

Come si è visto nei capitoli precedenti, l'ampliamento del concetto di domicilio tutelato dall'art. 14 della Costituzione italiana, fino a ricomprendere nei suoi confini anche il domicilio informatico alla stregua di un luogo virtuale nel quale si esprime la personalità umana e rispetto al quale il titolare vanta uno *ius excluendi alios*, ha rappresentato una delle soluzioni esegetiche maggiormente condivise al fine di

[480] BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 6.

[481] Si veda SEMPERE RODRÍGUEZ, *Artículo 18: Derecho al honor, a la intimidad y a la propia imagen*, in Alzaga Villaamil, *Comentarios a la Constitución española de 1978*, Edersa, Madrid, 1996, 425, che evidenzia come, in definitiva, l'esistenza di un evidente vincolo concettuale tra le singole disposizioni di cui all'art. 18 Cost. non significa che il diritto all'intimità personale e famigliare riceva esclusivamente una tutela indiretta. Al contempo, però, tale vincolo, da ricondurre anche alla più generale tutela della dignità umana, consente di riconoscere nel rispetto della vita privata un principio di carattere generale che svolge anche un ruolo di ausilio esegetico nella soluzione di eventuali conflitti interpretativi.

inquadrare in una categoria costituzionale esistente le aspettative di tutela dei singoli rispetto all'uso della tecnologia digitale.

Una simile riflessione non ha contrassegnato anche l'ordinamento spagnolo[482], nel quale il riconoscimento esplicito del diritto alla tutela della vita privata – con la conseguente esigenza di una base legale al fine di una sua restrizione – ha reso sostanzialmente superfluo tale dibattito in relazione a tutti quei casi in cui l'intrusione dell'autorità statale nei diritti dei singoli non fosse pianamente riconducibile a una violazione del segreto delle comunicazioni, con la conseguenza dell'applicazione dello statuto di tutele previsto a presidio di quel diritto. Simili intrusioni, infatti, sarebbero comunque riconducibili all'ambito applicativo della più ampia tutela accordata dall'art. 18 CE. Ciò rende particolarmente interessante quanto si vedrà più avanti in merito ai più recenti sviluppi del dibattito dottrinale e giurisprudenziale sul tema dei diritti incisi dalle misure tecnologiche di indagine: la circostanza che la Costituzione spagnola già prevedesse espressamente un ventaglio di tutele sufficientemente ampio per ricomprendere anche le aspettative di riservatezza informatica dei singoli (viepiù in virtù del combinato disposto del comma 1 dell'art. 18 CE – che tutela il diritto all'intimità – e del successivo comma 4 – che attribuisce alla legge il ruolo di limitare l'uso dell'informatica per garantire l'onore e l'intimità personale e famigliare dei cittadini e il pieno esercizio dei loro diritti) non ha impedito l'insorgere, negli ultimi anni, di un dibattito in merito alla necessità di riconoscere l'esistenza di un nuovo diritto costituzionale specificamente tarato sulle caratteristiche delle intrusioni tecnologiche di ultima generazione.

Per comprendere come si è giunti a ciò, pare imprescindibile spendere alcune considerazioni in merito alle tappe che hanno marcato l'evoluzione interpretativa delle componenti dell'art. 18 CE più rilevanti ai fini della presente analisi, a partire dal diritto

[482] Tanto, peraltro, nonostante la tendenza, che si è manifestata anche in quell'ordinamento, a interpretare il relativo concetto in termini piuttosto ampi e a emanciparlo dal corrispondente concetto privatistico. Fin dal 1984, con la STC, 17 febbraio 1984, n. 22, il Tribunale Costituzionale spagnolo ha evidenziato come il concetto di domicilio rilevante ai fini della tutela accordata dall'art. 18 CE è più ampio del corrispondente privato e amministrativo, dal momento che la sua protezione ha carattere strumentale alla tutela della vita privata delle persone. Trattasi, pertanto, di uno spazio che rappresenta l'emanazione della persona e della sua sfera privata, in cui l'individuo vive senza essere soggetto necessariamente agli usi e alle convenzioni sociali e dove esercita la sua libertà più intima. In dottrina, si veda AA.VV., *Derecho Constitucional III. Derechos y libertades*, Colex, 2003, 190 e TREVIJANO, *La inviolabilidad del domicilio*, Tecnos, 1992, 146 ss., che descrivono il domicilio alla stregua di uno spazio isolato dal mondo esterno, chiuso o solo parzialmente aperto, destinato allo sviluppo della personalità umana, rispetto al quale è indifferente il titolo del possesso, acquisendo rilievo, invece, la circostanza che lo spazio sia attualmente sfruttato dal soggetto (il che, però, non implica la sua perdurante presenza fisica nel luogo).

all'intimità[483] che, non dissimilmente da quanto accaduto nel nostro ordinamento, sta acquisendo connotati nuovi in ragione della sempre più evidente capacità delle nuove tecnologie di incidere sui suoi aspetti più pregnanti.

Sul finire degli anni '80, il Tribunale Costituzionale spagnolo descriveva l'intimità alla stregua di un diritto dal volto sostanzialmente passivo («*un ámbito proprio y reservado frente a la acción y el conocimiento de los demás necesario, segun las pautas de nuestra cultura para mantener una calidad mínima de la vida humana*»[484]) e comprimibile per la tutela di altri interessi rilevanti, sia pur in misura non superiore a quella necessaria per raggiungere altri fini costituzionalmente legittimi e rispettosa del suo contenuto essenziale[485].

Gli anni successivi hanno marcato un sempre più netto cambio di rotta: anche nell'ordinamento spagnolo il diritto alla tutela dell'intimità, dalla sua tradizionale veste di diritto ad essere lasciati soli e a non subire intrusioni esterne nello svolgimento delle attività che il soggetto intende mantenere riservate, si è arricchito di componenti inedite che ne rimarcano una dimensione non più meramente passiva. Tanto in ragione della comprensione dell'intrinseco legame che lo avvince non semplicemente all'aspettativa di una vita dotata di una "qualità minima", quanto piuttosto alla presenza delle condizioni necessarie, in senso più squisitamente proattivo, allo sviluppo della personalità dell'individuo[486].

Nel 1993, quindi, il Tribunale Costituzionale[487] includeva nel contenuto minimo del diritto all'intimità quello al controllo sui dati relativi alla propria persona, confermando questa posizione in una pronuncia del 1998[488]. Si tratta di una sentenza di particolare interesse in quanto evidenzia la correlazione tra il diritto all'intimità, tutelato dall'art. 18, comma 1, CE e il diritto alla protezione dei dati personali, protetto dal comma 4 del medesimo articolo, che, secondo la Corte, incorpora una garanzia costituzionale

---

[483] In relazione all'estensione e al contenuto del diritto all'onore e all'immagine, invece, si veda AA.VV., *Derecho Constitucional III. Derechos y libertades*, cit., 177 ss.

[484] STC, 27 ottobre 1988, n. 209; STC, 2 luglio 2001, n. 156.

[485] STC, 28 febbraio 1994, n. 57; STC, 3 aprile 2002, n. 70.

[486] Si veda, per tutti, la riflessione di DE LA MATA BARRANCO e BARINAS UBIÑAS, *La protección penal de la vida privada en nuestro tiempo social: ¿necesidad de redefinir el objeto de tutela?*, in *Rev. der. pen. y crim.*, 2014, 11, 41 ss., che parla dell'intimità come un diritto preposto ad assicurare, anzitutto, «*un pleno desarrollo personal, que garantice la conformación del propio ser tal como cada cual quiera moldearla […] con un aspecto positivo que garantiza la autodeterminación personal y negativo que impide a otros la merma de ésta*».

[487] STC, 20 luglio 1993, n. 254. Cfr. anche STC, 7 novembre 2011, n. 173.

[488] STC, 13 gennaio 1998, n. 11.

necessaria per rispondere a una nuova forma di minaccia alla dignità umana e ai diritti della persona, conseguente al trattamento massivo dei dati personali. Sicché, parafrasando le parole della Corte, il diritto all'intimità si arricchisce di una componente positiva che si traduce nel diritto al controllo sui dati relativi alla propria persona[489]. Tanto, però, con la precisazione che, a tal fine, non ha più senso distinguere tra spazi e informazioni pubbliche e private se è vero, come è vero, che esistono dati *a priori* del tutto irrilevanti sul piano della privatezza e che, tuttavia, se letti congiuntamente ad altri, consentono di ricostruire il profilo di un individuo e di violare, in tal modo, le sue più elementari aspettative di intimità[490].

In questo senso, con eccezionale schiettezza, la dottrina spagnola ha evidenziato che «*la idea de privacidad, como se ha conocido tradicionalmente, ya no existe. Nuestras decisiones, preferencias, gustos, el desarrollo de nuestra identidad e incluso nosotros mismos nos vemos reducidos a un algoritmo computacional que permite hacer fluir datos dentro de un espacio intangible e interconectado que todo lo ve, lo recuerda, lo relaciona y lo pone a disposición de quien pueda pagar por ello, sea capaz tecnológicamente de acceder a ello o pueda obligar a otros a proporcionárselo. Pero, tras esos datos hay personas y en este nuevo contexto hay que redefinir el contenido del derecho a la vida privada y acentuar dos dimensiones irrenunciables: la privacy informacional y la privacy decisional. Y no se trata de garantizar la reserva respecto de datos sensibles o íntimamente personales, sino de todos los datos, porque es su conjunción la que me define, la que configura mi identidad digital (gustos, preferencias,*

[489] Si riportano di seguito le parole della Corte: «*La garantía de la intimidad, latu sensu, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la persona misma. La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a la utilización de determinadas datos personales para hasta distintos de aquel legítimo que justificó la obtención*». In dottrina, si veda, in tal senso, Cfr. AA.VV., *Derecho Constitucional III. Derechos y libertades*, cit., 183, che parla di diritto all'intimità come «*la proteccion de la autorrealizacion del individuo. Es el derecho che que toda persona tiene a que permanezcan desconocidos determinados ambitos de su vida, asì como a controlar el conocimiento que terceros tienen de el. La intimidad es el elemento de desconnexion social. El concepto de derecho a la intimidad como estricto derecho de defensa tiene incardinacion directa en la dignidad humana y el libre desarrollo de la personalidad. La potestad de control de lo que afecta al individuo en su ambito de intimidad tiene una correlacion tambien directa con la libertad*».

[490] Questa ricostruzione, alquanto pioneristica, è, invero, assai risalente. Si veda MADRID CONESA, *Derecho a la intimidad, informatica y Estato de Derecho*, Universidad de Valencia, 1984, 45.

hábitos, ingresos, presencias) y la que la muestra a los demás, sin yo saberlo o, al menos, sin yo quererlo»[491].

È ragionevole ipotizzare che proprio sulla base di queste nuove acquisizioni abbia preso piede, anche in Spagna, il dibattito in merito all'esigenza di riconoscere un nuovo diritto costituzionale all' "*entorno virtual*", alla stregua di una prerogativa emergente dalla convergenza di altri diritti costituzionali già espressamente tutelati, tesa alla protezione del complesso di informazioni che l'individuo genera tramite l'uso delle nuove tecnologie. L'idea che sta alla base di una simile ricostruzione è, evidentemente, quella per cui, singolarmente considerate, le varie componenti del diritto alla vita privata enucleabili dall'art. 18 CE non hanno la capacità di contenere una prerogativa che ha tutta l'apparenza di un *novum* giuridico.

Dell'esistenza e della portata di tale nuova prerogativa si parlerà successivamente trattando dell'istituto del *registro remoto*. Quanto deve, invece, evidenziarsi già in questa sede è che l'evoluzione che ha condotto a tale riconoscimento espresso da parte dello stesso Tribunale Supremo[492] ha probabilmente risentito anche dei confini eccessivamente angusti che la giurisprudenza ha tradizionalmente riconosciuto al diritto al segreto delle comunicazioni, non dissimilmente da quanto accaduto nel nostro Paese.

Sia pur con notevoli oscillazioni interpretative, la giurisprudenza costituzionale e di legittimità spagnola sembra, infatti, orientata nel senso che la protezione del diritto al segreto delle comunicazioni riguardi il processo comunicativo in sé, rimanendo estranea al suo ambito applicativo l'intrusione che si realizzi una volta che lo stesso sia finalizzato. Sicché, l'eventuale captazione non contestuale di comunicazioni già realizzate e, dunque, memorizzate sul dispositivo utilizzato non dovrebbe essere soggetta alla protezione di cui al comma 3 dell'art. 18 CE quanto, piuttosto, a quella delle norme che tutelano l'intimità o altri diritti[493]. Tanto con la conseguenza, non

---

[491] DE LA MATA BARRANCO e BARINAS UBIÑAS, *La protección penal de la vida privada*, cit., 58.

[492] STS, 17 aprile 2013, n. 342, oggetto di successiva analisi.

[493] Cfr. STC, 3 aprile 2002, n. 70. In termini, STS, 17 aprile 2013, n. 342. In dottrina, sul contenuto del diritto al segreto delle comunicazioni, si veda ZOCO ZABALA, *Nuevas tecnologías y control de las comunicaciones. LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de la medidas de investigación tecnológica*, Thomson Reuters, 2015, 36, che evidenzia come la Costituzione protegga, nell'ambito del segreto comunicazioni, solo quelle che si realizzano mediante mezzo tecnico di conversazione, escludendo altre forme comunicative come immagini, conversazioni in presenza e dati personali, siano o no di traffico. Vi rientrerebbero, dunque, comunicazioni postali, telegrafiche e telefoniche e ogni altro artificio tecnico derivato dalla evoluzione delle nuove tecnologie (chat, videochat, correo elettronico, messaggi etc.), indipendentemente dallo strumento tecnico di trasmissione e dal fatto che la

trascurabile, che solo nel caso di captazione contestuale della comunicazione risulterebbe applicabile la normativa in materia di intercettazioni che, attuando il precetto costituzionale (di cui al comma 3 dell'art. 18 CE), prevede la necessaria risoluzione giudiziale. Nel caso, invece, di captazione non contestuale, l'operatività di altre prerogative costituzionali imporrebbe comunque l'esistenza di una solida base legale (riserva di legge)[494], ma non la necessaria risoluzione giudiziale motivata.

Come evidenziato, tuttavia, non sono mancate soluzioni in senso contrario[495] e, in generale, alcune contraddizioni ermeneutiche, come quella di inserire nell'ambito della protezione costituzionale del segreto delle comunicazioni anche i dati relativi al traffico telefonico[496] che, seguendo la linea interpretativa appena segnalata, a rigore, ne sarebbero dovuti rimanere esclusi[497].

Indipendentemente dalle più o meno marcate oscillazioni interpretative sul punto, i confini tracciati dalla giurisprudenza maggioritaria in materia di diritto al segreto delle comunicazioni devono essere apparsi eccessivamente angusti alla dottrina e – infine – anche alla giurisprudenza di quel Paese se rapportati alle forme di intrusione consentite dal ricorso alle nuove tecnologie. Come si vedrà nelle pagine dedicate alla normativa spagnola sulla vigilanza occulta e da remoto dei sistemi informatici di uso comune (il cosiddetto *registro remoto*) la sensazione della attuale inadeguatezza di soluzioni esegetiche restrittive, come quella appena analizzata, traspare in maniera piuttosto netta dalle considerazioni della dottrina più attenta. A ben vedere, però, in qualche misura, lo stesso legislatore ha dimostrato di preferire soluzioni normative improntate a livelli più

---

comunicazione sia pertinente a un ambito personale, intimo o riservato. Tale tutela, tuttavia, si estende solo alle comunicazioni in corso. Si veda anche RICHARD GONZÁLEZ, *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y garabación de imagen y sonido*, La Ley, 2017, 26.

494 Tanto in ragione del precetto di cui all'art. 53 CE che, in via generale, prevede la riserva di legge in relazione alla restrizione dei diritti fondamentali costituzionalmente tutelati. Si avrà modo di analizzarlo nel prossimo paragrafo.

495 Cfr. STC, 29 novembre 1984, n. 114, per la quale «*El bien constitucionalmeme protegido es así —a través de la imposición a todos del «secreto» — la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje —con conocimiento o no del mismo— o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)*»; STC, 5 novembre 2007, n. 230; STS, 5 febbraio 2010, n. 51.

496 STC, 5 novembre 2007, n. 230.

497 Per questo, nella circolare della *Fiscalía General del Estado* n. 1/2013, "*Sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*", dell'11 gennaio 2013, a pagina 30, si invitano i pubblici ministeri dello Stato ad agire secondo un principio di prudenza, richiedendo sempre l'autorizzazione giudiziale anche per l'acquisizione di dati relativi a conversazioni già consumate».

elevati di tutela di quelli che, secondo la giurisprudenza appena riportata, avrebbero potuto ritenersi "costituzionalmente" sufficienti: la disciplina introdotta nel 2015, come visto, richiede l'autorizzazione giudiziale per qualsivoglia accesso a un dispositivo di memorizzazione massiva dei dati, proprio sul presupposto che nello stesso possono essere conservati dati della più svariata natura, tra cui dati relativi alle comunicazioni che – indipendentemente dalla contestualità della captazione – sono stati, evidentemente, reputati meritevoli della più intensa tutela di cui all'art. 18, comma 3, CE.

1.2. Principio di legalità e principio di proporzionalità: la necessità di una base legale sufficiente.

Ai sensi dell'art. 53, comma 1, CE, la restrizione dei diritti fondamentali riconosciuti nel Capitolo II del Titolo I[498] della Costituzione spagnola può legittimamente realizzarsi solo per il tramite di una legge[499] che, in ogni caso, deve rispettarne il contenuto fondamentale.

L'esistenza di un simile precetto nel testo costituzionale, legittimando l'intrusione statale nelle prerogative fondamentali presidiate dal testo costituzionale nella sola misura in cui una legge dello Stato abbia definito i casi e le modalità della restrizione, ha reso sostanzialmente superflua, in quell'ordinamento, la *querelle* che imperversa da decenni nel sistema italiano in materia di prove incostituzionali: nell'ordinamento spagnolo, una prova atipica non potrebbe mai impattare su un diritto fondamentale perché, essendo per definizione non regolata dalla legge, sarebbe contraria al disposto dell'articolo appena menzionato e, prima ancora, contrastante con il contenuto del diritto fondamentale suscettibile di venire in rilievo nel caso di specie. L'effetto processuale dell'accertamento di una simile violazione è quello indicato – in termini generali, cioè con riferimento a qualsiasi tipo di procedimento giurisdizionale – dall'art. 11 Ley Orgánica del Poder Judicial[500], che stabilisce che «*no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades*

[498] Trattasi degli artt. da 14 a 38 della Costituzione spagnola.

[499] La riserva di legge in questione è da intendersi quale riserva di legge organica, stante il disposto dell'art. 81 CE che prevede che le leggi relative allo sviluppo dei diritti fondamentali siano leggi organiche, ovvero approvate con una maggioranza differente da quella ordinaria. In particolare, per l'approvazione, modificazione o abrogazione di una legge organica è necessaria la maggioranza assoluta del Congresso dei Deputati, ovvero una delle due Camere.

[500] D'ora in poi, anche Lopj.

fundamentales»[501]. Detto altrimenti, in materia di diritti e libertà fondamentali, la scelta del legislatore costituente spagnolo è stata quella di generalizzare il principio della riserva di legge e di far espressamente conseguire alla sua violazione l'inutilizzabilità del risultato probatorio acquisito.

Come conseguenza di ciò, dunque, anche la restrizione delle prerogative costituzionali tutelate dall'art. 18 CE presuppone l'esistenza di una base legale sufficiente e proprio a tal fine è stata approvata la Ley Organica 13/2015 del 5 ottobre 2015 in materia di strumenti di indagine tecnologici impattanti sul diritto al rispetto della vita privata.

Costituisce, peraltro, orientamento granitico del Tribunale Costituzionale quello secondo il quale la riserva di legge prevista in materia di diritti fondamentali non è una mera formalità, ma implica altresì precise esigenze rispetto al contenuto della legge medesima, che deve essere sufficientemente preciso allo scopo di realizzare due obiettivi: da un lato, assicurare che i diritti che la Costituzione riconosce ai cittadini non siano violati da ingerenze statali non autorizzate dai loro rappresentanti; dall'altro, assicurare l'effettività del principio – anch'esso previsto dalla Costituzione all'art. 117 CE – della sottoposizione dei magistrati alla sola legge. Tanto è stato costantemente ribadito dal Tribunale Costituzionale a partire dalle sue prime sentenze[502], con cui si è avviato un filone giurisprudenziale che proprio in materia di intrusioni a carattere tecnologico nel diritto alla vita privata ha condotto all'elaborazione più compiuta dei principi appena menzionati. Ci si riferisce, in particolare, alla sentenza del Tribunale Costituzionale del 1999 in materia di intercettazioni[503] – già precedentemente citata[504] – nella quale si sono individuati i presupposti per la legittimità dell'inferenza statale nel diritto al segreto delle comunicazioni. Nella pronuncia il Tribunale Costituzionale, ribadito il carattere essenziale della esistenza di una abilitazione legale alla restrizione dei diritti fondamentali, ne ha determinato in maniera precisa i contorni, imponendo al legislatore un contenuto minimo di qualsivoglia normativa regolatrice dell'intervento statale nelle prerogative fondamentali dei singoli.

---

[501] Parla, a proposito della norma, di una «diretta applicazione processuale delle norme costituzionali» MARCOLINI, voce *Processo penale spagnolo*, in *Enc. dir., Annali*, vol. II, tomo I, 2008, 782.

[502] MONTES ÁLVARO, *Regulación de las medidas de investigación tecnológica y la protección de los derechos reconocidos en el art. 18 CE*, in *Revista del Ministerio fiscal*, 2017, 3, 88. Si veda, ad esempio, STC, 24 luglio 1984, n. 83.

[503] STC, 5 aprile 1999, n. 49.

[504] Cfr. par. 1.

L'analisi del contenuto della pronuncia è opportuno tanto sul piano generale, quanto su quello specifico delle misure a carattere tecnologico impattanti sui diritti costituzionali.
Sotto il primo profilo, come si vedrà, tutti gli elementi contenutistici che, nell'ottica del Tribunale Costituzionale, rappresentano i presupposti irrinunciabili della legittimità della disciplina primaria impattante sui diritti fondamentali convergono nel senso della necessaria proporzionalità della normativa adottata dal legislatore in esecuzione del disposto dell'art. 53 CE: vale a dire, cioè, che perché la riserva di legge possa dirsi rispettata non basta che la legge medesima sia sufficientemente precisa nell'individuazione dei limiti e delle modalità attraverso le quali il diritto fondamentale può essere ristretto. È altresì necessario che la disciplina specifica adottata rappresenti la concretizzazione sul piano legislativo di un bilanciamento proporzionato tra i contrapposti interessi in campo.
Sotto il secondo profilo, l'analisi della pronuncia illumina le scelte regolatorie compiute dal legislatore del 2015 in materia di misure investigative a carattere tecnologico. La disciplina relativa a tali misure – soprattutto nella parte concernente le regoli comuni alle stesse – rappresenta, infatti, fedele trasposizione dei principi elaborati dalla pronuncia del 1999 e costantemente confermati dalla giurisprudenza successiva.
Un primo fondamentale requisito individuato dalla giurisprudenza in argomento quale presupposto della legittimità della restrizione di diritti fondamentali è quello della necessaria finalizzazione della stessa al compimento di un fine costituzionalmente legittimo. Requisito, questo, tendenzialmente soddisfatto laddove la misura sia finalizzata all'accertamento e alla repressione di una condotta penalmente rilevante. Di maggiore interesse, invece, l'ulteriore principio per il quale il sacrificio del diritto fondamentale deve essere – tanto sul piano regolatorio, quanto su quello della adozione della misura nel caso di specie – strettamente necessario per conseguire l'anzidetto interesse legittimo e proporzionato. L'esigenza di proporzionalità della misura opera, quindi, anzitutto sul piano legislativo e, in secondo luogo, su quello della concreta pratica giudiziaria, imponendo che il provvedimento che dispone l'adozione della misura motivi in maniera sufficientemente precisa: la costatazione della ragionevole commissione di un reato e della attribuibilità del medesimo a un soggetto determinato; la connessione esistente tra il possibile autore del reato e il soggetto concretamente affettato dall'esecuzione della misura; i dati obiettivi suscettibili di corroborare le

conclusioni anzidette, con la precisazione, dunque, che non sono sufficienti meri sospetti, essendo necessaria la presenza di elementi fattuali concretamente verificabili.

Nell'ottica fatta propria dal Giudice delle Leggi spagnolo, insomma, il principio di legalità e quello di proporzionalità si compenetrano nella misura in cui il compimento del secondo rappresenta una *condicio sine qua non* l'effettività del primo[505].

Come è stato rilevato nella dottrina spagnola, effettivamente, il Tribunale costituzionale ha invocato piuttosto spesso il principio di proporzionalità non solo nel giudizio relativo alla concreta applicazione del diritto, ma anche in quello afferente alla creazione di norme e, dunque, al piano più squisitamente legislativo, probabilmente in conseguenza della lettura secondo la quale la proporzionalità si atteggerebbe a necessario corollario del rispetto del contenuto essenziale del diritto fondamentale espressamente richiesto dall'art. 53 CE[506]. Indipendentemente dalla correttezza o meno di una simile impostazione, l'analisi della normativa adottata nel 2015 in materia di investigazioni tecnologiche manifesterà plasticamente come una simile ottica – secondo la quale il principio di legalità e quello di proporzionalità devono operare sinergicamente anzitutto nella previsione legislativa delle possibili restrizioni dei diritti e delle libertà fondamentali – sia stata, infine, adottata anche dal legislatore spagnolo.

Come si è già accennato, l'effetto, sul piano processuale, della violazione del diritto fondamentale – anche in dipendenza della mancata previsione dei casi e dei modi della restrizione ai sensi dell'art. 53 CE è indicato dall'art. 11 Lopj, che stabilisce la prova – illecita – in tal modo acquisita "non sortirà effetto".

Nel combinato disposto dell'art. 53 CE e dell'art. 11 Lopj la dottrina processualpenalistica spagnola ha rinvenuto una delle espressioni della categoria

---

[505] Tanto risulta particolarmente chiaro dalla lettura del seguente passaggio della pronuncia: «*del principio de proporcionalidad, cuya vigencia hemos reafirmado en el ámbito de las intervenciones telefónicas (SSTC 85/1994, fundamento jurídico 3º; 181/1995, fundamento jurídico 5º; 49/1996, fundamento jurídico 3º; 54/1996, fundamento jurídico 7º y 123/1997, fundamento jurídico 4º), se infiere inmediatamente que, tanto la regulación legal como la práctica de las mismas ha de limitarse a las que se hallen dirigidas a un fin constitucionalmente legítimo que pueda justificarlas y que se hallan justificadas sólo en la medida en que supongan un sacrificio del derecho fundamental estrictamente necesario para conseguirlo y resulten proporcionadas a ese sacrificio*».

[506] Si veda, sul punto, JIMÉNEZ CAMPO, *Artículo 53. Protección de los derechos fundamentales*, in Alzaga Villaamil, *Comentarios a la Constitución española de 1978*, Edersa, Madrid, 1996, 478, anche per la giurisprudenza citata. L'autore, in realtà, si manifesta critico rispetto all'impostazione adottata dal Tribunale Costituzionale, evidenziando come dalla lettura fatta proprio da quest'ultimo deriverebbe la possibilità di ritenere che il legislatore possa violare i diritti fondamentali non solo comprimendo il loro contenuto essenziale (come si desumerebbe dall'art. 53 CE), ma anche in ragione della ritenuta sproporzione della disciplina legislativa adottata. Tanto, in buona sostanza, conferirebbe al giudizio di legittimità costituzionale delle leggi un carattere eccessivamente discrezionale.

giuridica definita come "illiceità della prova" che, secondo la ricostruzione maggiormente accreditata[507], può derivare – oltre che dalla infrazione di un diritto fondamentale – anche dalla violazione di una espressa proibizione di legge o dalla irregolarità della prova, quest'ultima da intendersi come violazione delle norme che ne regolano l'acquisizione e che potrebbe, ricorrendone i presupposti di legge, determinarne la nullità[508]. Autorevole dottrina ha, peraltro, evidenziato come l'effetto che l'art. 11 Lopj riconnette alla violazione di un diritto fondamentale nell'acquisizione della prova non è assimilabile a un'ipotesi di nullità quanto, piuttosto, a una vera e propria inutilizzabilità[509]. Tanto con la conseguenza che non sussistono limiti in ordine alla allegazione del vizio processuale e, soprattutto, che non è necessario, per l'esclusione della prova dalla piattaforma probatoria, che la stessa abbia generato una violazione concreta del diritto di difesa (presupposto, questo, richiesto dall'art. 238 Lopj perché possa dichiararsi la nullità di un atto acquisito in violazione di norme essenziali del procedimento).

2. Le disposizioni comuni in materia di ricorso a mezzi di investigazione tecnologicamente avanzati.

Come già accennato, le disposizioni comuni alle misure di investigazione tecnologiche introdotte dalla legge organica del 2015 rappresentano la sostanziale trasposizione sul

[507] MIRANDA ESTRAMPES, *El concepto de prueba ilícita y su tratamiento en el proceso penal* (2a. ed.), J.M. Bosch Editor, 2008, 31. In termini, NIEVA FENOLL e TARUFFO, *La valoración de la prueba*. Marcial Pons, 2010, 189.

[508] Perché possa prodursi un simile effetto, è necessario che sia integrata una delle condizioni previste dall'art. 238 Lopj, ai sensi del quale «*Los actos procesales serán nulos de pleno derecho en los casos siguientes: 1.º Cuando se produzcan por o ante tribunal con falta de jurisdicción o de competencia objetiva o funcional. 2.º Cuando se realicen bajo violencia o intimidación. 3.º Cuando se prescinda de normas esenciales del procedimiento, siempre que, por esa causa, haya podido producirse indefensión. 4.º Cuando se realicen sin intervención de abogado, en los casos en que la ley la establezca como preceptiva. 5.º Cuando se celebren vistas sin la preceptiva intervención del letrado de la Administración de Justicia. 6.º En los demás casos en los que las leyes procesales así lo establezcan*».

[509] ASENCIO MELLADO, *La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales*, in *Diario La Ley*, 2013, 8009, 2, che evidenzia altresì come la categoria della prova acquisita in violazione di un diritto fondamentale abbia fondamento costituzionale e derivi dalla violazione di un diritto materiale e non processuale (non deriverebbe, dunque, anche dalla mera violazione del diritto di difesa di cui all'art. 24 CE). Dunque, l'inefficacia della prova incostituzionale dovrebbe operare in ogni stato e grado del procedimento, ivi inclusa la fase delle indagini preliminari, atteso che una diversa interpretazione sarebbe contraria all'effettività del diritto fondamentale violato. Inoltre, la formulazione di cui all'art. 11 Lopj dovrebbe intendersi come carenza di qualsivoglia effetto legale e non alla stregua di una mera proibizione di valutazione della prova.

piano normativo dei principi elaborati dalla giurisprudenza costituzionale in materia di restrizione dei diritti fondamentali finora analizzati[510].

Nell'ambito di tale complesso normativo, fondamentale importanza rivestono, in particolare, le disposizioni di cui all'art. 588 *bis* a Lecrim, nelle quali il legislatore individua i principi rettori comuni all'adozione di qualsivoglia misura restrittiva, tracciando le linee essenziali dell'apparato giustificativo del provvedimento autorizzativo della stessa. In tal modo, l'obbligo del giudice di motivare l'atto con il quale viene disposta la restrizione del diritto fondamentale risulta imbrigliato in una precisa sequenza argomentativa la cui finalità è, sostanzialmente, quella di dar conto nella maniera più particolareggiata possibile del rispetto, nel caso di specie, del principio di proporzionalità ed eccezionalità della restrizione.

L'intero sistema, dunque, si fonda sull'esistenza di una rete unificata di garanzie minime che si incrementano all'aumentare della *vis* intrusiva dell'atto concreto. Tanto con la conseguenza che le norme applicabili per l'adozione ciascuna misura sono, anzitutto, quelle previste dalla disciplina generale, cui si aggiungono quelle specificamente dettate per il singolo atto in funzione delle sue peculiarità e del suo livello di incidenza sui diritti fondamentali.

Dalla lettura dell'art. 588 *bis* a Lecrim possono isolarsi tre fondamentali principi rettori comuni a tutte le misure di investigazione tecnologiche, da ravvisarsi nella riserva di giurisdizione, nel principio di specialità e nella necessaria proporzionalità della restrizione.

In ossequio al primo comma dell'articolo in argomento, infatti, l'adozione, nel corso delle indagini, di una delle misure previste dagli articoli successivi può essere disposta solo previa autorizzazione giudiziale dettata nel rispetto dei principi di specialità, idoneità, eccezionalità, necessità e proporzionalità in senso stretto della misura.

La medesima disposizione si preoccupa, nei commi successivi, specificare la portata di ciascuno di tali principi. Fermo restando che ciascuno di essi sarà successivamente singolarmente approfondito, una breve panoramica del loro contenuto appare necessaria per restituire un quadro completo del complesso delle disposizioni comuni introdotte con la legge del 2015.

---

[510] LÓPEZ CAUSAPÉ, *Las medidas de investigación tecnológica en la ley de enjuiciamiento criminal tras la reforma de la LO 13/2015 de 5 de octubre. Referencia a las disposiciones comunes*, in *Boletín digital AJFV Penal*, 6 luglio 2016, 4.

In virtù del principio di specialità, ciascuna misura deve essere relazionata alla investigazione di un delitto concreto, mentre non possono autorizzarsi misure investigative tecnologiche che abbiano la finalità di prevenire o scoprire reati o vagliare meri sospetti in assenza di una base fattuale oggettiva. Il principio, dunque, impedisce in radice lo svolgimento di indagini meramente esplorative e impone al giudice di motivare in ordine alla sussistenza di dati obiettivi dai quali possa desumersi ragionevolmente la previa commissione di un reato concreto.

Il principio di idoneità, invece, serve a definire l'ambito oggettivo e soggettivo, nonché la durata della singola misura in ragione della sua concreta utilità[511]. Pertanto, esso si riferisce alla relazione tra i dati e le prove che si intendono acquisire e la misura adottata nel caso di specie, imponendo al giudice di vagliare – e motivare – le ragioni per le quali la stessa si reputa idonea al raggiungimento del risultato prefissato. Strettamente legati a tale criterio sono i successivi principi di necessità ed eccezionalità e di proporzionalità in senso stretto, che con il primo concorrono alla definizione di un generale principio di necessaria proporzionalità della misura.

Quanto alla necessità ed eccezionalità della restrizione, è lo stesso comma 4 dell'articolo in commento a stabilire che la misura restrittiva può accordarsi solo in presenza di due condizioni da reputarsi concorrenti: anzitutto, è necessario che, stanti le caratteristiche della singola indagine, non siano disponibili altri mezzi meno gravosi sui diritti fondamentali coinvolti ugualmente utili per la ricostruzione del fatto; in secondo luogo, si richiede che la scoperta o la prova del fatto investigato, la determinazione del suo autore o del luogo in cui egli si trova o la localizzazione degli effetti del reato sia resa gravemente difficoltosa senza il ricorso alla misura.

Con riferimento, infine, al principio di proporzionalità in senso stretto, il comma 5 dell'articolo in argomento stabilisce le misure adottabili a norma delle disposizioni contenute nel capitolo si reputano proporzionate quando, considerate le circostanze del caso, il sacrificio dei diritti ristretti non sia superiore al beneficio generato dall'adozione della misura in termini di interesse pubblico o di terzi concretamente soddisfatto per il suo tramite. Per la ponderazione di tali interessi in conflitto, si prevede che il vaglio condotto in merito all'interesse pubblico soddisfatto con la misura debba basarsi su una serie di parametri predeterminati: la gravità dei fatti, il loro impatto sociale

[511] RICHARD GONZÁLEZ, *Investigación y prueba*, cit., 97.

(testualmente, il legislatore parla di «*trascendencia social*») e l'ambito tecnologico nel quale si sono verificati, la gravità degli indizi esistenti e la rilevanza del risultato perseguito con l'adozione della misura[512].

Secondo una parte della dottrina, non sarebbe chiaro se i criteri di cui sopra siano o meno concorrenti[513]. Sia l'argomento letterale che quello sistematico e teleologico, tuttavia, inducono a preferire la risposta positiva. Sotto il primo profilo, il comma 1 dell'art. 588 *bis* a Lecrim non adopera disgiuntive e, anzi, espressamente prevede che debbano essere rispettati "i principi" successivamente elencati («*Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida*»).

Sul piano sistematico e teleologico, poi, risulta evidente come tutti i principi appena menzionati siano logicamente interdipendenti nella misura in cui sono finalizzati ad assicurare il risultato della eccezionalità[514] e non arbitrarietà dell'atto di indagine tecnologico, risultato consentito dall'operare congiunto dei principi di idoneità, necessità e proporzionalità in senso stretto della misura e, ovviamente, del principio di specialità, che impedisce all'autorità pubblica di perpetrare intrusioni nella sfera privata dei singoli non giustificate dall'esigenza di accertare o reprimere un reato concreto. Il sacrificio di un diritto fondamentale, insomma, non deve rappresentare un'occorrenza normale o rutinaria dell'investigazione penale, ma piuttosto un'eventualità tollerabile solo nella misura in cui sia strettamente necessaria per realizzare l'interesse statale alla repressione delle condotte antisociali[515].

A quest'ultimo proposito, rilievo peculiare assume il riferimento alla proporzionalità in senso stretto della misura. Risulta di particolare interesse l'enunciazione legislativa dei

---

[512] In merito a tutti i presupposti appena analizzati, si veda Bachmaier Winter, *Registro remoto de equipos informáticos*, cit., 16.

[513] SÁNCHEZ RUBIO, *El principio de proporcionalidad en las medidas de investigación tecnológicas*, in AA.VV., *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos*, a cura di Zamora, Pereira, Ordóñez Ponz, Moral García, Aranzadi, 2021, 63, il quale, tuttavia, specifica che la motivazione risulterebbe certamente più completa ove prendesse in considerazione tutti i principi appena menzionati, così riducendosi il rischio di una successiva declaratoria di illiceità della misura.

[514] In termini, AÑÓN CALVETE, *Diligencias de Investigación Tecnológica y Derechos Fundamentales*, Tirant lo Blanch, 2015, 5; JIMÉNEZ SEGADO e PUCHOL AIGUABELLA, *Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos* in *Diario La Ley*, n. 8676, Sección Doctrina, 7 gennaio 2016.

[515] In tal senso, si veda, in tema di intercettazioni telefoniche STS, 3 giugno 2002, n. 998.

criteri sulla base dei quali tale vaglio deve essere compiuto dal giudice, chiamato a contemperare l'interesse del singolo al rispetto dei suoi diritti fondamentali e quello dello stato all'accertamento dei reati.

Anzitutto, sul piano generale, può notarsi come una ulteriore trasposizione legislativa di un simile principio si rinvenga nella normativa di dettaglio dettata in relazione alle singole misure, il cui ambito di operatività è generalmente limitato ad alcune fattispecie – specificamente indicate – di reati gravi o di reati commessi per il tramite di tecnologie informatiche. Tale delimitazione legislativa – che, ad ogni modo, riguarda la maggior parte ma non tutte le misure investigative tecnologiche[516] – non esaurisce, però, il vaglio giudiziale di proporzionalità in senso stretto della misura[517]: in altre parole, l'accertamento in ordine alla riconducibilità del reato investigato all'ambito di quelli per i quali è legittimo il ricorso alla misura non esime il giudice dall'onere di vagliare altresì la sussistenza nel caso di specie degli altri presupposti previsti dalla legge (la gravità dei fatti, il loro impatto sociale e l'ambito tecnologico nel quale si sono verificati, la gravità degli indizi esistenti e la rilevanza del risultato perseguito con l'adozione della misura).

Quanto al contenuto specifico di tale vaglio, risultano chiarificatrici le parole adoperate dal Tribunale Supremo in una pronuncia del 2002 in materia di intercettazione telefonica[518], nella quale si è specificato che dalla concorrenza dei requisiti di eccezionalità e proporzionalità di un mezzo investigativo impattante sui diritti fondamentali dei singoli deriva la necessità che il delitto da investigare sia sufficientemente grave. Ciò in quanto l'interesse dello Stato alla persecuzione dei reati è direttamente proporzionale alla gravità di questi ultimi, con la conseguenza che, dinanzi a fattispecie lievi, la restrizione di un diritto fondamentale risulterebbe priva di giustificazione. Una simile valutazione, però, come si diceva, deve essere condotta dal giudice sul piano concreto: vale a dire, cioè, che anche laddove si procedesse in relazione a un titolo di reato grave, ciò non implicherebbe automaticamente un esito positivo del vaglio di proporzionalità in senso stretto, dovendo il giudice prendere in considerazione le caratteristiche del caso concreto e tutti gli altri criteri indicati dal comma 5 dell'art. 588 *bis* a Lecrim. Da questo punto di vista, può notarsi come il

[516] Non riguarda, ad esempio, la perquisizione e il sequestro di dati contenuti i dispositivi di memorizzazione di massa (art. 588 sexies a Lecrim, corrispondente a una perquisizione e sequestro informatici), al quale può procedersi in relazione a qualsivoglia fattispecie di reato.
[517] SÁNCHEZ RUBIO, *El principio de proporcionalidad*, cit., 65.
[518] STS, 3 giugno 2002, n. 998.

requisito della "trascendenza sociale" del fatto investigato, se sotto il profilo logico è certamente suscettibile di influire sull'intensità dell'interesse statale alla repressione del reato, potrebbe avere effetti distorsivi se interpretato nel senso dell'impatto dei fatti oggetto di indagine sull'opinione pubblica e non – secondo un criterio più obiettivo – come concreta idoneità dell'atto delittivo a rompere l'equilibrio sociale nel quale si inserisce.

Per quanto concerne le altre disposizioni comuni in materia di investigazioni tecnologiche, esse sono contenute negli articoli da 588 *bis* b a 588 *bis* k Lecrim[519] e hanno carattere più specificamente operativo, designando le linee essenziali della disciplina processuale sottesa alla loro applicazione e cessazione, oltre alla regolamentazione di ulteriori aspetti processuali come l'eventuale affettazione di soggetti terzi rispetto all'investigazione (in relazione alla quale l'art. 588 *bis* h Lecrim si limita, invero, a rinviare alla disciplina di dettaglio prevista per le singole misure) o la distruzione dei dati raccolti quando non siano più necessari.

Come si avrà modo di spiegare nei paragrafi successivi, la disciplina comune di dettaglio relativa al procedimento applicativo si presenta fortemente connessa ai principi rettori di cui si è appena parlato: vale a dire, cioè, che tali regole individuano una scansione procedimentale evidentemente improntata alla concreta realizzazione di tali principi e, dunque, al rispetto effettivo dei criteri di specialità, eccezionalità e proporzionalità e, ovviamente, della riserva di giurisdizione, da cui occorre prendere le mosse[520].

2.1. La riserva di giurisdizione.

Un aspetto peculiare della disciplina messa a punto dal legislatore spagnolo del 2015 è rappresentato generalizzazione del principio della riserva di giurisdizione in relazione

[519] Come si vedrà a breve, tali disposizioni sono specificamente dedicate: all'individuazione del contenuto necessario della richiesta di applicazione della misura avanzata dal pubblico ministero o dalla polizia giudiziaria e della conseguente autorizzazione giudiziale; alla disciplina del segreto in merito agli atti realizzati; al regime di durata, proroga e cessazione delle misure; ai controlli operati dal giudice in costanza di esecuzione della misura; all'eventuale affettazione dei diritti dei terzi; all'uso del materiale probatorio acquisito in altri procedimenti; alla distruzione dei registri relativi alla misura quando la loro conservazione non sia più necessaria.

[520] Cfr. anche punto IV del Preambolo alla Ley Organica 13/2015, che, in termini marcatamente critici, evidenzia che «*la práctica forense no es ajena a casos de solicitudes policiales y de ulteriores resoluciones judiciales que adolecen de un laconismo argumental susceptible de vulnerar el deber constitucional de motivación. A evitar ese efecto se orienta la minuciosa regulación del contenido de esa solicitud, así como de la resolución judicial que, en su caso, habilite la medida de injerencia*».

alle varie misure di investigazione tecnologica introdotte, con la sola eccezione di alcune attività investigative di carattere tecnico prodromiche alla realizzazione di atti investigativi veri e propri, ovvero precipuamente finalizzati all'acquisizione di elementi utili per la ricostruzione del fatto[521].

La peculiarità di tale opzione normativa risiede, essenzialmente, nel fatto che la stessa non fosse costituzionalmente imposta: l'art. 18 CE, infatti, stabilisce la riserva di giurisdizione solo con riferimento alla compressione dei diritti inviolabili al domicilio e alla segretezza delle comunicazioni. Tale scelta sistematica pare spiegabile alla luce di due considerazioni probabilmente concorrenti: per un verso potrebbe essere stata la peculiare intrusività nel diritto al rispetto della vita privata comune a tutte le misure di investigazione tecnologica a determinare la scelta di affidare sempre al giudice il compito di adottare il provvedimento applicativo della misura. Tanto anche in ragione della complessità della valutazione di concreta proporzionalità della stessa che rappresenta necessario presupposto per la sua adozione e a cui corrisponde un penetrante onere motivazionale. Per altro verso, tale scelta potrebbe essere stata determinata dalla consapevolezza che le misure in questione, per il carattere poliedrico e multifunzionale degli strumenti informatici, potrebbero restringere – anche contemporaneamente –diverse componenti del diritto alla vita privata, senza che sia predeterminabile di volta in volta quale o quali saranno quelle effettivamente incise.

Quale che sia la considerazione di opportunità sottesa a tale opzione, in ragione della stessa il filtro di legalità della singola misura è affidato sempre al giudice[522], che generalmente la autorizza in virtù di una richiesta degli organi inquirenti, ma che può disporla anche in via officiosa. Peculiarità, quest'ultima, che non ha mancato di suscitare la critica di autorevole dottrina[523] e che pare nondimeno trovare un contrappeso nell'imposizione al giudice dell'obbligo di procedere, in ogni caso,

---

[521] Cfr. nota n. 476.

[522] Come si è già accennato, però, la legge regola, nondimeno, i casi in cui, a causa dell'urgenza di procedere alla realizzazione della misura, la stessa può essere disposta da soggetti diversi dal giudice, salva la sua successiva convalida. Cfr. nota 471.

[523] BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 19, che evidenzia come la circostanza che il giudice possa accordare la misura d'ufficio rappresenta una peculiarità del sistema processuale spagnolo e non risulta del tutto adeguata sotto un punto di vista teorico. Ciò in quanto «*que el mismo juez que dirige la instrucción y asume la búsqueda de la verdad en el proceso penal, sea quien deba decidir que la medida que él mismo solicita cumple con todas las garantías, es cuanto menos conceptualmente cuestionable*».

all'audizione del pubblico ministero prima di disporre la misura[524]. Non è prevista, invece, la possibilità per le parti private – neppure per la difesa del soggetto sottoposto alle indagini – di sollecitare l'applicazione delle misure investigative previste a seguito della riforma del 2015.

La risoluzione giudiziale adottata in conformità del disposto degli artt. 588 *bis* a e ss. Lecrim deve essere motivata, dunque sostenuta da un apparato argomentativo sufficiente a dar conto della sussistenza di tutti i presupposti e requisiti previsti dalla legge e dell'effettuazione, da parte del giudice, di una valutazione autonoma rispetto alla richiesta di applicazione della misura avanzata dal pubblico ministero o dalla polizia giudiziaria[525].

La componente giurisdizionale del procedimento applicativo della misura, peraltro, non si esaurisce nella necessità che sia il giudice a disporla: il legislatore spagnolo ha, infatti, affidato a quest'ultimo altresì il compito di procedere a una verifica costante in ordine alla perdurante utilità e legittimità della misura nei momenti successivi alla sua adozione. In questo senso, l'art. 588 *bis* c, comma 3, lett. f), Lecrim prevede che l'autorizzazione giudiziale contenga altresì la forma e la periodicità con la quale il soggetto che ha sollecitato la misura deve provvedere a informare il giudice dei risultati della medesima. Da tale regola può desumersi che la misura è adottata *rebus sic stantibus*: pertanto, in caso di misure non istantanee, ma destinate ad essere applicate per un certo lasso di tempo (si pensi all'intercettazione o all'accesso remoto a dispositivi informatici), è necessario che la ricorrenza dei presupposti per la restrizione del diritto fondamentali perduri per tutta la durata dell'atto investigativo. In questo senso, l'art. 588 *bis* j Lecrim prevede, in generale, che il giudice determini la cessazione delle misure laddove scompaiano le circostanze che ne giustificarono l'adozione o risulti evidente che attraverso le stesse non si stiano ottenendo i risultati sperati. Pertanto, il controllo giurisdizionale abbraccia tre estremi essenziali: che lo svolgimento concreto dell'atto investigativo sia conforme rispetto a quanto autorizzato; che non si realizzino eccessi nell'esecuzione della misura, in dipendenza dell'eccessiva durata della stessa o della ingerenza ingiustificata in altri ambiti o diritti di terzi estranei

[524] Nel senso che tale audizione previa deve svolgersi anche in caso di misura adottata d'ufficio, cfr. LÓPEZ CAUSAPÉ, *Las medidas de investigación tecnológica*, cit., 5.
[525] AÑÓN CALVETE, *Diligencias de Investigación Tecnológica*, cit., 3.

all'indagine; che lo svolgimento dell'atto sia tale da assicurare alle parti private un esercizio effettivo del diritto di difesa una volta terminate le operazioni[526].

2.2. Il principio di specialità.

In base al principio di specialità, l'adozione di una misura investigativa a carattere tecnologico deve essere relazionata a un delitto concreto e, pertanto, presuppone la sussistenza di una base indiziaria sufficientemente solida, dalla quale possa desumersi la probabile commissione di un reato. Tale regola di carattere generale serve, come detto, a evitare misure meramente esplorative e, in quanto tale, risulta idealmente collegata al principio di proporzionalità. Tale caratteristica dell'atto sarebbe radicalmente carente ove lo stesso venisse disposto in assenza di elementi obiettivi comprovanti l'esigenza concreta di procedere alla compressione del diritto fondamentale per soddisfare il contrapposto interesse statale alla repressione dei reati.

La necessaria sussistenza di dati obiettivi di commissione del reato, peraltro, consente di evitare che l'indagine straripi dai suoi confini ordinari, contrassegnati da una data ipotesi investigativa la cui corrispondenza a concreti elementi di fatto – sia pur non probatori in senso stretto – è necessario presupposto perché il soggetto sottoposto all'indagine possa esercitare, nei limiti connaturati alla fisionomia di tale fase, il diritto di difesa: ciò, evidentemente, presuppone una delimitazione per quanto possibile precisa dei fatti che gli si addebitano[527]. Peraltro, la solidità dei riscontri all'ipotesi investigativa già acquisiti permette anche di meglio calibrare il grado di invasione nei diritti fondamentali possibile nel caso di specie, anche in ossequio al precedentemente analizzato principio di proporzionalità in senso stretto, che impone di vagliare il corretto equilibrio fra i contrapposti interessi in campo, tra l'altro, sulla base della gravità degli indizi esistenti.

Ciò esclude che possano avere qualunque tipo di rilievo meri sospetti o allegazioni non sostenuti da dati obiettivi e, soprattutto, verificabili[528]: una recente sentenza del Tribunale Supremo si è espressa in tal senso in maniera piuttosto categorica con riferimento alle intercettazioni di comunicazioni, ribadendo che, perché sia costituzionalmente legittima, una ingerenza nel diritto al segreto delle comunicazioni

[526] AÑÓN CALVETE, *Diligencias de Investigación Tecnológica*, cit., 4.
[527] RICHARD GONZÁLEZ, *Investigación y prueba*, cit., 60.
[528] STS, 17 febbraio 2020, n. 52.

presuppone la verifica della presenza di indizi effettivamente costatabili e dotati di una certa potenzialità accreditativa. Tanto impone al soggetto che avanza la richiesta di applicazione della misura un penetrante onere di allegazione: costui, che si tratti del pubblico ministero o della polizia giudiziaria, è tenuto ad apportare al giudice istruttore gli elementi obiettivi sui quali si fonda il giudizio di probabilità di commissione del reato perché egli possa realizzarlo in maniera autonoma, non limitandosi a ratificare la ricostruzione del proponente in maniera vicaria[529].

Una fondamentale conseguenza del principio di specialità è quella per la quale l'atto abilitante deve essere costantemente associato alla investigazione di un delitto concreto. Ciò equivale a escludere che l'autorizzazione concessa in relazione all'investigazione di una certa ipotesi delittiva continui ad essere spendibile in relazione ad altre ipotesi di reato che dovessero emergere nel corso dell'attività investigativa medesima. Eventualità, questa, tutt'altro che remota se si considera che le misure di cui si discute sono, generalmente, destinate a protrarsi per un più o meno apprezzabile arco di tempo. Ciò ha condotto il legislatore a introdurre, per la prima volta, una disciplina espressa in materia di "*hallazgo casual*", termine con il quale si indica l'emersione di fatti di reato nuovi rispetto a quelli originariamente investigati e in relazione ai quali, dunque, sorge un duplice problema: da un lato, quello di sapere come deve procedersi ad avviare l'indagine per l'accertamento dell'ulteriore ipotesi di reato; dall'altro, quello di sapere se, nel procedimento eventualmente scaturito dall' *hallazgo casual*, gli elementi di prova acquisiti precedentemente e in maniera del tutto casuale siano utilizzabili.

Tale questione, originariamente sorta con riferimento all'istituto delle intercettazioni, era stata oggetto di molteplici – e non sempre convergenti – pronunce giurisprudenziali che, in assenza di una normativa legislativa espressa, avevano elaborato alcuni criteri e alcune regole specifiche. Con la riforma del 2015, il legislatore ha introdotto una disciplina specifica sul punto all'art. 588 *bis* i Lecrim, che si applica, in via generale, a tutte le misure investigative a carattere tecnologico.

Tale disciplina sarà analizzata nel prosieguo, quando ci si occuperà delle misure legislative specificamente volte al contenimento della circolazione indiscriminata dei

[529] Ancora, si legge nella pronuncia, a questo proposito, che «*la constatación de la solidez de esos indicios es parte esencial del proceso discursivo y valorativo que debe realizar el Juez antes de conceder la autorización. Es el Instructor quien ha de sopesar el nivel de probabilidad que se deriva de los indicios. Sólo cuando éste adquiera cotas que sobrepasen la mera posibilidad, estará justificada la injerencia*».

dati. Per ora, pare sufficiente rilevare come la normativa dettata dal legislatore sia decisamente più permissiva delle regole che la giurisprudenza aveva ricavato: sostanzialmente, i limiti alla circolazione probatoria dei risultati delle indagini tecnologiche sono quasi nulli. La scelta, dunque, sembra in qualche misura disarmonica rispetto alle soluzioni, altamente garantiste, escogitate dal legislatore spagnolo in punto di presupposti e requisiti della compressione dei diritti fondamentali coinvolti.

2.3. Il principio di proporzionalità e la sua trasposizione nel procedimento applicativo della misura.

Come si è già detto, la proporzionalità della misura rappresenta, nell'ottica del legislatore spagnolo, presupposto irrinunciabile della sua legittimità. Proprio per tale ragione, si prevede che tanto nella richiesta di autorizzazione della misura (art. 588 *bis* b, comma 2, n. 2) Lecrim), quanto nel provvedimento autorizzativo adottato dal giudice (art. 588 *bis* c, comma 3, lett. c) Lecrim) occorre dare conto delle ragioni per le quali la stessa si reputa conforme ai principi rettori indicati nel precedente art. 588 *bis* a Lecrim, a partire dal criterio della necessaria proporzione.

Coerentemente, pertanto, tale principio informa di sé tutta la disciplina normativa prevista in relazione alle singole misure di indagine tecnologica oltre che, naturalmente, la restante parte della disciplina comune alle stesse.

Alla luce di ciò, conformemente al principio di idoneità, si prevede la necessaria indicazione, nella richiesta di misura, del contenuto e della forma di esecuzione della stessa; lo stesso dicasi per quanto concerne l'enunciazione del fatto di reato per il quale si procede (in modo tale che il giudice possa procedere, conformemente al disposto dell'art. 588 *bis* c, comma 3, lett. a) Lecrim, a qualificarlo giuridicamente) e per il soggetto sottoposto all'investigazione, con la specificazione dei mezzi di comunicazione impiegati a tal fine e dell'unità investigativa di polizia giudiziaria incaricata dello svolgimento della misura e la durata di quest'ultima.

Nella richiesta, poi, devono essere esplicitati gli indizi di criminalità sussistenti che, con la denominazione di "indizi razionali"[530], compongono altresì il contenuto minimo della

[530] Sul punto, cfr. BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 9, che evidenzia come «*ni la doctrina ni la jurisprudencia, como ya se ha mencionado, establecen una diferenciación clara entre «sospechas razonables», «indicios racionales» y «delito probable» a la hora de medir el grado de sospecha. […] En definitiva, lo anterior significa que la solicitud de la medida del registro*

risoluzione giudiziale autorizzativa. Tale ultima esigenza non è corollario esclusivamente del precedentemente analizzato principio di specialità, ma si pone in diretto collegamento anche con quello di idoneità in quanto, contribuendo a delineare gli elementi obiettivi acquisiti in merito al fatto investigato – consente altresì verificare l'utilità concreta della misura prescelta per l'accertamento delle componenti del fatto già emerse e di quelle che si reputano di poter scoprire proprio grazie al suo svolgimento.

Conformemente, poi, al principio di eccezionalità e stretta necessità, il legislatore richiede l'esposizione dettagliata delle ragioni che la giustificano e della finalità perseguita dalla misura. Tale regola presuppone che, tanto nella richiesta di autorizzazione, quanto nella conseguente risoluzione giudiziale sia messo a punto un apparato motivazionale adeguato che, partendo dall'analisi dei fatti per i quali si procede, degli elementi obiettivi a loro riscontro, del contenuto e della durata della misura richiesta o accordata, dia conto del fatto che la stessa sia strettamente necessaria per le finalità perseguite e che un'altra misura meno gravosa non sia esperibile o, comunque, renda eccessivamente difficoltoso l'accertamento del delitto.

Con specifico riferimento alla durata della misura, l'art. 588 *bis* e Lecrim contiene una disciplina di carattere generale applicabile a tutte le investigazioni tecnologiche, fermo restando che, in relazione a ciascuna di esse, è la normativa di dettaglio a stabilire la durata massima in base alla gravità dell'ingerenza. In via generale, però, l'estensione temporale di ciascuna di esse deve rispettare quanto stabilito dall'art. 588 *bis* e Lecrim, che prevede che non possano durare oltre il tempo strettamente necessario per l'accertamento dei fatti[531]. È possibile, nondimeno, che il giudice, d'ufficio o previa richiesta motivata dell'organo che l'ha sollecitata, conceda una proroga laddove persistano le ragioni[532] che ne giustificarono originariamente l'adozione. Trascorso il termine originariamente previsto o quello prorogato, ad ogni modo, la misura cessa a

remoto de equipos informáticos debe referirse a unos hechos concretos y ha de explicar el origen de la información que sustenta las sospechas objetivas».

[531] Nel senso che la previsione di una durata massima delle misure restrittive dei diritti fondamentali è essenziale per assicurarne la proporzionalità, STC, 14 marzo 2011, n. 25.

[532] A questo fine, ai sensi dell'art. 588 *bis* f Lecrim, la richiesta di proroga deve contenere un'informativa dettagliata dei risultati fino a quel momento raggiunti con la misura e delle ragioni che ne giustificano la continuazione.

tutti gli effetti, con la conseguenza che elementi di prova eventualmente acquisiti successivamente devono reputarsi illegittimi[533].

Un contenuto del provvedimento autorizzativo di cruciale importanza per il soddisfacimento del criterio di stretta necessità della misura è quello previsto dalla lett. c) dell'art. 588 *bis* c Lecrim: il riferimento è all'indicazione dell'"*alcance*" della misura, ovvero della sua concreta estensione in relazione con gli elementi obiettivi del fatto di reato per il quale si procede. Tale indicazione, nell'ottica del legislatore spagnolo, dovrebbe consentire, in concreto, il contenimento della portata misura e la pertinenza degli elementi conoscitivi ricercati rispetto all'ipotesi di reato per la quale si procede. Si conseguirebbe, in tal modo, l'effetto di evitare che la risoluzione giudiziale che consente l'accesso, ad esempio, a un dispositivo informatico in vista della sua perquisizione si traduca in una sorta di autorizzazione in bianco a operare una ricerca a tappeto e, dunque, indiscriminata in tutti i dati in esso contenuti. Il tema è particolarmente interessante. Proprio la difficoltà di assicurare la pertinenza delle indagini informatiche è una delle questioni maggiormente dibattute in materia e che più di ogni altra condiziona il dibattito in merito alla effettiva possibilità di realizzare appieno, in questo campo, il principio di proporzionalità. La questione verrà, pertanto, trattata autonomamente nel prossimo paragrafo.

Per concludere, occorre fare riferimento al principio di proporzionalità in senso stretto che, come già anticipato, impone al giudice di verificare il corretto bilanciamento dei contrapposti interessi in campo sulla base dei criteri indicati dallo stesso testo di legge, secondo quanto si è già precedentemente osservato nei paragrafi 2 e seguenti.

2.3.1. Pertinenza della misura come necessario presupposto della proporzionalità della stessa: aspetti critici.

Come si diceva, al fine di assicurare la pertinenza – e, dunque, la proporzionalità[534] – della investigazione tecnologica rispetto all'ipotesi di reato oggetto di accertamento il legislatore spagnolo ha annoverato tra i contenuti essenziali del provvedimento autorizzativo quello dell'indicazione del cosiddetto "*alcance*" della misura, ovvero della sua concreta portata. In virtù di tale previsione, il giudice che autorizzi l'esecuzione di

[533] AÑÓN CALVETE, *Diligencias de Investigación Tecnológica*, cit., 4.

[534] CABEZUDO RODRÍGUEZ, *Ciberdelincuencia e investigación criminal*, cit., 24; ESPIN LOPEZ, *Investigacion sobre equipos informaticol y su prueba en el proceso penal*, Aranzadi, 2021, 75.

un mezzo di investigazione tecnologica è tenuto a predeterminare i "confini" dell'attività di ricerca svolta dagli inquirenti sulla base delle caratteristiche dell'investigazione in corso, del fatto da accertare e dei dati, utili all'accertamento, che si ritiene di poter acquisire con l'attività di ricerca medesima.

Lo scopo della previsione è, ovviamente, quello di arginare prassi investigative poco conformi al principio di proporzionalità, consistenti nella ricerca e apprensione indiscriminata di dati o informazioni relazionate ai sistemi informatici di uso comune, indipendentemente dalla loro effettiva pertinenza all'indagine in corso.

Concretamente, il giudice potrebbe ottemperare alla previsione legale in vario modo. Nel caso, ad esempio, di una perquisizione e sequestro di un *personal computer*, il provvedimento applicativo potrebbe individuare le cartelle o la tipologia di *file* all'interno dei quali può svolgersi la ricerca. Allo stesso modo, si potrebbe limitare la perquisizione solo a determinati applicativi del sistema informatico o a determinati *software*; o ancora, disporre il ricorso all'uso di *software* che consentano la individuazione dei *file* rilevanti tramite l'inserimento di determinate parole chiave. Le vie percorribili, insomma, sono diverse e dipendono, in buona sostanza, dalla tipologia di reato oggetto di accertamento e, naturalmente, dagli elementi di prova già acquisiti e quelli che si reputano acquisibili per mezzo dell'esecuzione della misura[535].

Tale regime è, ad ogni modo, mitigato da correttivi che consentono agli inquirenti di acquisire contenuti ulteriori eventualmente scoperti nel corso della ricerca e utili per l'accertamento dei fatti che potrebbero porsi al di fuori dei confini dell'"*alcance*" originariamente indicato nel provvedimento autorizzativo. In particolare, in relazione alla perquisizione e al sequestro informatico ("*registro*[536] *de dispositivos de almacenamiento masivo de información*"), sia in presenza (art. 588 *sexies* c, comma 3 Lecrim) che da remoto (art. 588 septies a, comma 3, Lecrim) il legislatore ha previsto la possibilità, per i soggetti preposti allo svolgimento della ricerca, di estenderla ad altri sistemi informatici o parte dei medesimi quando abbiano fondate ragioni per ritenere che i dati ricercati siano ivi memorizzati e sempre che siano accessibili per mezzo del

[535] Nel caso di un reato tributario, ad esempio, la ricerca potrebbe essere limitata ai *file* contenenti la contabilità del soggetto sottoposto all'indagine, mentre potrebbe risultare sproporzionato l'accesso a contenuti come fotografie, video e così via.

[536] Con il termine *registro*, si intende l'accesso al sistema informatico, cui può conseguire la acquisizione dei dati presenti nello stesso.

sistema informatico originario[537]. In ogni caso, l'estensione deve essere autorizzata dal giudice ma, in caso di *registro* informatico in presenza, il comma 4 dell'art. 588 *sexies* c Lecrim prevede la possibilità, per gli inquirenti, di procedere in via d'urgenza informando immediatamente il giudice che dovrà, poi, convalidare l'atto nelle settantadue ore successive all'adozione della misura[538].

Tali regole dovrebbero, nell'ottica del legislatore spagnolo, ovviare alle storture potenzialmente derivanti dalla circostanza che ad essere sottoposto a un'attività di ricerca non è uno spazio fisico ma virtuale. Come giustamente rilevato dalla dottrina di quel Paese, nel corso di una perquisizione "tradizionale" è del tutto fisiologico che vengano apprese le sole cose relazionate con il fatto delittivo. Al contrario, laddove la ricerca di elementi utili all'indagine si svolga in uno spazio virtuale, gli "oggetti" relazionati ai fatti di reato per i quali si procede non sono immediatamente visibili e la stessa maniera con cui i dati sono memorizzati su un dato dispositivo potrebbe rendere complicata la loro identificazione[539]. Ciò non giustifica, nell'ottica del legislatore spagnolo, un'attività di ricerca indiscriminata nel sistema informatico che, in quanto tale, confliggerebbe senz'altro con il principio di proporzionalità. Da ciò, l'imposizione al giudice di un obbligo di motivazione "rafforzato" rispetto a quello che sarebbe tipico di una perquisizione in un luogo fisico, con la conseguente delimitazione della concreta portata della misura.

Se, tuttavia, su un piano astratto la soluzione escogitata dal legislatore spagnolo pare idonea ad assicurare la pertinenza della misura rispetto al perimetro dell'indagine in corso, su un piano più squisitamente pratico il raggiungimento di un simile obiettivo può essere più complicato di quanto sembri.

---

[537] Secondo una lettura dottrinale, ciò implicherebbe la possibilità di estendere la ricerca ai dati memorizzati in altra rete privata o nel *cloud*, CABEZUDO RODRÍGUEZ, *Ciberdelincuencia e investigación criminal*, cit., 45-46. Se così fosse, le capacità esplorative degli inquirenti risulterebbero fortemente ampliate. Basti pensare al fatto diversi marchi di elettronica, sfruttando il sistema della cosiddetta "nube", consentono di far confluire in un unico spazio digitale i dati memorizzati in dispositivi fisici differenti appartenenti al medesimo usuario. In casi di questo tipo, l'accesso a uno solo dei dispositivi informatici consentirebbe, di fatto, un'intrusione contestuale in tutti gli altri dispositivi adoperati dal soggetto. Ragionevolmente, dunque, si prevede che l'estensione della ricerca sia subordinata all'autorizzazione del giudice.

[538] CONDE-PUMPIDO TOURÓN, *La reforma procesal. Registros de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informático*, in *Jornadas de especialistas en materia de criminalidad informática, Centro de estudios jurídicos*, 2016, 8. Come si vedrà successivamente, la medesima possibilità non è prevista in relazione all'accesso remoto al sistema informatico.

[539] BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 27.

In primo luogo, in ragione delle peculiarità dell'ipotesi investigativa formulata dagli inquirenti è possibile che una effettiva limitazione della portata della misura non sia praticabile. Ciò può verificarsi, in particolare, nei procedimenti relativi a ipotesi di reato che, in dipendenza della stessa formulazione della fattispecie incriminatrice[540], sono deputate all'accertamento di elementi fattuali o condotte non predeterminabili a priori. È il caso, ad esempio, delle fattispecie associative: la dimostrazione dell'esistenza del vincolo associativo non trova, generalmente, riscontro in dinamiche fattuali o comportamentali relative esclusivamente ad alcuni segmenti della vita del soggetto investigato. Più spesso, in ciascuno di tali segmenti può rinvenirsi un elemento dimostrativo della sua appartenenza all'associazione. In tali casi, una delimitazione previa dell'ambito della ricerca potrebbe impedire l'apprensione di dati potenzialmente molto rilevanti per l'accertamento dei fatti. O ancora, si pensi a un'ipotesi di omicidio: anche in questo caso, elementi di riscontro all'individuazione di un determinato autore possono rinvenirsi negli ambiti più disparati della sua quotidianità.

Altro fattore che potrebbe incidere sull'effettività di una simile regola è la volatilità dei dati digitali, che, come ormai più volte emerso, sconsiglia di procedere a una selezione dei dati da apprendere. Al fine di evitare modifiche o cancellazioni degli stessi, dunque, si dovrebbe procedere a una previa apprensione dell'intero contenuto del sistema informatico, per poi procedere ed estrapolare le sole informazioni rilevanti in un secondo momento. Che una simile soluzione, però, sia conforme al principio di proporzione – per come, peraltro, interpretato dalla giurisprudenza della Corte di Strasburgo[541] – è cosa di cui è lecito dubitare: essa, infatti, presuppone che la compressione delle prerogative costituzionali e convenzionali incise dalla misura si realizzi solo al momento dell'accesso ai dati e non al momento della loro sottrazione all'esclusiva disponibilità del soggetto inciso dalla misura. A ciò si aggiunga che anche l'eventuale, successiva eliminazione dei dati raccolti non funzionali all'indagine

[540] Nel senso che il ricorso a programmi informatici che consentono di individuale i *file* rilevanti per l'indagine tramite l'inserimento di parole chiave potrebbe non essere sempre adeguato e condurre, in alcuni casi, a scartare materiale utile all'indagine, ancora, Bachmaier Winter, *Registro remoto de equipos informáticos*, cit., 29.

[541] Dubita di ciò anche la dottrina spagnola. Cfr. BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit, 30 ss., che evidenzia come, in un caso relativo alla perquisizione di un *computer* di uno studio professionale di un avvocato, la Corte europea dei diritti dell'uomo ha reputato che l'apprensione di un numero molto elevato di dati non relazionati con l'investigazione violasse la Convenzione. L'autrice evidenza come, se questa giurisprudenza dovesse reputarsi applicabile in via generale nel caso di perquisizione e sequestro di materiale informatico, la clonazione dell'intero contenuto del dispositivo informatico per poi procedere alla selezione dei dati dovrebbe reputarsi vietata.

presupporrebbe, comunque, la loro cognizione da parte degli investigatori e la possibilità di procedere a una vera e propria profilazione del soggetto sottoposto all'indagine.

Sotto altro punto di vista, poi, una delimitazione, *a priori*, del contenuto del sistema informatico analizzabile, con l'indicazione, ad esempio, delle cartelle e delle tipologie di documenti ai quali limitare la ricerca potrebbe essere ostacolata dalla circostanza che, evidentemente, prima dell'accesso al sistema informatico gli investigatori potrebbero non avere idea di come lo stesso sia stato effettivamente articolato e organizzato dall'usuario.

Da ultimo, deve segnalarsi che la soluzione in commento potrebbe rivelarsi strutturalmente inefficace nel caso del cosiddetto *registro remoto*. Tanto in ragione della stessa fisionomia della misura investigativa in questione, tesa a realizzare un controllo perdurante sul dispositivo bersaglio e, dunque, a consentire l'acquisizione di una serie futura di dati dalla più disparata natura, rispetto ai quali una previa delimitazione non sarebbe sempre concretamente praticabile.

In un simile scenario, il rischio di un ricorso sistematico a pratiche investigative sproporzionate è reale. Per avvedersi di ciò, d'altronde, basta far cenno alle linee guida diramate dalla *Fiscalía General* dello Stato spagnolo nel 2019[542]. Nelle stesse si sostiene, infatti, che un accesso al contenuto dell'intero dispositivo informatico non sarebbe sproporzionato nel caso in cui «*se investiguen comportamientos delictivos capaces de generar registros informáticos de distinta naturaleza. Sería el caso, por ejemplo, de la investigación de delitos complejos, como el tráfico de drogas y blanqueo de capitales, que exigiría registrar la práctica totalidad de los datos almacenados (comunicaciones, datos económicos, fotografías, vídeos…). Otro tanto ocurriría en el caso de la investigación de delitos especialmente graves, en los que el principio de proporcionalidad podría justificar una intromisión más relevante en el conjunto de datos que conforman el entorno digital de una persona*». Conseguentemente, «*lo realmente determinante para la validez de la medida, lo que hará que la misma resulte ajustada a derecho, será siempre que la resolución habilitante haya fijado un determinado alcance del registro –que podrá ser de todo el dispositivo o de parte del mismo–, y que, al mismo tiempo, haya reflejado las razones y motivos en los que*

[542] Cfr. Boletín Oficial del Estado, n. 70, 22 marzo 2019, Sec. III.

descansa esa decisión. A partir de aquí, será la razonabilidad o no del juicio valorativo, lo que dará validez o no a la decisión judicial».

Prescindendo dalle disfunzioni e storture che nella prassi possono derivare da una lettura "aperturista" del tipo di quella segnalata[543], non sembra che la mera difficoltà di individuare a priori la direzione più opportuna da impartire alla ricerca possa giustificare l'aprioristica rinuncia alla individuazione di qualsivoglia limite all'attività investigativa – potenzialmente sterminata – realizzabile. Difficoltà, peraltro, che ben potrebbe derivare dallo stato embrionale dell'indagine o, addirittura, da una non adeguata conduzione della stessa da parte degli organi inquirenti.

Allo stesso modo, che per il solo fatto che si proceda in relazione a un reato grave sia legittimo scandagliare l'intera esistenza digitale di un sospettato è cosa di cui è lecito dubitare. In termini di proporzionalità, a ben vedere, le valutazioni da compiere in ordine alla gravità del reato e alla definizione dell'ambito applicativo concreto della misura si pongono su due piani distinti (il primo, quello della proporzionalità in senso stretto della misura, il secondo quello della sua pertinenza e, dunque, necessità) ed autonomi. In altri termini, il solo fatto che il reato per cui si procede sia particolarmente grave non giustifica che possa rinunciarsi *tout court* alla necessaria pertinenza della misura. Tanto per la banale ragione che ciò condurrebbe irrimediabilmente a escludere la corrispondenza della stessa al canone di necessità.

In definitiva, se il rispetto del canone della necessaria pertinenza della misura è risultato il cui raggiungimento non sempre può essere concretamente assicurato nel caso di perquisizione e sequestro informatici (tradizionali e da remoto), esso appare una vera e propria chimera nel caso di effettuazione di una sorveglianza perdurante del dispositivo informatico del soggetto investigato.

In considerazione di ciò, come si è visto nel Capitolo precedente, acquisisce peculiare rilievo la predeterminazione dei reati per i quali possono disporsi le misure in commento in termini quanto più possibile restrittivi. Soluzione, quest'ultima, non certamente risolutiva alla luce di quanto è stato appena osservato, ma in grado, quanto meno, di ridurre l'impatto complessivo di simili tecniche sui diritti dei singoli.

[543] La pratica giudiziaria testimonia, d'altronde, l'allarmante abbassamento dei livelli qualitativi delle motivazioni dei provvedimenti giudiziari, dovuta anche al sovraccarico di lavoro dei magistrati.

Oltre a ciò, è quanto mai opportuna la proposta, formulata nell'ambito della dottrina spagnola[544], di limitare la circolazione probatoria dei risultati di prova ottenuti e impedirne l'utilizzazione in procedimenti relativi a reati diversi. Ciò consentirebbe, quanto meno, di scongiurare il più preoccupante degli effetti negativi connessi alla possibilità di realizzare intrusioni a così ampio spettro nella riservatezza dei cittadini, da rinvenirsi nella strumentalizzazione delle misure in discorso a fini preventivi[545].

2.4. Limiti alla circolazione indiscriminata dei dati: garanzie relative all'utilizzo della prova in altri procedimenti e distruzione dei dati.

L'elevata invasività delle misure in argomento e l'ingente quantitativo di dati che le stesse permettono di raccogliere rendono la questione relativa ai limiti alla circolazione indiscriminata dei medesimi successivamente alla loro raccolta di cruciale importanza. Per tale ragione, la disciplina articolata dal legislatore spagnolo sul punto appare scarsamente incisiva e sembra mossa da una *ratio* distonica rispetto a quella che ha improntato l'intervento legislativo nel suo complesso. All'elevato rigore delle garanzie che contrassegna la prima parte delle misure comuni alle misure di investigazione tecnologica fa da contraltare l'ampio margine lasciato alla circolazione probatoria dei dati.

Ai sensi dell'art. 588 *bis* i Lecrim, infatti, l'utilizzazione delle informazioni ottenute per il tramite delle misure tecnologiche di indagine in procedimenti diversi è regolata dall'art. 579 *bis* Lecrim, che disciplina l'uso in altri procedimenti dei risultati ottenuti con l'apertura della corrispondenza scritta o telegrafica. In ragione della tutto sommato limitata quantità di dati e informazioni acquisibili per il tramite di tale atto acquisitivo, la norma in questione non prevede un regime improntato a particolari *standard* di garanzia, limitandosi a sancire che «*la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal*». A tal fine, è sufficiente che nel procedimento nel quale i risultati probatori vengono riversati si proceda all'acquisizione delle prove testimoniali

[544] BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 32.

[545] Nel senso che la circostanza che le investigazioni si dirigano a fatti o persone non relazionati con la *notitia criminis* e siano, dunque, esorbitanti costituisce un segnale rivelatore dell'esistenza di una *inquisitio generalis*, nella quale il procedimento è strumentalizzato al servizio di una investigazione illimitata e obiettivamente indefinita, AGUILERA MORALES, *Proceso penal y causa general*, Thomson, 2008, 85.

occorrenti ad accreditare la legittimità dell'originaria ingerenza e che si alleghi la documentazione a tal fine necessaria che, in ogni caso, deve contenere la richiesta di applicazione della misura, l'atto giudiziale con la quale fu accordata e le eventuali proroghe accordate. Quanto, invece, al caso in cui, in ragione dell'applicazione della misura, vengano scoperti nuovi delitti non coperti dall'atto autorizzativo iniziale (cosiddetto "*hallazgo casual*"), la loro investigazione può continuare previa ulteriore autorizzazione del giudice competente, che la rilascia solo nel caso in cui reputi che non fosse stato possibile richiedere la misura fin dal principio anche con riferimento al reato casualmente scoperto.

In tal modo, il legislatore spagnolo ha risolto buona parte dei problemi interpretativi che, antecedentemente alla riforma del 2015, riguardavano la questione dell'"*hallazgo casual*", ossia l'individuazione delle condizioni alle quali, scoperto in ragione di una certa attività di indagine un delitto non conosciuto antecedentemente, l'investigazione potesse continuare in relazione al nuovo reato e gli elementi di prova raccolti potessero essere usati nel nuovo procedimento. La questione, in assenza di una normativa specifica sul punto, era divenuta particolarmente dibattuta con riferimento alle scoperte casuali di reati ulteriori realizzate a seguito dell'attività di intercettazione, conducendo allo stratificarsi di orientamenti giurisprudenziali non sempre coerenti tra loro.

In via generale, il principio cui la giurisprudenza spagnola si era costantemente ispirata in materia – pur con differenti sfumature – è quello della cosiddetta "*prohibición de novación*", quale logico corollario del principio di specialità: dato che la legittimità di una misura restrittiva dei diritti fondamentali presuppone che la misura medesima sia e permanga collegata a un determinato delitto concreto, l'originaria autorizzazione non copre nuovi delitti che dovessero essere scoperti nel corso dell'esecuzione della stessa[546]. In ragione di ciò, le prime pronunce giurisprudenziali sul punto erano particolarmente rigorose nell'escludere la possibilità di utilizzare i risultati di prova ottenuti in virtù di una autorizzazione collegata a un certo delitto concreto per l'accertamento di reati diversi scoperti casualmente in costanza di esecuzione della misura. Tale rigore era andato, poi, attenuandosi nella giurisprudenza successiva, che si era attestata nel senso della mancata violazione del principio di specialità nel caso in cui

[546] Vedi NADAL GÓMEZ, *El régimen de los hallazgos casuales en la ley 13/2015, de modificación de la ley de enjuiciamiento criminal,* in *Revista General de Derecho Procesal*, 40, 2016, 37 ss., anche per la ricostruzione che segue.

l'*hallazgo casual* non comportasse una novazione del tipo penale investigato e fosse, dunque, in qualche misura riconducibile al perimetro investigativo originario. In tal caso, si ammetteva altresì che, in presenza di certi presupposti, i risultati probatori relativi al nuovo delitto potessero essere usati nel diverso procedimento avviato per il suo accertamento non solo alla stregua di una mera *notitia criminis*, ma di vera e proprio mezzo di prova, purché lo stesso fosse relativo a reati per i quali avrebbe potuto, fin dal principio, disporsi l'intercettazione[547].

In ragione del consolidamento di tale linea interpretativa[548], la scoperta di un nuovo delitto nel corso delle intercettazioni imponeva, anzitutto, agli inquirenti di informare il giudice e di richiedere allo stesso il rilascio dell'autorizzazione per la prosecuzione dell'indagine in relazione al nuovo reato, con l'eccezione del caso in cui la scoperta non avesse comportato una novazione del tipo penale investigato, nel qual caso l'ulteriore autorizzazione non era richiesta e i risultati conoscitivi ottenuti potevano essere utilizzati anche per la prova del fatto nuovo. Nel caso, invece, in cui il nuovo delitto presentasse una connessione con quello per il quale era stata richiesta l'intercettazione ai sensi dell'art. 17 Lecrim[549], quanto scoperto poteva utilizzarsi non solo come *notitia criminis*, ma anche come prova nell'ulteriore procedimento a patto che fosse stata richiesta e ottenuta un'integrazione dell'originaria autorizzazione giudiziale. Nel caso di fatti non connessi, invece, si sarebbe dovuto procedere, secondo le norme ordinarie, a informare il giudice competente, che avrebbe avviato il nuovo procedimento e disposto, al ricorrere dei presupposti, l'attività intercettiva. Quanto agli esiti di quella precedentemente svolta, essi si sarebbero potuti usare solo come *notitia criminis*.

---

[547] STS, 6 maggio 2011, n. 362, per la quale «*la intervención telefónica requiere que la medida sea necesaria, proporcionada y motivada. Si estos requisitos se cumplen carece de relevancia que la medida haya sido dispuesta en unas diligencias en las que los recurrentes no eran perseguidos...los hallazgos casuales no carecen de validez como prueba, cuando han sido obtenidos de una manera jurídicamente no objetable". Sentencia esta que recoge la doctrina ya sentada con mayor amplitud en la S. 1313/2000 de 21.7; al precisar que "en el derecho penal europeo, la regla que rige al respecto viene a establecer que si los hallazgos casuales fueron obtenidos en condiciones en las que se hubiera podido ordenar la interceptación de las comunicaciones telefónicas, la utilización de los mismos en otra causa no vulnera ningún derecho. El parágr. 100 b) de la Ordenanza procesal penal alemana (StPO) prevé una autorización expresa en este sentido y el Código de procedimientos penales italiano, que excluye en principio la utilización en otro proceso, admite, sin embargo, una excepción para los casos de delitos de cierta gravedad que contempla el art.389 CPrP (ver art. 270 del mismo código)*».

[548] Cfr. per la sua particolare chiarezza ricostruttiva, STS, 14 marzo 2013, n. 291.

[549] Trattasi, in buona sostanza, dei casi di delitti commessi da persone riunite o in concerto tra loro, dei delitti strumentali alla commissione di altri o ad assicurare la loro impunità, dei delitti commessi in danno reciproco, del delitto di favoreggiamento o riciclaggio di capitali rispetto al loro antecedente. A tali casi specifici, va aggiunto quello di delitti non connessi che, però, siano stati commessi dalla stessa persona e si trovino in rapporto di analogia o relazione tra loro.

Il regime così ricostruito dalla giurisprudenza assicurava, entro certi limiti, un argine alla circolazione indiscriminata delle prove in procedimenti diversi.

La normativa nel 2015, al contrario, sembra muoversi nell'opposta direzione di dilatare a dismisura le possibilità di circolazione probatoria del materiale raccolto.

Nella nuova regolamentazione, viene meno la distinzione tra reati connessi e non connessi; allo stesso modo, non si prevede che l'utilizzo probatorio dei risultati delle captazioni sia limitato ai procedimenti aventi ad oggetto un reato in relazione al quale si sarebbe potuta, in ipotesi, disporre l'intercettazione.

In virtù della disciplina attualmente vigente, in buona sostanza, i risultati probatori acquisiti per il tramite di una attività investigativa che abbia condotto alla scoperta casuale di delitti diversi sono spendibili in altri procedimenti sol che ricorrano i seguenti presupposti: che l'atto di indagine compiuto sia conforme alla legge e ciò deve essere appurato – nel procedimento diverso in cui devono essere utilizzati i suoi risultati – tramite lo svolgimento di una prova testimoniale; che il giudice competente all'accertamento dell'ulteriore reato scoperto casualmente autorizzi, in relazione a quel delitto, la prosecuzione delle investigazioni, valutando – sulla base delle circostanze della scoperta casuale – l'impossibilità di includere fin dal principio nella richiesta di autorizzazione della misura il nuovo fatto di reato[550]. Stante la formulazione della norma, deve ritenersi che la mancanza di tale autorizzazione impedisca non solo la continuazione dell'indagine in relazione al nuovo delitto, ma altresì l'uso probatorio dei risultati ottenuti in altri procedimenti. Trattasi di una lettura che sembra conforme alla *ratio* della disposizione in quanto, in tal caso, mancherebbe una valutazione giudiziale in merito alla effettiva casualità della scoperta. Si evitano, in tal modo, prassi poco ortodosse, come quella di procedere a investigazioni meramente esplorative con la prospettiva di utilizzarne i risultati in relazione a qualsivoglia reato emerga dalle stesse[551].

Al di là, poi, del caso in cui si scopra un delitto non originariamente conosciuto dagli investigatori, l'utilizzazione dei risultati di prova ottenuti in altri procedimenti risulta assoggettata al semplice presupposto che l'atto investigativo fosse legittimo e alla dimostrazione di ciò tramite l'allegazione della relativa documentazione e

[550] NADAL GÓMEZ, *El régimen de los hallazgos casuales*, cit., 45.
[551] Di nuovo, NADAL GÓMEZ, *El régimen de los hallazgos casuales*, cit., 48.

l'acquisizione di una prova testimoniale, da svolgersi nel procedimento in cui la prova deve essere riversata.

Nel complesso, una simile disciplina non sembra suscettibile di assicurare adeguati limiti alla circolazione di prove tra procedimenti distinti e rischierebbe, soprattutto in certi contesti investigativi[552], di favorire un abuso al ricorso a strumenti di indagine fortemente invasivi al fine di accumulare materiale probatorio spendibile anche in processi diversi. L'assetto antecedente alla riforma, pur essendo il frutto dello stratificarsi di orientamenti giurisprudenziali non sempre coerenti, aveva avuto il pregio di evitare una circolazione sostanzialmente indiscriminata di elementi probatori raccolti per il tramite di attività restrittive di un diritto fondamentale di elevato rango, quale è quello di comunicare riservatamente. Nell'intento di fornire una risistemazione della materia e di stabilire una disciplina chiara ed unitaria, il legislatore ha allargato fortemente le maglie della "circolabilità" della prova tra distinti procedimenti. Tanto, peraltro, nonostante la nuova normativa si riferisca anche ad attività investigative che, rispetto a una intercettazione tradizionale, consentono l'acquisizione di una mole di dati e informazioni incomparabilmente maggiore e sono caratterizzate da una maggiore attitudine esplorativa.

D'altronde, proprio la *ratio* di evitare un'eccessiva circolazione della mole di elementi e informazioni acquisibili con il ricorso alle investigazioni tecnologiche ispira la disciplina dettata in tema di cancellazione dei dati una volta che la loro conservazione non sia più necessaria. Così, opportunamente, l'art. 588 *bis* k Lecrim stabilisce che, una volta concluso il procedimento mediante sentenza passata in giudicato, occorre ordinare l'eliminazione degli originali memorizzati sui sistemi informatici utilizzati per l'esecuzione delle misure, previa realizzazione di una copia la cui conservazione è affidata al segretario giudiziario. Quanto alla distruzione delle copie, la stessa può disporsi, ove il giudice non reputi necessaria la loro conservazione, trascorsi cinque anni dall'esecuzione della pena, dalla prescrizione del reato o della pena, o dalla assoluzione dell'investigato.

[552] Si pensi, ad esempio, alle indagini relative alle associazioni di stampo mafioso. La prassi già attesta l'esistenza di marcate contaminazioni a livello investigativo e probatorio tra procedimenti diversi afferenti a contesti criminali contigui.

3. Il *registro remoto*.

Tra le misure investigative a carattere tecnologico introdotte nel 2015 il legislatore spagnolo ha previsto specificamente quella dell'accesso remoto a un dispositivo informatico di memorizzazione massiva dei dati, innestando la relativa regolamentazione all'art. 588 *septies* a Lecrim. In tal modo, come può leggersi nel punto n. IV del Preambolo alla Ley Organica 13/2015, si è inteso superare il vuoto normativo che caratterizzava la materia e adeguare la legislazione dello stato a quella di altri sistemi europei, nei quali la misura risultava già prevista.

La scelta del legislatore spagnolo, dunque, è stata quella di distinguere nettamente, sul piano del trattamento processuale, l'intrusione occulta e da remoto nel sistema informatico dall'istituto, contiguo ma profondamente distinto per grado di intrusione nei diritti individuali, della semplice perquisizione informatica realizzata "in presenza", la cui disciplina è contenuta nel precedente art. 588 *sexies* Lecrim[553].

La netta percezione della differente invasività delle due misure[554] si coglie in alcuni punti nodali della loro regolamentazione, a partire dalla limitazione dell'ambito applicativo dell'accesso remoto a una serie di delitti particolarmente gravi. Demarcazione che, invece, non caratterizza la misura di cui all'art. 588 *sexies* Lecrim che, astrattamente, potrebbe autorizzarsi in relazione a qualsivoglia fattispecie di reato[555].

---

[553] Si prevede la necessaria autorizzazione del giudice (art. 588 *sexies* b Lecrim). Peraltro, il legislatore ha chiaramente esplicitato il principio della necessaria motivazione individualizzata per l'esecuzione della misura. Si è escluso, così, che alla stessa possa procedersi nel corso della perquisizione domiciliare, pur previamente autorizzata, nella quale si rinvengano *computer*, strumenti di comunicazione o, comunque, dispositivi elettronici di memorizzazione di massa delle informazioni digitali in mancanza di apposita autorizzazione all'accesso al contenuto del dispositivo. Dunque, anche laddove la misura si inserisca nel contesto di una più ampia operazione investigativa, è imprescindibile l'autorizzazione del giudice alla realizzazione dell'intrusione nel dispositivo; autorizzazione che, eventualmente, può concedersi in seguito all'apprensione fisica del dispositivo medesimo ove non fosse già stata rilasciata antecedentemente. In caso di urgenza, tuttavia, l'accesso al dispositivo è consentito anche senza la previa autorizzazione giudiziale, fermo restando l'esigenza di una successiva convalida da parte del giudice. Il comma 4 dell'art. 588 *sexies* c Lecrim, infatti ove si apprezzi un interesse costituzionale legittimo che renda imprescindibile la misura, la polizia giudiziaria può procedere in via d'urgenza all'esame dei dati contenuti nel dispositivo elettronico dandone comunicazione al giudice non oltre le ventiquattro ore. La misura deve essere convalidata entro settantadue ore dal momento in cui fu ordinata.

[554] Nel prossimo paragrafo si analizzeranno specificamente le ricostruzioni della dottrina e della giurisprudenza spagnola relativamente al diritto fondamentale inciso dalle due misure.

[555] Nel senso che il *registro remoto* sia nettamente più invasivo del suo corrispondente "in presenza", RICHARD GONZÁLEZ, *Investigación y prueba*, cit., 198. DELGADO MARTÍN, *Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015,* in *Diario La Ley*, n. 8693, Sección Doctrina, 2 febbraio 2016, 11, evidenzia come nel *registro remoto* si determina un'ingerenza avente carattere continuativo, suscettibile di aumentare tanto l'estensione quanto l'intensità della restrizione dei diritti del singolo in ragione della prolungata possibilità per gli investigatori di accedere a

In prima approssimazione, ma ciò sarà ulteriormente argomentato nelle pagine a venire, l'analisi della regolamentazione messa a punto dal legislatore spagnolo lascia trapelare come, rispetto all'introduzione di una disciplina relativa al sequestro e alla perquisizione informatica tradizionali, quella relativa al corrispondente strumento da remoto non fosse stata avvertita con la medesima urgenza né con il medesimo grado di attenzione ed elaborazione da parte di dottrina e giurisprudenza. Tanto si è riflesso nel più elevato livello di dettaglio che contrassegna la regolamentazione del primo istituto, a fronte di una disciplina che, come si vedrà, è per molti versi laconica in relazione al secondo.

La ragione di ciò è da rinvenirsi, probabilmente, nello scarso utilizzo che gli organi investigativi di quel paese hanno fatto – e, per verità, continuano a fare in ragione di pretese difficoltà tecniche riscontrate al momento dell'inoculazione del *virus* nel dispositivo informatico[556] – del mezzo investigativo in questione, dimostrato dalla quasi totale assenza di precedenti giurisprudenziali rilevanti in materia.

Prima della riforma, infatti, la questione relativa alla legittimità dell'accesso in un dispositivo informatico nel corso dell'investigazione si era posta soprattutto con riguardo all'analisi di dispositivi elettronici rinvenuti nel corso di una perquisizione locale e, in particolare, domiciliare. La mancanza di una disciplina specifica sul punto aveva fatto insorgere il problema della legittimità di una simile attività di indagine nel caso di mancanza, nel provvedimento autorizzativo della perquisizione domiciliare, della specifica autorizzazione ad accedere altresì al contenuto del dispositivo informatico eventualmente rinvenuto nel corso della stessa. A fronte del consolidarsi di una prima linea interpretativa aperturista[557], la giurisprudenza di legittimità aveva poi finito per affermare l'illegittimità di tale prassi sul presupposto che l'autorizzazione giudiziale all'accesso nel domicilio non fosse suscettibile di fornire copertura altresì

---

tutto il contenuto del dispositivo informatico bersaglio. Si veda, sul punto, anche BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 7, che critica la tesi secondo la quale l'accesso da remoto al dispositivo informatico sarebbe nulla più che una peculiare modalità tecnica di realizzare una perquisizione informatica ricorrendo al duplice argomento del suo carattere occulto e della durata nel tempo dell'intrusione.

556 SÁNCHEZ RUBIO, *Los registros remotos sobre equipos informáticos: la investigación del «hacker legal»*, in AA.VV., *Fodertics 6.0 los nuevos retos del derecho ante la era digital*, a cura di Bueno de Mata, Comares, 2017, 212.

557 Cfr. nota 458.

all'accesso al dispositivo informatico, in ragione della natura e dell'estensione delle prerogative costituzionali incise per il suo tramite[558].

Un simile dibattito non si era, invece, sviluppato con riferimento all'accesso da remoto al dispositivo informatico. Proprio a tale circostanza sembra altresì riconducibile la mancanza di una riflessione dottrinale e giurisprudenziale in merito all'esistenza di una distinzione netta tra le prerogative costituzionali incise dalle due misure[559]. Il tema merita di essere autonomamente trattato.

3.1 I beni costituzionali incisi.

Al momento di individuare le prerogative costituzionali incise dall'accesso ai dispositivi informatici dei singoli per trarne elementi di riscontro all'ipotesi investigativa la dottrina e la giurisprudenza spagnole non sembrano distinguere tra le varie alternative esperibili, rappresentate dall'accesso realizzato in presenza (dunque, con la disponibilità fisica del dispositivo medesimo), dall'accesso remoto con apprensione immediata e istantanea dei dati e dall'accesso prolungato nel tempo, con la conseguente sottoposizione dell'utilizzatore del dispositivo a una vera e propria sorveglianza.

La mancanza di una simile distinzione, tuttavia, acquista in quell'ordinamento uno scarso rilievo almeno per due ordini di ragioni: in primo luogo, in quanto, come si è visto in apertura del capitolo, non è mai stata in discussione l'incidenza di simili misure, quanto meno, sul diritto all'intimità, rientrante tra quelle prerogative costituzionali per la cui restrizione è imprescindibile l'esistenza di una base legale. A differenza, quindi, dell'ordinamento italiano, quello spagnolo esclude per definizione l'esperibilità di simili misure in assenza di una legge abilitante.

In secondo luogo, in quanto l'evoluzione del dibattito giurisprudenziale e dottrinale in materia di beni incisi dall'intrusione dei pubblici poteri nelle aspettative di riservatezza tecnologica dei singoli ha condotto alla maturazione di un indirizzo ermeneutico che riconduce tutte le tre alternative prima tracciate sotto il ventaglio di un'unica

[558] Cfr. STS, 17 aprile 2013, n. 342, che sarà successivamente analizzata con specifico riferimento alle considerazioni in essa contenute con riguardo al bene giuridico inciso dall'accesso al dispositivo informatico del soggetto sottoposto all'indagine. Proprio in virtù dell'affermazione di un simile principio si spiega la circostanza che la disciplina introdotta con la riforma del 2015 preveda la necessità di un'autorizzazione specifica all'accesso al dispositivo informatico anche nel caso di previa risoluzione giudiziale autorizzativa di una perquisizione domiciliare.

[559] Nonostante ciò, come già detto, l'osservazione per la quale il *registro remoto* comporta un'intrusione molto più marcata nelle prerogative individuali è ricorrente in dottrina e ha certamente determinato alcune differenze di disciplina tra i due istituti.

prerogativa – come si vedrà, inedita – il cui rango è unanimemente riconosciuto come particolarmente elevato ed esigente la tutela più intensa possibile.

Nonostante, per le ragioni appena dette, il dibattito sviluppatosi nell'ordinamento Spagnolo sul tema in questione non abbia l'importanza che ha assunto nel nostro – in cui, come si è visto, ha una dimensione pratica fondamentale nella misura in cui i suoi esiti possono spostare l'ago della bilancia nel senso della utilizzabilità o meno di certi risultati investigativi – è nondimeno interessante costatare come esso si sia sviluppato lungo una traiettoria in buona parte sovrapponibile a quella che ha contrassegnato il suo corrispondente italiano. Da questo punto di vista, può certamente dirsi che entrambi gli ordinamenti hanno subito l'influsso delle riflessioni avviate dalla Corte costituzionale tedesca[560] nel lontano 1983 in merito alla portata e al rango delle prerogative vantate dai singoli a fronte delle sempre più ampie potenzialità dell'intrusione statale nell'uso riservato delle tecnologie informatiche.

Nell'ordinamento spagnolo, tale riflessione ha condotto all'affermazione di un diritto alla protezione dell'"*entorno virtual*", definito come il congiunto delle informazioni in formato digitale che una persona genera per il tramite delle attività realizzate mediante dispositivi elettronici, in maniera consapevole o inconsapevole, volontaria o involontaria[561].

Sul piano dogmatico, la giustificazione razionale dell'esistenza di un simile diritto è stata tradizionalmente rinvenuta nell'insufficienza delle singole prerogative costituzionali espressamente tutelate in sé considerate a dare conto delle peculiarità e dell'intensità dell'intrusione nella "vita tecnologica" del singolo. Tanto alla luce, anzitutto, del carattere polifunzionale degli strumenti tecnologici di uso quotidiano, che non consente di limitare la individuazione del bene inciso a questa o quella prerogativa costituzionale e conduce, invece, all'identificazione di una nuova entità suscettibile di trascendere quelle aventi *nomen iuris* proprio. Di ciò dà perfettamente conto la celebre pronuncia con cui il Tribunale Supremo, nell'anno 2013, ha espressamente riconosciuto l'esistenza di tale prerogativa. Nella sentenza del 17 aprile di quell'anno, n. 342[562], il giudice di legittimità spagnolo ha evidenziato come la ponderazione delle ragioni che

[560] Cfr. cap. 1.
[561] DELGADO MARTÍN, *Investigación del entorno virtual*, cit., 3.
[562] L'orientamento in questione è stato costantemente riaffermato. Si vedano: STS, 28 febbraio 2015, n. 823; STS, 4 luglio 2017, n. 508.

nel contesto di una investigazione penale giustificano il sacrificio dei diritti dell'usuario di un dispositivo informatico debba effettuarsi senza perdere di vista il carattere multifunzionale dei dati che nello stesso sono memorizzati. Tale caratteristica conduce ad affermare che il trattamento giuridico di quei dati – e, conseguentemente, dei limiti imposti ai pubblici poteri nell'accesso ai medesimi – è più adeguato se essi si contemplano di forma unitaria: «*más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual*». Tale diritto, secondo il Tribunale, rappresenterebbe sì una manifestazione di diritti costituzionali già espressamente riconosciuti, ma sarebbe posto a precipua tutela di quell'impronta della personalità dell'usuario del dispositivo che il trattamento congiunto dei dati generati tramite il medesimo permetterebbe di ricostruire, indipendentemente dal carattere riservato o meno, sensibile o meno di quegli stessi dati singolarmente considerati[563]. «*Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital*»[564].

[563] In dottrina, in questi termini, vedi CONDE-PUMPIDO TOURÓN, *La reforma procesal*, cit., 6, che evidenzia come sia necessario un trattamento giuridico unitario delle intrusioni realizzabili nell'ambito delle prerogative di riservatezza informatica dei singoli in quanto, in ragione del carattere multifunzionale dei dati informatici, non è possibile predeterminare la violazione di una specifica guarentigia costituzionale prima dell'effettuazione dell'accesso ai dati medesimi. Con specifico riferimento all'istituto del *registro remoto*, vedi RODRÍGUEZ LAINZ, *Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción,* in *Diario La Ley*, n. 8896, 2017, 9, che evidenzia come tale metodica di indagine impatti, contemporaneamente, sul diritto alla segretezza delle comunicazioni, alla protezione dei dati, alla *privacy* e alla intimità in generale.

[564] Non c'è dubbio, peraltro, che la pronuncia in commento sia debitrice di quanto lucidamente ricostruito in una ulteriore sentenza di due anni prima, nella quale, però, il Tribunale Supremo non era ancora giunto ad affermare espressamente l'esistenza di un diritto alla protezione dell'"*entorno virtual*". Il riferimento è a STS, 7 novembre 2011, n. 173, nella quale, significativamente, si legge che: «*Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) —por lo que sus funciones podrían equipararse a los de una agenda electrónica—, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano […]. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona*». L'aspetto che, senz'altro, suscita maggior interesse è il riconoscimento espresso dell'irrilevanza della natura privata o riservata dei dati rispetto all'esigenza della loro tutela, atteso che una lettura congiunta dei medesimi è comunque suscettibile di consentire agli inquirenti di tracciare il profilo della personalità dell'usuario del dispositivo. Da questo punto di vista,

Da questo punto di vista, sembra che lo stesso impianto normativo messo a punto con la riforma del 2015 abbia recepito un simile assetto[565]. Ciò è testimoniato, in primo luogo, dall'inserimento di tutte le misure di investigazione tecnologica nel perimetro degli strumenti impattanti sulle prerogative di cui all'art. 18 CE, senza distinzione in ordine alle singole componenti di quella disposizione costituzionale; in secondo luogo, dalla definizione di garanzie minime comuni a tutte le misure.

Tanto non significa, però, che dalla stessa regolamentazione relativa all'accesso remoto al dispositivo informatico non possa evincersi la percezione netta della sua maggiore invasività rispetto alle altre misure, come testimoniato, d'altronde, dal maggior rigore della relativa disciplina.

3.2. Presupposti applicativi.

La particolare gravità dell'ingerenza prodotta per il tramite di un'intrusione occulta e continuativa nel dispositivo elettronico dell'investigato si rispecchia, nella disciplina elaborata dal legislatore spagnolo, nella restrizione del suo ambito applicativo a una serie di reati particolarmente gravi, elencati al comma 1 dell'art. 588 *septies* a Lecrim. In particolare, si tratta dei reati commessi nell'ambito di organizzazioni criminali; dei reati di terrorismo; di quelli commessi contro minori o persone incapaci; dei reati contro la costituzione e contro la difesa nazionale. Chiude l'elenco delle fattispecie abilitanti il riferimento ai delitti commessi attraverso strumenti informatici o tecnologici che, come si vedrà, rappresenta la categoria maggiormente problematica in termini di proporzionalità.

Al netto di tale ultima categoria, trattasi di un novero di fattispecie suscettibili di generare un elevato allarme sociale e in ciò si giustifica la scelta di rendere disponibile agli investigatori un mezzo di indagine tanto invasivo. Un raffronto con il campo applicativo delineato dalla riforma del 2015 rispetto alle altre misure di investigazione tecnologica manifesta che, nell'ottica del legislatore spagnolo, trattasi della più invasiva

---

sembra compiere un passo indietro STS, 19 aprile 2017, n. 287, che sostiene che il cosiddetto "*entorno virtual*" è suscettibile di ampliarsi o ridursi in ragione delle scelte del proprio titolare. Sicché, ad esempio, la circostanza che egli condivida con altri le chiavi di accesso al proprio dispositivo assottiglierebbe il confine tra quanto deve reputarsi intimo e riservato e quanto non lo è. Una simile lettura, per tutto quanto emerso finora, non è condivisibile.

[565] In termini, ZARAGOZA TEJADA, *El registro de dispositivos de almacenamiento masivo de la informacion,* in AA.VV., *Investigation tecnologica y derechos fundamentales. Comentario a las modificaciones introducidas por la Ley 13/2015*, Aranzadi, 2017, 408 ss.

delle misure introdotte con la riforma. Tanto è vero che le stesse intercettazioni telefoniche – che rappresentano, idealmente, la seconda misura più invasiva in termini di gravità dell'ingerenza prodotta – possono essere autorizzate in relazione a un novero di fattispecie ben più ampio che comprende, oltre ai delitti di terrorismo e criminalità organizzata, anche tutti quelli puniti con pena detentiva superiore nel massimo a tre anni (art. 588 *ter* a Lecrim).

Proprio per tale ragione, alcuni autori hanno criticato la scelta legislativa di inserire nel catalogo delle fattispecie abilitanti tutti i reati commessi per il tramite delle tecnologie informatiche, atteso che trattasi di un ventaglio di fattispecie contenente anche delitti non particolarmente gravi[566]. In giurisprudenza[567], si è osservato come tale inclusione tra i reati presupposto della misura si giustifica per il fatto che, in relazione a tali fattispecie, la proporzionalità sarebbe integrata non tanto in virtù della gravità dei reati quanto, piuttosto, della peculiare natura degli stessi e delle difficoltà del loro accertamento senza il ricorso agli strumenti di indagine tecnologicamente più avanzati[568].

Ad ogni modo, sembra corretta la ricostruzione di quanti ritengono che, pur a fronte di una fattispecie come quelle in considerazione, il giudice non possa esimersi dallo svolgere un vaglio di proporzionalità in concreto della misura, secondo quanto richiesto dai principi rettori comuni a tutte le misure investigative tecnologiche, che ponga a raffronto, tra le altre cose, la gravità dell'ingerenza che si pretende di perpetrare e quella del reato oggetto di investigazione[569]. Come si è visto precedentemente, d'altronde, la verifica dell'inserimento del reato per cui si procede tra quelli per i quali può disporsi una misura investigativa tecnologica non esaurisce il compito del giudice, che deve altresì vagliare la corrispondenza della misura al principio di proporzionalità in senso stretto sul piano concreto. In conseguenza di ciò, ad esempio, il ricorso a un *registro remoto* che, per durata e ambito applicativo, appaia particolarmente invasivo non

---

[566] ZARAGOZA TEJADA, *El registro remoto de equipos informaticos*, in AA.VV., *Investigation tecnologica y derechos fundamentales. Comentario a las modificaciones introducidas por la Ley 13/2015*, Aranzadi, 2017, 460; BUENO DE MATA, *Comentarios y reflecciones sobre la Ley Orgánica 13/2015*, cit., 5; CONDE-PUMPIDO TOURÓN, *La reforma procesal*, cit., 17.

[567] STS, 9 dicembre 2015, n. 811.

[568] In dottrina, per la medesima osservazione, BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 23, che evidenzia come la proporzionalità della misura in relazione a tali fattispecie sia da ravvisarsi nell'elevato interesse statale ad evitare l'impunità di fatti di reato che, senza il ricorso a tale strumento di indagine, potrebbero essere impossibili da accertare.

[569] CONDE-PUMPIDO TOURÓN, *La reforma procesal*, cit., 17; DELGADO MARTÍN, *Investigación del entorno virtual*, cit., 12.

parrebbe giustificato a fronte di un reato non particolarmente grave, per quanto sia commesso per il tramite di tecnologie informatiche e per quanto il suo accertamento sia complicato senza il ricorso alla misura. Tanto discende, com'è ovvio, dall'applicabilità di tutte le regole dettate nel contesto della disciplina comune alle misure investigative tecnologiche anche al *registro remoto*.

Tra queste, particolare rilievo assume, nel caso di specie, la regola secondo la quale la misura può essere disposta solo nel caso in cui altre misure meno invasive non siano efficacemente praticabili. Come correttamente rilevato dalla dottrina, con specifico riguardo alla misura in commento, ciò implica che il ricorso alla stessa debba reputarsi limitato ai casi in cui non sia possibile la localizzazione fisica del dispositivo informatico infettato[570].

Una questione particolarmente rilevante relativa all'ambito applicativo della misura è quella che riguarda la possibile affettazione dei terzi. Come si è visto parlando delle norme comuni alle misure tecnologiche di indagine, l'art. 588 *bis* h Lecrim prevede che esse possano disporsi anche a carico di soggetti terzi rispetto all'indagine "nei casi e alle condizioni regolati nelle disposizioni specifiche di ciascuna misura". In relazione al *registro remoto*, la Lecrim non contiene alcuna previsione specifica. Sorge, dunque, l'interrogativo se con la misura in questione possa acquisirsi il controllo di un soggetto diverso da quello sottoposto all'indagine.

Senza dubbio, la lettura congiunta dell'art. 588 *septies* a Lecrim (che stabilisce che il *registro remoto* del dispositivo informatico è disposto «*sin conocimiento de su titular o usuario*») e dell'art. 588 *bis* h Lecrim non osta a che l'atto sia disposto relativamente a un dispositivo che, pur non essendo nella titolarità o disponibilità esclusiva dell'investigato, sia da quest'ultimo utilizzato, anche se non in via esclusiva. Naturalmente, in un simile caso la motivazione dell'atto dovrebbe dar conto delle ragioni e degli elementi fattuali in base ai quali si ritiene che il dispositivo sia adoperato anche dal soggetto investigato e che nel medesimo possano, pertanto, scovarsi informazioni necessarie per l'accertamento dei fatti.

Laddove, invece, il dispositivo fosse utilizzato in via esclusiva dal terzo – ancorché si reputi che possano nel medesimo rinvenirsi elementi utili all'indagine –, pare mancare una norma di copertura che, conformemente a quanto stabilito dalla disposizione

[570] Ancora, BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 23.

comune, individui le condizioni e le modalità per l'intrusione nelle prerogative del terzo. Una soluzione che escluda una la possibilità di ricorrere alla misura nel caso di specie, d'altronde, non sembra irragionevole in virtù della elevata intrusività della medesima[571]. In altre parole, non appare tanto singolare che il legislatore abbia reputato non proporzionato il ricorso alla misura a carico di un soggetto non sospettato della commissione di alcun reato, alla luce della evidente intrusività della stessa.

Tale soluzione sembra, nondimeno, avversata da una parte della dottrina che reputa applicabile in via analogica la disposizione prevista in materia di intercettazione di comunicazioni[572]. Il riferimento è, in particolare, all'art. 588 *ter* c Lecrim, che prevede che possa intercettarsi l'utenza di una persona terza rispetto all'indagine in tre casi: laddove risulti che l'investigato si serva del terzo per trasmettere o ricevere informazioni; laddove il titolare del dispositivo collabori con il soggetto investigato per il raggiungimento dei suoi scopi illeciti o, comunque, tragga beneficio dalla sua attività; infine, nel caso in cui il dispositivo oggetto di investigazione sia utilizzato maliziosamente da terzi per via informatica o telematica, senza conoscenza del suo titolare. La norma, come si vede, consente l'intercettazione del terzo in ragione di un suo qualche coinvolgimento nei fatti o, comunque, laddove possa riscontrarsi un uso, anche occulto, del dispositivo da parte dell'investigato. Tuttavia, in virtù della disposizione, è possibile che l'utenza del terzo sia sottoposta a controllo benché egli non sia minimamente coinvolto nell'attività dell'indagato e indipendentemente dal fatto che il dispositivo sia da quest'ultimo utilizzato, anche solo occasionalmente. L'applicazione della disposizione, dunque, amplierebbe la possibilità del ricorso al controllo del dispositivo di titolarità di un terzo ben al di là di quanto sembrerebbe consentito in ragione della formulazione del primo comma dell'art. 588 *septies* a Lecrim. In buona sostanza, si tratterebbe di un'analogia *in malam partem* in un campo nel quale è, invece, opportuno mantenersi sui binari di un quanto mai serrato rigore interpretativo. Peraltro, come visto prima, lo stesso dato letterale sembra deporre nel senso della non ammissibilità della misura in relazione a dispositivi utilizzati esclusivamente da terzi.

---

[571] RODRÍGUEZ LAINZ, *Intervención judicial de comunicaciones*, cit., 13.

[572] BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 12; SÁNCHEZ RUBIO, *Los registros remotos sobre equipos informáticos*, cit., 208. Tale conclusione viene giustificata in ragione dell'osservazione per la quale il *registro remoto*, al pari dell'intercettazione, comporta pur sempre la captazione di un processo di comunicazione quale via obbligata per accedere al contenuto del dispositivo.

3.3. Il procedimento applicativo della misura.

L'art. 588 *septies* a Lecrim individua due possibili modalità esecutive del *registro remoto*. L'accesso al sistema informatico può avvenire o tramite l'uso di dati identificativi e codici di sicurezza che proteggono il sistema stesso o tramite l'inoculazione di un *software*. Naturalmente, la prima modalità presuppone che gli investigatori siano a conoscenza delle *password* del sistema in uso al soggetto sottoposto all'indagine. Essa, inoltre, consente l'ingresso limitatamente a quei sistemi informatici (*cloud,* servizio di posta elettronica e così via) consistenti in *software* e programmi determinati, accessibili da qualsivoglia terminale fisico. Tramite il ricorso a tale modalità, insomma, non sembra possibile acquisire il controllo dell'intero contenuto dello *smartphone* in uso al soggetto indagato.

La seconda delle modalità operative indicate dalla disposizione consiste, sostanzialmente, nell'inserimento da remoto, nel dispositivo informatico, di un *trojan virus* che consente agli investigatori di acquisire il suo totale controllo dalla postazione remota e di effettuare una vera e propria sorveglianza continuativa di tutte le attività realizzate per il tramite dello stesso.

I sistemi informatici che possono essere bersaglio dell'atto di indagine in argomento sono indicati dal comma 1 dell'art. 588 *septies* a Lecrim. La norma fa riferimento a «*un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos*». Trattasi, come si vede, di un novero molto ampio di strumenti informatici, nel quale sono suscettibili di rientrare, stante il riferimento a qualsivoglia strumento di memorizzazione di massa di dati, tutti i dispositivi informatici di uso comune anche diversi dal *personal computer*, come *smartphone, tablet* e così via.

Conformemente alla riserva di giurisdizione di generale applicazione nella materia che occupa, il provvedimento applicativo della misura è emesso da giudice che, al suo interno, deve fornire una serie di indicazioni particolari che, ovviamente, si aggiungono a quelle previste dalle norme comuni e, in particolare, dall'art. 588 *bis* c Lecrim, precedentemente analizzato.

Così, la risoluzione giudiziale che autorizza il *registro remoto* deve contenere precisa indicazione del sistema informatico bersaglio dell'attività (lett. a), art. 588 *septies* s Lecrim); l'ambito applicativo della misura, la modalità operativa attraverso la quale si

procederà all'accesso al sistema informatico e all'apprensione dei dati in esso contenuti rilevanti per la causa, nonché il *software* adoperato per l'esecuzione delle operazioni (lett. b) del medesimo articolo); gli agenti incaricati di eseguire la misura, l'eventuale autorizzazione per procedere alla copia e alla conservazione dei dati e le misure necessarie per la preservazione della loro integrità, per la loro inaccessibilità o per la loro soppressione (rispettivamente, lett. c), d) ed e) dell'art. 588 *septies* a Lecrim). Tale ultima disposizione, in particolare, sembra facoltizzare il giudice a interdire, anche momentaneamente, l'accesso ai dati rinvenuti o a disporne la soppressione. Ciò, ad esempio, potrebbe essere opportuno nel caso in cui si proceda in relazione a reati particolarmente gravi, come la pedopornografia, che suggeriscono un intervento immediato al fine di impedire l'ulteriore circolazione del materiale illecito contenuto nel sistema[573].

A differenza di quanto il precedente art. 588 *sexies* c Lecrim[574] sancisce in relazione alla perquisizione e sequestro informatici che non si svolgano da remoto ma in presenza, l'art. 588 *septies* a non prevede la possibilità che il *registro remoto* sia disposto in via d'urgenza dalla polizia giudiziaria. Tanto ha, a parere di chi scrive correttamente, indotto buona parte della dottrina[575] a concludere nel senso che la procedura in via d'urgenza sia da escludersi *tout court* nel caso di specie. Tanto si giustificherebbe, secondo alcuni, in ragione della peculiare intrusività della misura in argomento[576]; secondo altri, per la stessa impraticabilità tecnica di un accesso urgente, trattandosi di una misura che, per poter essere eseguita, necessità di una complessa preparazione sul piano tecnico[577].

Quanto alla durata massima della misura, anche nella prescrizione relativa a tale aspetto si evince come il legislatore spagnolo abbia colto la più elevata intrusività della misura in questione rispetto a tutte le altre attività di investigazione tecnologica: si prevede il termine di un mese, prorogabile fino a un massimo di tre mesi (art. 588 *septies* c

---

[573] RICHARD GONZÁLEZ, *Investigación y prueba*, cit., 199.

[574] La disposizione, al comma 4, prevede che nei casi di urgenza in cui si apprezzi la presenza di un interesse costituzionalmente legittimo che renda imprescindibile la misura, la polizia giudiziaria può procedere all'esame del sistema informatico senza autorizzazione del giudice, comunicando allo stesso l'esecuzione della misura e le ragioni che l'hanno giustificata nel termine di 24 ore. Il giudice deve convalidare la misura nelle 72 ore successive alla sua esecuzione.

[575] Critico, invece, nei confronti di questa soluzione, MONTES ÁLVARO, *Regulación de las medidas de investigación tecnológica*, cit., 116.

[576] DELGADO MARTÍN, *Investigación del entorno virtual*, cit., 12.

[577] CABEZUDO RODRÍGUEZ, *Ciberdelincuencia e investigación criminal*, cit., 47.

Lecrim). Trattasi di una durata ben inferiore a quella prevista per le stesse intercettazioni, che possono estendersi, considerando le proroghe, fino a un massimo di diciotto mesi. Non è mancato chi ha criticato l'opzione a favore di un termine tanto breve, sul presupposto che sarebbe irragionevole una distinzione tanto marcata con il regime previsto in materia di intercettazioni[578], ma l'osservazione appare fuori fuoco se solo si tiene conto del carattere plurioffensivo della misura, idonea a incidere contemporaneamente, oltre che sul diritto alla segretezza delle comunicazioni, anche su altri diritti fondamentali[579].

Per quanto concerne la utilizzazione probatoria dei risultati ottenuti tramite l'attività di sorveglianza, la legge non prevede, in relazione al *registro remoto*, una disciplina specifica in materia di accesso delle parti ai relativi atti e di selezione delle conversazioni rilevanti per la causa, come quella prevista dall'art. 588 *ter* i Lecrim per le intercettazioni di comunicazioni. Secondo la dottrina, in mancanza di una normativa *ad hoc* dovrebbe ricorrersi allo strumento della perizia, tramite il quale dovrebbe procedersi, anzitutto, ad accreditare che i risultati di prova ottenuti siano il risultato dell'investigazione condotto e che questa sia stata realizzata nel rispetto dei limiti imposti dalla legge e dal provvedimento autorizzativo[580].

Prima di concludere sul punto, vale la pena di richiamare quanto si è già visto precedentemente in merito alla strategia normativa adottata dal legislatore spagnolo al fine di assicurare la pertinenza della misura rispetto all'indagine in corso. Come si è detto parlando delle regole comuni alle misure di investigazione tecnologica, il giudice che autorizza l'atto deve indicare l'"*alcance*" dello stesso, ossia effettuare una previa delimitazione dei dati e delle parti del sistema informatico che possono essere riguardate dalla ricerca. La regola, ovviamente, assume particolare importanza con riferimento al mezzo di indagine in argomento, atteso che è alle sue stesse specifiche operative e tecniche è connaturato il rischio di un suo uso a fini meramente esplorativi. Tanto è vero che, nonostante ciò sia già ricavabile dalla previsione generale, il legislatore ribadisce, nella norma dedicata al *registro remoto*, l'esigenza dell'indicazione dell'ambito della

[578] Bachmaier Winter, *Registro remoto de equipos informáticos*, cit, 17; MARCHENA GOMEZ, *La reforma de las diligencias de investigacion limitativas de los derechos reconocidos en el art. 18 de la ce. Proceso penal y nuevas tecnologias*, in Marchena Gómez e González Cuéllar Serrano, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Ediciones Jurídicas Castillo de Luna, 2015, 390; MONTES ÁLVARO, *Regulación de las medidas de investigación tecnológica*, cit., 116.

[579] ZARAGOZA TEJADA, *El registro remoto*, cit., 455.

[580] RICHARD GONZÁLEZ, *Investigación y prueba*, cit., 329 ss.

misura specificando che con la stessa possono acquisirsi solo i dati rilevanti per la causa in relazione alla quale viene eseguita (art. 588 *septies* a, lett. b), Lecrim).

Non possono che ribadirsi, in questa sede, i dubbi già espressi a suo tempo circa la possibilità che l'operatività di tale regola possa offrire risultati apprezzabili in termini di concreta riduzione dell'impatto della misura sugli ambiti di riservatezza del singolo. Tanto più quando, come nel caso di specie, si tratta di una misura destinata all'acquisizione di dati futuri di varia natura, rispetto ai quali una valutazione di effettiva pertinenza all'indagine può compiersi solo successivamente alla loro formazione. Trattasi di una circostanza che determina un elevato rischio di scollamento dai principi di necessaria pertinenza e proporzionalità, difficilmente riducibile per il tramite della mera imposizione al giudice dell'obbligo di circoscrivere la misura con esclusivo riferimento agli ambiti materiali di operatività della stessa.

3.4. I dubbi interpretativi.

All'indomani dell'entrata in vigore della disciplina sull'accesso remoto a un sistema informatico la dottrina spagnola ha segnalato molteplici difficoltà interpretative con riferimento all'effettivo ambito di operatività della disposizione e, in particolare, alle attività legittimamente realizzabili per il suo tramite. Viste le ampie potenzialità esplorative dello strumento e la forte incidenza dello stesso su prerogative fondamentali di elevato rango costituzionale, la dottrina[581] ha immediatamente rilevato l'urgenza di risolvere simili interrogativi.

L'art. 588 *septies* a Lecrim, infatti, si limita a stabilire che tramite tale misura è possibile accedere al "contenuto" del sistema informatico, da remoto e senza la conoscenza del suo utilizzatore, ma non precisa quali attività possono concretamente realizzarsi, né stabilisce se la visione e apprensione del contenuto del sistema siano limitate ai dati già esistenti nello stesso al momento dell'accesso o se sia altresì possibile acquisire dati non ancora formati. Insomma, la laconicità della disposizione è tale che, addirittura, non è chiaro se lo strumento investigativo in questione possa essere utilizzato per compiere la stessa attività per la quale pare essere stato concepito, cioè l'effettuazione di una sorveglianza continuativa esplicabile tramite il controllo di tutti gli applicativi dello strumento informatico bersaglio.

[581] SÁNCHEZ RUBIO, *El principio de proporcionalidad*, cit., 214.

La dottrina si è orientata verso soluzioni non coincidenti. Così, secondo alcuni commentatori, il ricorso allo strumento in questione consentirebbe un accesso indefinito a tutti i dati, preesistenti e futuri, rinvenibili nel sistema informatico[582], con la conseguenza che potrebbe condurre a una vera e propria profilazione del soggetto alla stessa sottoposto tramite l'accesso in tempo reale a qualsivoglia attività realizzata con il dispositivo e il monitoraggio di tutti i suoi terminali[583]. Altri, invece, evidenziano come, benché lo strumento renda tecnicamente possibile l'accesso al microfono, alla *webcam* e ad ogni altra funzionalità propria del sistema, il riferimento normativo al "contenuto del dispositivo" escluderebbe che tali funzionalità possano effettivamente attivarsi con la conseguente registrazione anche di tutto ciò che non è nel dispositivo, ma intorno allo stesso[584].

Ad ogni modo, la circostanza che sia prevista una durata estesa della misura (un mese, prorogabile fino a tre mesi) sembra deporre per la conclusione che sia ammesso anche il monitoraggio dei dati sopravvenuti all'accesso al dispositivo e non solo ai dati già memorizzati nello stesso in quel momento[585].

La questione si complica ulteriormente con riferimento alla possibilità di adoperare la misura anche al fine di effettuare un'attività di intercettazione delle comunicazioni. Mentre, infatti, alcuni hanno evidenziato come essa consenta agli investigatori di venire a conoscenza anche delle conversazioni mantenute dall'investigato nel periodo di tempo in cui è sottoposto al controllo[586], altri hanno avanzato dubbi in merito alla correttezza di una simile conclusione[587].

In realtà, la risposta non sembra essere univoca, dipendendo, piuttosto, dalla tipologia di intercettazione che si intenda realizzare e dalla disciplina che si intenda applicare. La questione, insomma, non può essere analizzata da un unico punto di vista ma va ripartita in tre sotto questioni: se possa ricorrersi all'accesso remoto al dispositivo informatico al fine di realizzare un'intercettazione di comunicazioni applicando la normativa prevista in materia di intercettazioni all'art. 588 *ter* a ss. Lecrim; se possa legittimamente

[582] ZARAGOZA TEJADA, *El registro remoto*, cit., 454.
[583] Così, MONTES ÁLVARO, *Regulación de las medidas de investigación tecnológica*, cit., 115; in termini, BALLESTEROS, *Medidas de investigación tecnológica*, cit., 201. Cfr. anche Delgado Martín, *Investigación del entorno virtual*, cit., 11, che evidenzia come sarebbe esperibile anche la funzione di *keylogging*.
[584] RICHARD GONZÁLEZ, *Investigación y prueba*, cit., 217.
[585] Lo evidenzia anche CONDE-PUMPIDO TOURÓN, *La reforma procesal*, cit., 13.
[586] MONTES ÁLVARO, *Regulación de las medidas de investigación tecnológica*, cit., 115.
[587] BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 15; RODRÍGUEZ LAINZ, *Intervención judicial de comunicaciones*, cit., 11.

effettuarsi una intercettazione di comunicazioni tramite accesso remoto applicando la normativa prevista in relazione a quest'ultimo istituto; se possa legittimamente effettuarsi un'intercettazione ambientale ricorrendo alla normativa prevista in materia di accesso remoto.

La soluzione di simili dubbi interpretativi ha importanti risvolti pratici. Trattasi, infatti, di istituti che presentano presupposti applicativi differenti, sicché la preferenza accordata all'una o all'altra conclusione finisce per influenzare le sorti processuali del materiale investigativo raccolto con l'una o con l'altra modalità.

Con riferimento alla prima questione, sembra che la risposta possa essere positiva. In effetti, la disciplina in materia di intercettazioni non contiene previsioni in merito allo strumento tecnico da utilizzare, sicché non pare integrare alcuna violazione della relativa disciplina l'uso del captatore al fine di intercettare le conversazioni telefoniche e telematiche della persona sottoposta alla misura. Ciò implica il rispetto di tutti i presupposti applicativi di quell'istituto, a partire dalla necessaria individuazione di una tra le ipotesi di reato per le quali l'intercettazione di comunicazioni può legittimamente disporsi. In conseguenza, ad esempio, deve ritenersi che il captatore informatico possa essere utilizzato al fine di intercettare comunicazioni relative a qualunque reato punito con la pena della reclusione superiore, nel massimo, a tre anni, ma non anche con riguardo ai reati commessi per il mezzo di strumenti informatici che siano puniti con pena inferiore (per i quali sarebbe, invece, esperibile un *registro remoto*). Semmai, un problema potrebbe sorgere con riferimento alle misure da adottare per limitare effettivamente l'uso del dispositivo alla captazione di conversazioni telefoniche e telematiche, con l'esclusione del suo utilizzo al fine di realizzare le ulteriori attività possibili per mezzo dello stesso. A ciò potrebbe ovviare lo stesso provvedimento autorizzativo della misura. Come si è visto parlando delle disposizioni generali, nella richiesta di applicazione della misura di investigazione tecnologica il pubblico ministero è tenuto a indicare le modalità esecutive della stessa (art. 588 *bis* b, n. 6, Lecrim). Nonostante l'art. 588 *bis* c Lecrim, che disciplina il contenuto dell'atto autorizzativo, non preveda nulla a riguardo, un'interpretazione sistematica della disposizione depone nel senso che il giudice sia altresì onerato di fornire tali indicazioni al momento dell'emissione del relativo provvedimento. La norma in questione andrebbe letta in combinato disposto con l'art. 588 *ter* d Lecrim che, in materia di contenuto della

richiesta autorizzativa avanzata in materia di intercettazioni, prevede che debbano indicarsi «*la forma tipo de comunicaciones a las que afecta*». Spetterebbe, dunque, allo stesso giudice individuare le specifiche comunicazioni intercettabili e le modalità tecniche attraverso le quali procedere all'esecuzione dell'atto di indagine limitando l'uso del *virus* alla captazione dei soli contenuti comunicativi.

Ben più complessa sembra la questione sottesa al secondo quesito: alla soluzione positiva, infatti, sembrano opporsi una serie di considerazioni. Anzitutto, con l'introduzione di due distinti istituti per l'accesso remoto e la captazione di comunicazioni, il legislatore spagnolo sembra aver inteso differenziare due diverse tipologie di indagine, rispondenti a presupposti distinti e aventi finalità non coincidenti quanto alla natura dei dati da acquisire. Effettivamente, se si consentisse la realizzazione di un'attività di intercettazione tramite la normativa prevista in materia di *registro remoto*, tale ultimo istituto rischierebbe di sconfinare nell'ambito applicativo del primo e viceversa, data la differenza di reati presupposto.

Come, però, giustamente rilevato dalla dottrina spagnola[588], la distinzione rischia di sfumare e di perdere qualsiasi rilevanza pratica con riferimento alle conversazioni memorizzate sul dispositivo informatico svolte tramite programmi di messaggistica, di posta elettronica, di *social networks* e così via: effettivamente, il mantenimento del *virus* all'interno di un dispositivo informatico per un periodo più o meno esteso determina la possibilità di acquisire e scaricare man mano le conversazioni tenute dal soggetto. Una simile attività, secondo la distinzione invalsa nella giurisprudenza spagnola maggioritaria costituzionale e di legittimità in materia di intercettazioni[589], non inciderebbe sul diritto al segreto delle comunicazioni e non imporrebbe, di conseguenza, l'applicazione della normativa in materia di intercettazioni telefoniche[590]. In tal caso, dunque, sembrerebbe legittimo sfruttare la normativa prevista in materia di *registro remoto*, con la conseguente possibilità, nel corso dell'esecuzione del medesimo, di affiancare il *download* delle conversazioni memorizzate sul dispositivo a tutte le altre

[588] BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 15.
[589] Cfr. par. 1.1.
[590] Per tale ragione, non sembra corretta la soluzione di quanti ritengono che l'accesso tramite captatore informatico alle conversazioni memorizzate sul dispositivo e non in corso di realizzazione dovrebbe avvenire con l'applicazione della normativa in materia di intercettazioni, RODRÍGUEZ LAINZ, *Intervención judicial de comunicaciones*, cit., 17 ss.

attività di controllo, anche in tempo reale, esperibili tramite lo stesso, con l'esclusione della possibilità di intercettare conversazioni contestualmente al loro svolgimento[591].

Trattasi di una soluzione che, pur essendo imposta alla stregua delle categorie processuali esistenti e da un risalente tradizione pretoria, lascia scoperti i nervi delle garanzie, atteso che non si coglierebbe, neppure sul piano fenomenologico, la differenza tra un'acquisizione contestuale e una non contestuale quando quest'ultima, come nel caso di specie, potrebbe realizzarsi a intervalli ravvicinati per lunghi periodi di tempo, con la conseguenza che, come spesso accade quando il diritto interagisce con le nuove tecnologie, la eccessiva rigidità delle categorie giuridiche tradizionali conduce a soluzioni formalistiche e scarsamente efficaci dal punto di vista della tutela dei diritti dei singoli.

Da ultimo, occorre chiedersi se tramite l'utilizzo di un *troyan virus* possa legittimamente realizzarsi un'intercettazione ambientale, con eventuale contestuale captazione di immagini[592]. La questione è sovrapponibile a quella, appena analizzata, relativa alle intercettazioni telefoniche e telematiche, con cui le intercettazioni ambientali condividono alcune differenze rispetto al *registro remoto* quanto al novero dei reati presupposto[593] e alla durata delle operazioni. Con riferimento a quest'ultimo aspetto, in particolare, la normativa spagnola prevede un regime peculiare, stabilendo che la misura debba essere vincolata alla captazione di comunicazioni che possono aver luogo durante uno o vari incontri concreti dell'investigato con altre persone il cui svolgimento risulti prevedibile sulla base degli elementi acquisiti nel corso dell'investigazione. Anche in questo caso, dunque, possono ribadirsi le considerazioni svolte in materia di intercettazioni telefoniche: il legislatore sembra aver delineato due distinte figure investigative che non dovrebbero interferire tra loro. L'elemento che, tuttavia, sembra più dirimente nel senso della maggiore plausibilità della soluzione negativa è quello per il quale, come si è visto, l'articolo relativo al *registro remoto* facoltizza l'accesso al "contenuto" del dispositivo, così escludendo, ragionevolmente, la possibilità di acquisire dati relativamente a quanto si svolge non tramite, ma intorno al medesimo. Tale considerazione sembra escludere altresì – a differenza di quanto visto

[591] BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 15.

[592] Tanto è permesso dalla disciplina in materia di intercettazioni ambientali, contenuta agli artt. 588 quater a ss. Lecrim.

[593] Si tratta sempre delle fattispecie in materia di terrorismo e di criminalità organizzata e dei reati puniti con pena superiore nel massimo a tre anni.

in materia di intercettazioni – che l'intrusione di cui si discute possa realizzarsi applicando la normativa – e dunque i presupposti – dettati in materia di intercettazione ambientale e limitandosi ad utilizzare il *virus* alla stregua di un mero strumento di realizzazione della misura.

Lo scarso ricorso, da parte delle procure, alla misura in questione pare ostacolare la soluzione dei dubbi interpretativi appena evidenziati, che potrebbe essere favorita da una prassi giurisprudenziale che, per tale ragione, sembra faticare a consolidarsi.

Al contempo, quanto appena visto pare rafforzare le conclusioni raggiunte nei precedenti capitoli in merito alla necessità di differenziare, sul piano legislativo, l'accesso dinamico e statico al dispositivo informatico, con la conseguente distinzione tra l'acquisizione ai dati preesistenti all'intrusione e la realizzazione di una vera e propria attività di sorveglianza perdurante, che dovrebbe essere limitata a casi del tutto eccezionali data l'elevatissima incidenza sulle prerogative fondamentali dei singoli.

4. L'agente informatico sotto copertura.

Con la riforma attuata tramite la Ley 13/2015, il legislatore spagnolo ha altresì posto rimedio a un ulteriore vuoto normativo, riguardante la ammissibilità del ricorso alla figura dell'agente sotto copertura in ambito informatico. L'art. 282 *bis* Lecrim, infatti, già disciplinava lo svolgimento dell'indagine sotto copertura, ma solo con riferimento alla sua possibile implementazione nel corso di un'indagine svolta nel mondo fisico, non prevedendo alcuna regola peculiare per il caso di *undercover* operante nella rete. A seguito della modifica, l'articolo in questione contiene, oggi, un sesto comma che autorizza espressamente il ricorso a tale peculiare figura. Per quanto essa sia estranea al *corpus* normativo dedicato alle indagini tecnologiche, evidenti ragioni di affinità con la materia trattata consigliano l'illustrazione, in questa sede, degli aspetti principali della relativa disciplina, che, pur avendo indiscutibili peculiarità, afferisce pur sempre alla realizzazione di attività investigative occulte e da remoto[594].

Prima della novella normativa, l'ammissibilità del ricorso a tale tecnica di indagine per l'investigazione di reati commessi per il tramite delle tecnologie informatiche era assai discussa. Per un verso, l'utilità e, anzi, la necessità di ricorrere a tale strumento era sempre più avvertita, soprattutto al fine di combattere efficacemente il crescente

[594] In termini, anche RICHARD GONZÁLEZ, *Investigación y prueba*, cit., 201.

fenomeno della pedopornografia nelle reti internet protette da forme di anonimato e da misure di protezione che rendevano estremamente complessa la loro penetrazione senza un previo invito da parte dei gestori delle stesse[595]. Per altro verso, l'assetto normativo preesistente non sembrava del tutto adeguato a fornire copertura legale a simili attività di indagine. L'art. 282 *bis* Lecrim, infatti, prevedeva – e continua a prevedere – quali necessari presupposti dell'applicazione dell'istituto con riferimento all'attività sotto copertura classica che si proceda in relazione a determinate fattispecie di reato[596] commesse nell'ambito del crimine organizzato. In buona sostanza, proprio la fattispecie suscettibile di creare maggiore allarme sociale, rispetto alla quale il ricorso all'agente sotto copertura pareva poter offrire maggiori benefici, rischiava di restare esclusa dal novero dei reati per il quali il congegno investigativo di cui all'art. 282 *bis* Lecrim era azionabile. Tanto in ragione del fatto che anche laddove si fosse proceduto in relazione a una delle fattispecie espressamente indicate dalla disposizione (tra le quali le più affini sarebbero state quelle relative alla prostituzione) molte delle condotte illecite rientranti nell'ambito della criminalità informatica erano – e sono – poste in essere da soggetti che, pur operando all'interno di determinate reti, agiscono in maniera isolata, senza alcun previo accordo e senza alcuna struttura organizzata[597].

In conseguenza di ciò, la normativa introdotta nel 2015 in relazione all'agente informatico sotto copertura si differenzia, quanto a presupposti, rispetto a quella classica: anzitutto, non si richiede che si proceda in relazione a reati commessi nell'ambito della criminalità organizzata; in secondo luogo, è molto più ampio il novero dei reati in relazione ai quali il ricorso alla tipologia investigativa in argomento può disporsi. Si tratta, infatti, di tutte le fattispecie già previste dell'art. 282 *bis* con

---

[595] LAFONT NICUESA, *El agente policial encubierto*, Tirant lo Blanch, 2022, 421.

[596] Trattasi dei reati di traffico di organi di esseri umani, sequestro di persona, traffico di esseri umani, delitti relativi alla prostituzione, alcuni delitti contro il patrimonio e contro l'ordine socioeconomico, alcuni delitti relativi alla proprietà intellettuale e industriale, alcuni delitti contro i diritti dei lavoratori e dei cittadini stranieri, delitti di traffico di flora o fauna a rischio di estinzione, delitti di traffico di materiale nucleare e radioattivo, alcuni delitti contro la salute pubblica, delitti di deposito di armi, munizioni ed esplosivi e delitto di falsificazione della moneta, di carte di debito o credito o di assegni e di alcuni delitti contro il patrimonio storico.

[597] ZARAGOZA TEJADA, *La modificación operada por la ley 13/2015. El agente encubierto informático*, Curso de formación continua de fiscales, Centro de Estudios jurídicos, 2016, 19. Occorre segnalare, tuttavia, una decisione piuttosto recente in cui il Tribunale Supremo ha riconosciuto la legittimità dell'attività di indagine informatica svolta sotto copertura in un arco temporale antecedente all'entrada in vigore della Ley 13/2015 sul presupposto che la mancanza di una regolamentazione precisa dell'istituto non impedisse il ricorso a tale modalità di indagine laddove la stessa fosse da reputarsi, nel caso concreto, conforme al principio di proporzione (STS, 28 marzo 2019, n. 171).

riferimento all'*undercover* che svolga la sua attività nel mondo fisico, cui si aggiungono tutti gli altri delitti per i quali, ai sensi del combinato disposto degli artt. 588 *ter* a e art. 579, comma 1, Lecrim, può disporsi attività di intercettazione. Vi rientrano, quindi, anche tutti i delitti puniti con la reclusione superiore nel massimo a tre anni[598]. Ove, dunque, si proceda in relazione a tali tipologie di reato, ai sensi del nuovo comma 6 dell'art. 282 *bis* Lecrim, il giudice può autorizzare funzionari di polizia giudiziaria ad attuare sotto copertura "in comunicazioni mantenute in canali chiusi di comunicazione". Tale locuzione è da intendersi diretta a ricomprendere qualunque piattaforma di rete gestita da un soggetto o da soggetti che abbiano la possibilità di escludere terzi dal processo comunicativo[599], ivi inclusi i *social network* laddove siano adoperate funzionalità che consentano di escludere altri dal dialogo in corso[600]. In ciò, la figura in questione si distingue da quella del "*ciberpatrullator*", ovvero dell'agente di polizia che realizza investigazioni e indagini in canali aperti di comunicazione e che, pertanto, non è tenuto a richiedere la previa autorizzazione giudiziale[601].

Al ricorrere dei presupposti appena menzionati, dunque, può disporsi lo svolgimento di un'attività sotto copertura nelle reti sociali o in altre forme di connessione in internet[602].

A tale attività si applicano le restanti regole previste, in generale, dallo stesso art. 282 *bis* Lecrim con riferimento a qualsivoglia attività di indagine sotto copertura[603], con l'unica, importante, peculiarità che, nel caso di agente informatico, è strettamente necessaria l'autorizzazione da parte del giudice, non essendo sufficiente un provvedimento del pubblico ministero. Secondo la dottrina spagnola, alla base di tale regola vi sarebbe la considerazione che l'attività in questione comporta pressoché sistematicamente – a differenza di quella svolta nel mondo fisico – l'intrusione in uno spazio destinato alle comunicazioni nel quale un numero potenzialmente elevatissimo di soggetti scambia espressioni, opinioni e comunicazioni che, per quanto illecite, ricadono

---

[598] Per la tesi secondo la quale il giudice sarebbe comunque onerato di compiere un vaglio di proporzionalità dell'ingerenza nel caso di specie, ZARAGOZA TEJADA, *La modificación operada por la ley 13/2015*, cit., 22.

[599] Ancora, LAFONT NICUESA, *El agente policial encubierto*, cit., 428, che specifica che, conseguentemente, l'agente sotto copertura deve essere appartenente alla polizia giudiziaria e che l'incarico può essere assunto solo su base volontaria.

[600] STS, 29 aprile 2021, n. 357.

[601] STS, 11 aprile 2018, n. 173.

[602] VALIÑO CES, *Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015*, in *Diario La Ley*, n. 8731, 2016, 3.

[603] LAFONT NICUESA, *El agente policial encubierto*, cit., 452.

sotto l'ombrello protettivo del diritto al segreto delle comunicazioni di cui all'art. 18, comma 4, CE[604].

Quanto all'autorizzazione giudiziale, ai sensi dell'art. 282 *bis* Lecrim, essa dovrebbe contenere il riferimento al fatto di reato investigato, alla necessità della misura per le investigazioni e alla sua idoneità a conseguire la finalità perseguita. Ai sensi del comma 7 del medesimo articolo, inoltre, l'autorizzazione può prevedere la possibilità, per l'agente informatico sotto copertura, di scambiare o inviare archivi di dati con contenuti illeciti e di analizzare i risultati degli algoritmi applicati per l'identificazione, nella rete, degli anzidetti archivi illeciti. Trattasi di una norma inserita con la chiara finalità di dare copertura legale allo scambio di materiale pedopornografico, consentendo l'applicabilità della scriminante prevista dalla disposizione (art. 282 *bis*, comma 5, Lecrim) anche laddove lo scambio o l'invio di materiale non rappresenti la conseguenza necessaria dello svolgimento dell'attività sotto copertura già avviata, ma piuttosto un'attività prodromica, attraverso la quale l'*undercover* riesce ad accedere alla rete chiusa di comunicazioni[605]. Presupposto generale per l'applicazione della relativa scriminante è, ad ogni modo, che l'attività compiuta si sia mantenuta nei limiti della proporzionalità e non sia sfociata in una provocazione alla commissione del delitto[606].

In ogni caso, il comma 3 dell'art. 282 *bis* Lecrim prevede, per qualsivoglia operazione sotto copertura, che laddove le attività realizzate dall'*undercover* incidano su diritti fondamentali quest'ultimo sia tenuto a chiedere l'autorizzazione al giudice competente. Allo stesso modo, il giudice, ai sensi del comma 7, può autorizzare l'acquisizione di immagini e la registrazione di conversazioni "mantenute nel corso di incontri previsti tra l'agente sotto copertura e il soggetto investigato". A meno di ritenere che l'autorizzazione giudiziale emessa per consentire l'avvio dell'operazione informatica sotto copertura sia già suscettibile di ricomprendere tali attività, la norma deve essere

---

[604] ZARAGOZA TEJADA, *La modificación operada por la ley 13/2015*, cit., 22.

[605] ZARAGOZA TEJADA, *La modificación operada por la ley 13/*2015, cit., 25, segnala che una delle difficoltà ad accedere a tali reti è rappresentata dal fatto che spesso i soggetti che le gestiscono subordinano l'accesso di nuovi partecipanti all'invio, da parte loro, di materiale pedopornografico. Tale invio, in assenza della norma in commento, avrebbe rischiato di rimanere fuori dall'ambito di operatività della prevista dall'art. 282 bis, comma 5, Lecrim, che copre solo le attività delittuose realizzate quale conseguenza necessaria dello sviluppo dell'operazione sotto copertura.

[606] Secondo la dottrina, i parametri per l'individuazione di un'attività di provocazione al delitto sono gli stessi dell'attività sotto copertura tradizionale: pertanto, il proposito delittuoso non deve svilupparsi in conseguenza dell'intervento dell'*undercover* ma deve essere preesistente allo stesso. LAFONT NICUESA, *El agente policial encubierto*, cit., 465.

sistematicamente interpretata nel senso che l'ulteriore autorizzazione sia comunque richiesta per la acquisizione di immagini e conversari che si svolgono nella rete internet.
Conformemente a quanto previsto dal comma 1 dell'art. 282 *bis* Lecrim, l'agente sotto copertura – anche informatico – ha l'obbligo di riferire i risultati ottenuti, nel minor tempo possibile, all'organo che ha autorizzato l'operazione (trattandosi di agente informatico, come detto, il giudice). La stessa disposizione prevede altresì che tali informazioni dovranno apportarsi, nella loro integrità, anche nel processo, ove devono essere valutate dall'organo giudiziale competente.
Come rilevato in dottrina[607], la regola generale è che l'agente sotto copertura sia citato quale testimone nel corso del giudizio e sottoposto all'esame delle parti in ordine all'attività realizzata e ai suoi risultati. Tanto in ossequio al principio del contraddittorio e anche allo specifico fine di consentire una rigorosa valutazione della legittimità del suo operato[608].

5. Riflessioni conclusive sulla possibile introduzione delle tecniche investigative di *remote searching* e *remote surveillance* nell'ordinamento italiano.

L'analisi condotta nelle pagine precedenti sullo strumento di indagine, introdotto nell'ordinamento spagnolo a partire dal 2015, del *registro remoto* e sulle problematiche interpretative che ne sono scaturite rende necessario, prima di concludere la trattazione, porsi un ultimo interrogativo. Esso, prima ancora che al piano tecnico normativo, attiene al profilo dell'effettiva opportunità di introdurre strumenti di ricerca della prova connotati da così elevati livelli di intrusività in un ordinamento che intenda mantenere intatti i suoi equilibri democratici.
In altre parole, volendo immaginare, come si è fatto nei precedenti capitoli III e IV, un intervento normativo sul punto, non può farsi a meno di chiedersi, in definitiva, se tutte le guarentigie che si sono in quella sede delineate al fine di contenere nei limiti della proporzione una tanto elevata invasione nella sfera del singolo siano sufficienti o se non siano, piuttosto, ipotizzabili soluzioni più trancianti, ad esempio quella di riservare l'utilizzo di tali strumenti a settori estranei dal processo penale, come quello dei servizi

[607] LAFONT NICUESA, *El agente policial encubierto*, cit., 469 ss.
[608] Secondo ZARAGOZA TEJADA, *La modificación operada por la ley 13/2015*, cit., 25, ciò non toglie che gli elementi probatori quali fotografie, video, registrazioni di immagini e suoni possano confluire nella piattaforma probatoria quali prove documentali.

di sicurezza dello Stato. Una soluzione, quest'ultima, che potrebbe sembrare tutto sommato ragionevole se solo si considera che l'attribuzione di più ampi poteri di intrusione occulta nella riservatezza dei singoli apparirebbe più facilmente giustificabile se intesa a salvaguardare non già l'interesse dello Stato alla repressione di una singola condotta delittuosa ma, addirittura, la sicurezza della Nazione e la sua protezione da fenomeni che rappresentano una minaccia per la sua stessa esistenza e per la sua sovranità[609]. Potrebbe, allora, immaginarsi l'introduzione di una disciplina che, sulla falsariga di quanto previsto dall'art. 266 disp. att. c.p.p. in materia di intercettazioni preventive, subordini il ricorso allo strumento all'applicazione di alcune garanzie minime quanto ai presupposti e al controllo della legittimità dell'atto e, al contempo, preveda la non utilizzabilità dei risultati nel procedimento penale. In questo modo si raggiungerebbe altresì l'obiettivo di escludere che il frutto una intrusione di tale portata nel diritto fondamentale del singolo sia funzionale alle limitazioni della libertà personale che sono tendenzialmente connaturate all'incedere del procedimento penale[610].

Altra possibile soluzione è quella di consentire il ricorso all'atto nella sola fase delle indagini preliminari, senza che i suoi risultati possano essere riversati nel dibattimento. Tanto permetterebbe, quanto meno, di evitare che la fase processuale deputata alla formazione della conoscenza spendibile per lo scioglimento del dubbio concernente l'alternativa tra la colpevolezza e l'innocenza sia inquinata dai frutti del ricorso a strumenti altamente invasivi dei diritti individuali che, in fase di investigazione, potrebbe reputarsi "bilanciato" dalla necessità di compensare il *gap* conoscitivo che

---

[609] Per l'inquadramento dell'attività svolta dai Servizi per la sicurezza dello Stato nei termini di un processo finalizzato alla raccolta di informazioni per la prevenzione di «*fenomeni e comportamenti, tutti meritevoli di attenzione per i loro contenuti di minaccia attuale o potenziale alla sicurezza dello Stato*», DI BITONTO, *Raccolta di informazioni e attività di* intelligence, in *Contrasto al terrorismo interno e internazionale*, a cura di Kostoris e Orlandi, Giappichelli, 2006, 253, che trae la definizione da CONSO, *Sicurezza fra informazione, segreto e garanzie*, in *Per aspera ad veritatem*, 1995, 3, 27. Si vedano, comunque, le considerazioni dell'autrice con riferimento alla possibile intersezione tra attività di indagine e attività di *intelligence* svolta dai Servizi. Si veda anche CURTOTTI, *Procedimento penale e* intelligence *in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. e giust*., 2018, 3, 435 ss. Sul tema dei rapporti tra segreto di Stato e *intelligence*, si veda GREVI, *Spunti e variazioni in tema di rapporti tra segreto di Stato e servizi di sicurezza*, in *Pol. dir.*, 1987, 1, 551.

[610] Nel senso che la proiezione dell'attività di indagine penale sul piano processuale e le sue dirette ricadute sull'aspettativa di libertà del singolo renderebbe il ricorso ad attività di indagine altamente intrusive meno giustificabile di quanto non lo sia nel contesto dell'attività di raccolta di informazioni da parte dei Servizi per la sicurezza dello Stato, RICOTTA, *Questioni sull'utilizzo della backdoor a scopo processuale*, in *Cass. pen.*, 2022, 7/8, 2848.

connota le posizioni dell'inquirente e dell'inquisito nelle prime battute del procedimento penale.

Tenendo, per ora, ferme queste ipotesi, pare che l'analisi delle soluzioni possibili possa essere più proficuamente operata mantenendo distinti, come finora si è fatto, i due strumenti dell'*online search* e dell'*online surveillance*. Quanto, infatti, al primo di tali mezzi, sembra percorribile una soluzione ulteriore rispetto a quelle appena ipotizzate e parzialmente difforme anche da quella che si è vagliata nel precedente capitolo III.

In quella sede si è visto come l'incidenza dello strumento in questione, quanto meno, sul domicilio informatico imponga la ricerca di soluzioni normative improntate al massimo rigore e alla realizzazione di una stretta proporzionalità della misura. Si è altresì evidenziato come, dal punto di vista tecnico-normativo, l'aspetto più complicato da normare sia quello attinente alle modalità concrete di realizzazione dell'accesso da remoto al dispositivo informatico: tale accesso non deve, infatti, realizzarsi in maniera dinamica, consentendo anche l'acquisizione di dati futuri, ma dovrebbe limitarsi a una visione "retrospettiva" e statica del contenuto, con la conseguente possibilità di scaricare solo i dati già formati nello stesso al momento dell'ingresso degli inquirenti. Ove così non fosse, infatti, l'attività realizzata si tramuterebbe in una vera e propria sorveglianza che, incidendo su un bene giuridico diverso e di più elevato rango, dovrebbe rispondere al più rigoroso statuto di tutele abbozzato nel capitolo IV. Nel delineare le coordinate di un possibile intervento normativo, tuttavia, non si è rinunciato a quello che pare essere un aspetto essenziale dello strumento in questione, ovvero il suo carattere occulto. Allo stesso tempo, non sfugge come tale caratteristica sia altresì quella che connota in termini di più elevata intrusività tale strumento, atteso che, rispetto a una ordinaria attività di perquisizione e sequestro, l'accesso all'enorme mole di dati che esso consente non viene neppure compensato dalle possibilità di controllo di chi tale intrusione subisce e del suo difensore di fiducia. Tuttavia, l'essenzialità di un simile connotato nelle attività di *online search* è, forse, solo apparente.

La questione che si agita al fondo del problema è, in buona sostanza, se sia praticabile una soluzione che consenta, al contempo, di non snaturare l'atto – o meglio, di non vanificare le peculiari esigenze investigative allo stesso sottese – e di meglio tutelare la posizione del singolo che lo subisce, realizzando un migliore equilibrio degli interessi in campo. Tale soluzione pare potersi rinvenire nel punto di intersezione tra un

fondamentale principio processuale in tema di prova, quale quello di "non sostituibilità"[611], e le stesse caratteristiche tecniche dello strumento di cui si discorre.

Come si è visto, proprio l'occultezza di quest'ultimo ne determina la non riconducibilità al tradizionale alla perquisizione e al sequestro tradizionali. Esattamente per questa ragione, d'altronde, una parte della dottrina spagnola ritiene che il ricorso a un simile strumento sia legittimo nella misura in cui vi siano speciali esigenze investigative che non consentano di procedere al corrispondente palese dell'atto[612]. Ragionando diversamente, in effetti, si otterrebbe un aggiramento delle garanzie collegate ad atti di indagine che, pur dovendo essere a sorpresa, non necessariamente devono essere occulti, potendo, pur se realizzati in maniera palese, soddisfare le esigenze investigative cui sono finalizzati. Se così è, vi è da chiedersi se anche il cosiddetto sequestro remoto possa realizzarsi a sorpresa ma in maniera palese ed essere, in tal modo, ricondotto all'archetipo processuale del sequestro codicistico. Ne conseguirebbe la possibilità, per chi lo subisce, di partecipare al compimento dell'atto e, conseguentemente, un sensibile riequilibrio degli interessi in campo. Naturalmente, ove la risposta fosse positiva il principio di non sostituibilità e quello di minimo sacrificio quale corollario della proporzionalità suggerirebbero di perseguire tale soluzione anche sul piano normativo.

Da un punto di vista squisitamente investigativo, l'esigenza di realizzare l'atto in questione in maniera occulta deriva dal fatto che, ove fosse dato previo avviso alla parte, nel corso delle operazioni il titolare del dispositivo potrebbe alterarne con estrema facilità il contenuto. Tanto in ragione, da un lato, della caratteristica volatilità dei dati digitali e, dall'altro, del fatto che durante l'intero svolgimento dell'atto il titolare del dispositivo permarrebbe in possesso dello stesso. Si è anche visto, però, che nel momento in cui si accede a un dispositivo informatico da remoto è possibile realizzare immediatamente un *download* integrale del suo contenuto: ciò equivarrebbe, sostanzialmente, a "congelare" i dati presenti al suo interno. Per far ciò, non è necessario procedere a uno *screening* dei dati, ovvero a setacciarli realizzando, di fatto, una perquisizione. Se così è, potrebbe immaginarsi una scansione procedimentale così articolata: il pubblico ministero dovrebbe richiedere al giudice l'autorizzazione a procedere, da remoto, a un "congelamento" del contenuto del sistema informatico, giustificato, ad esempio, dall'impossibilità, difficoltà o dalla non opportunità dal punto

[611] Si veda il cap. 2, par. 2.
[612] BACHMAIER WINTER, *Registro remoto de equipos informáticos*, cit., 23.

di vista investigativo[613] di realizzare l'atto "in presenza". Ottenuta l'autorizzazione, potrebbe apprendersi l'intero contenuto del sistema informatico – senza però procedere alla sua analisi – al solo fine di metterlo al riparo da manipolazioni o alterazioni. A questo punto, l'autorità giudiziaria procedente sarebbe onerata di notificare alla persona sottoposta alle indagini e al suo difensore – nonché all'eventuale terzo interessato – il giorno e il luogo di effettuazione della perquisizione, con l'avviso del diritto di comparire per assistere al compimento dell'atto ed eventualmente di avvalersi di tecnici informatici di propria fiducia nel corso delle operazioni[614]. Quanto alle garanzie successive, a questo punto ben potrebbero operare quelle ordinariamente previste in materia di sequestro codicistico, ivi inclusa quella del deposito di cui all'art. 366 c.p.p. e del riesame.

Vero è che, come si è già evidenziato[615], anche la sola apprensione del contenuto del sistema informatico determina una intrusione nel diritto del singolo atteso che questi perde l'esclusiva disponibilità del dato. È altrettanto vero, però, che tale aspetto sarebbe bilanciato dall'incremento delle garanzie difensive connesse allo svolgimento della successiva perquisizione. Peraltro, la presenza della persona sottoposta alle indagini, del suo difensore e di eventuali terzi nel corso delle operazioni dovrebbe comportare un fisiologico contingentamento dei tempi di durata dell'atto e una ricerca più puntuale e mirata da parte degli inquirenti che vi procedono, con la conseguenza di ridurre il rischio di una cognizione indiscriminata e dilatata nel tempo dell'intero contenuto del sistema informatico. In ogni caso, poi, dovrebbe procedersi all'immediata eliminazione dei dati non acquisiti in quanto non rilevanti per l'accertamento dei fatti. Tale soluzione, infine, consentirebbe altresì di rendere più controllabile l'effettiva limitazione della misura ai soli dati preesistenti, riducendo notevolmente il rischio di un'indebita estensione della stessa a dati futuri ed evitando, al contempo, la ricerca e la trasposizione legislativa delle complicate soluzioni informatiche che dovrebbero mettersi a punto a questo scopo[616].

---

[613] Che dovrebbe declinarsi nei termini, quanto meno, di una potenziale compromissione delle esigenze investigative concrete, che dovrebbe, comunque, essere adeguatamente motivata e fondata su elementi concreti.

[614] Quanto alle successive scansioni procedimentali, ben potrebbero mantenersi ferme quelle già delineate nel capitolo 3.

[615] Cfr. cap. 3, par. 4.3.

[616] Cfr. cap. 3, par. 4.1.3. e 4.3.

Il discorso si complica, invece, per quanto riguarda l'*online surveillance*. L'esigenza investigativa sottesa allo svolgimento dell'atto è, essenzialmente, quella di consentire una vigilanza continuativa ed occulta del soggetto che non sembra in alcun modo riconducibile ad alcun corrispondente codicistico. Allo stesso tempo, essa incide su un bene costituzionale di rango tanto elevato e con modalità tanto penetranti da rendere necessaria una riflessione sulla effettiva opportunità di una sua introduzione nel processo penale.

Tornano, allora, sul tappeto le alternative precedentemente prospettate, come quella di riservarne l'utilizzo alla sola attività di *intelligence* o all'istruzione penale. Si tratta, però, di soluzioni solo apparentemente convincenti.

Quanto alla prima, essa va incontro all'obiezione che non molti anni fa si sollevò rispetto alla proposta avanzata, sul piano politico, per porre rimedio all'eccessivo sacrificio del diritto di *privacy* dei cittadini da tempo denunciato in tema di intercettazioni. Rispetto all'ipotesi di limitarne l'utilizzo alla sola attività di prevenzione, si osservò come in tal modo si sarebbe corso il rischio di peggiorare oltremisura il *vulnus* al diritto fondamentale coinvolto in quanto «l'attività di prevenzione – collocandosi in ambito preprocedimentale – sfugge alle garanzie ed alle tutele che le previsioni costituzionali sono in grado di assicurare all'espletamento delle attività endoprocedimentali. Un rischio troppo alto, che forse non vale la pena di correre, se il filtro alla diffusività delle intercettazioni – pur con le riferite smagliature – dovesse funzionare, ancorché in parte»[617].

Da questo punto di vista, potrebbe apparire più convincente la soluzione di consentire il ricorso allo strumento nella sola fase delle indagini, senza la possibilità di utilizzarne i risultati nel dibattimento. Anch'essa, però, non appare del tutto ragionevole per la banale ragione che gli elementi di prova ottenuti potrebbero comunque essere posti a fondamento delle restrizioni di libertà personale adottabili in fase di indagini. Tanto, peraltro, in una fase caratterizzata da una più accentuata sproporzione tra la posizione del pubblico ministero e quella della persona sottoposta alle indagini e che riserva all'esercizio del diritto di difesa uno spazio più angusto che in dibattimento.

Infine, entrambe le soluzioni in analisi sembrano passibili di un'ulteriore obiezione: esse sarebbero imposte da sole ragioni di opportunità politica. L'esercizio del potere

[617] SPANGHER, *Linee guida per una riforma delle intercettazioni telefoniche*, in *Dir. pen. e proc.*, 2008, 10, 1210.

legislativo trova, infatti, un limite insuperabile nei soli principi costituzionali che, ove violati, determinerebbero l'esigenza di attivare il controllo di costituzionalità al fine di espellere dall'ordinamento giuridico la norma illegittima. Tuttavia, il solo fatto che una determinata misura incida su un diritto fondamentale non vieta in alcun modo al legislatore di introdurla, imponendogli, semmai, esclusivamente di mettere a punto un reticolo di limiti e di garanzie che assicurino il corretto bilanciamento con gli altri interessi costituzionali coinvolti. Unico limite che si frappone all'intervento legislativo, anche nell'ambito processuale penale, è quello del nucleo essenziale del diritto[618], non essendo lo stesso bilanciabile e non tollerando, conseguentemente, alcun tipo di restrizione. Se si tiene fermo questo assunto, solo ove l'attività di *online surveillance* incidesse sul nucleo essenziale del diritto alla riservatezza e all'autodeterminazione nell'uso delle tecnologie informatiche[619] la sua introduzione sarebbe vietata allo stesso legislatore. Di conseguenza, non è possibile escludere *tout court* la legittimità dell'introduzione della misura se essa è improntata a un adeguato bilanciamento degli interessi in campo. È, però, senz'altro possibile affermare che restano comunque escluse soluzioni normative tali da incidere sul nucleo fondamentale e incomprimibile del diritto. Solo in ciò il legislatore incontra un limite invalicabile.

Conviene, allora, tentare di individuare in maniera per quanto possibile puntuale il nucleo incomprimibile del diritto in questione. Pur nella piena consapevolezza dell'estrema discrezionalità che caratterizza una simile operazione[620], sembra potersi affermare con sufficiente convinzione che esso debba rinvenirsi nel diritto di ciascuno di noi a impedire – se non la conoscenza, da parte di terzi, di alcuni tratti della nostra personalità – quanto meno la ricostruzione della nostra personalità nel suo complesso. Questo rischio, però, sembra essere ontologicamente connesso allo svolgimento di un'attività di sorveglianza *online* che si protragga per un periodo di tempo sufficiente a delineare le caratteristiche della quotidianità e del contesto relazionale nel quale l'individuo si muove, fino a pervenire a una sua profilazione. Non rimarrebbe, allora, che una possibilità: visto che bisogna escludere del tutto il ricorso allo strumento con

[618] Per la considerazione secondo la quale laddove una misura comporti un sacrificio totale del nucleo duro dell'istanza si è di fronte ad atti "non disciplinabili" dalla legge, BACCARI e CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy*: uno sguardo d'insieme,* in *Dir. pen. proc*., 2021, 6, 721.

[619] Cfr. cap. 1, par. 3.3.

[620] Cfr. anche le considerazioni del cap. 3, par. 3.

modalità anche solo potenzialmente suscettibili di violare il nucleo essenziale del diritto, occorre prevedere che lo svolgimento di un'attività avente le caratteristiche di quella in oggetto[621] sia circoscritto nel tempo e nello spazio in modo tale da ridurre il raggio dei dati acquisibili in ordine alla vita e alla personalità del suo bersaglio. Una soluzione in questo senso potrebbe essere quella ancorare lo svolgimento dell'*online surveillance* all'esigenza di acquisire informazioni ed elementi di prova rispetto a specifiche attività o incontri che possano ragionevolmente avere luogo nell'ambito del contesto criminale sottoposto ad attenzione investigativa. Si tratterebbe di una soluzione simile a quella messa a punto dal legislatore spagnolo in relazione alla captazione e registrazione di comunicazioni orali ambientali. Come visto[622], gli art. 588 *quater* a ss. Lecrim ammettono il ricorso a tale strumento investigativo ove sia vincolato a comunicazioni che possono aver luogo in incontri concreti tra l'investigato e altre persone e purché si possa ragionevolmente prevedere la misura apporti all'investigazione dati essenziali e di rilievo probatorio per la ricostruzione dei fatti e l'identificazione dell'autore. La misura, in questo modo, risponderebbe a un criterio di assoluta eccezionalità e sarebbe connessa a esigenze investigative specifiche e concretamente controllabili: le problematiche connesse alla sua dubbia proporzionalità[623] verrebbero drasticamente ridimensionate. Al fine di evitare qualsivoglia strumentalizzazione o uso improprio, la norma andrebbe più opportunamente costruita in termini negativi, con la previsione di un divieto di carattere generale e l'individuazione di una precisa e circostanziata eccezione, i cui presupposti dovrebbero trovare ampia e verificabile giustificazione nel provvedimento autorizzativo.

[621] Cfr. cap. 1, par. 2 e cap. 4, par. 1.
[622] Cfr. cap. 5, par. 1.
[623] Cfr. cap. 4, parr. 7 ss.

Bibliografia

AA.VV., *Derecho Constitucional III. Derechos y libertades*, Colex, 2003

AA.VV., *Prova scientifica, ragionamento probatorio e decisione giudiziale*, a cura di Bertolino e Ubertis, Jovene, 2015

AA.VV., *Le indagini atipiche*, a cura di Scalfati, Giappichelli, 2019

AA.VV., *Manuale dei diritti fondamentali in Europa*, Il Mulino, 2019

AGUILERA MORALES, *Proceso penal y causa general*, Thomson, 2008

ALONZI, *L'escalation dei mezzi di intrusione nella sfera privata: ripartire dalla Costituzione,* in *Rev. bras. dir. proc. pen*., 2019, 5

ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della privacy e onde eversive,* in *Arch. pen*., 2015, 3

AÑÓN CALVETE, *Diligencias de Investigación Tecnológica y Derechos Fundamentales*, Tirant lo Blanch, 2015

ASENCIO MELLADO, *La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales*, in *Diario La Ley*, 2013, 8009

ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen. e proc.*, 2008, 6

BACCARI e CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy*: uno sguardo d'insieme,* in *Dir. pen. proc*., 2021, 6

BACHMAIER WINTER, *Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015*, in *Boletín del Ministerio de Justicia*, n. 2195, 2017

BACHMAIER WINTER, *Telephone tapping in the Spanish Criminal Procedure: An Analysis from the European Court of Human Right's Perspective*, JURA, 2007/2 (University of Pécs)

BAILO, *Prosegue la "costituzionalizzazione" del principio di proporzionalità delle pene nella giurisprudenza della Consulta*, in *Giur. it.*, 2013, 1

BALDASSARRE, *Diritti inviolabili*, in *Enc. giur.*, XI, 1989, ora in *Diritti della persona e valori costituzionali*, Giappichelli, 1997

BALDUCCI, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Giuffrè, 2002

BALLESTEROS, *Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la LO 13/2015*, in *Anuario Jurídico y Económico Escurialense*, LII, 2019

BALSAMO, *Le intercettazioni mediante* virus *informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 2016, 5

BARBERA, *Commento all'art. 2 della Costituzione*, in *Commentario della Costituzione*, a cura di Branca, Zanichelli, 1975

BARILE, *Diritti dell'uomo e libertà fondamentali*, Il Mulino, 1984

BARILE, *Le libertà nella costituzione*, Cedam, 1966

BARROCU, *Il captatore informatico: un virus per tutte le stagioni*, in *Dir. pen. e proc.*, 2017, 3

BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali*, in AA.VV., *Le indagini atipiche*, a cura di Scalfati, Giappichelli, 2019

BETZU, *Regolare internet. Le libertà di informazione e di comunicazione nell'era digitale*, Giappichelli, 2012

BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della* privacy, in *Giur. cost.*, 2016, 1

BIN, *L'applicazione diretta della Costituzione, le sentenze interpretative, l'interpretazione conforme a Costituzione della legge*, testo provvisorio della relazione svolta al convegno AIC 2006, in www.astridonline.it

BONINI, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa,* in *Proc. pen. giust*., 2019, 2

BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 2018, 4

BOZIO, *La prova atipica*, in AA.VV., *La prova penale*, a cura di Ferrua, Marzaduri e Spangher, Giappichelli, 2013

BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in AA.VV., *Il diritto alla riservatezza e la sua tutela penale, Atti del terzo simposio di studi di diritto e procedura penali*, Giuffrè, 1970

BRIGHI, *Funzionamento e potenzialità investigative del* malware, in AA.VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie*, a cura di Giostra e Orlandi, Giappichelli, 2018

BRONZINI, *La Carta dei diritti dell'Unione europea come strumento di rafforzamento e protezione dello Stato di diritto*, in *Pol. dir.*, 2016, 1-2

BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in AA.VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra e Orlandi, Giappichelli, 2018

BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* in *Riv. it. scienze giur*., 2017, 8

BUENO DE MATA, *Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*, in *Diario La Ley, Nº 8627, Sección Doctrina*, 19 ottobre 2015

BUZZELLI, *Le letture dibattimentali*, Giuffrè, 2000, 27

BUZZELLI, *Perquisizione di spazi virtuali e preview*, in AA.VV. *Dimensione tecnologica e prova penale*, Giappichelli, 2019

CABEZUDO RODRIGUEZ, *Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal,* in AA.VV., *Nuevos horizontes del derecho procesal*, J.M. Bosch Editor, 2016

CABEZUDO RODRÍGUEZ, *Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal,* in *Las reformas del proceso penal, I Jornada del Boletín del Ministerio de Justicia*, LXX, n. 2186, febbraio 2016

CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont*., 2014, 3-4

CAJANI, *Odissea del captatore informatico*, in *Cass. pen*. 2016, 11

CALO, *Robotics and the Lessons of Cyberlaw*, in *California Law Review*, 2015, vol. 103, n. 3

CAMON, *Sulla inutilizzabilità accordata nel processo penale dei tabulati relativi al traffico telefonico degli apparecchi «cellulari» acquisiti dalla polizia senza autorizzazione dell'autorità giudiziaria*, in *Cass. pen.*, 1996, 12

CAMON, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove incostituzionali*, in *Cass. pen*., 1999, 4

CAMON, *L'acquisizione dei dati sul traffico di comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, 2

CAMON, *Cavalli di troia in Cassazione*, in *Arch. Nuova proc. pen*, 2017, 1

CAMON, *La fase che "non conta e non pesa": indagini governate dalla legge?* in *Dir. pen. e proc.*, 2017, 4

CAMON, *Le indagini preliminari*, in AA.VV., *Fondamenti di procedura penale*, Cedam, 2021

CAMON, *Le prove*, in AA.VV., *Fondamenti di procedura penale*, Cedam, 2021

CAMON, *Le intercettazioni nel processo penale*, Giuffrè, 1996

CAPRIOLI, *Colloqui riservati e prova penale*, Giappichelli, 2000

CAPRIOLI, *Nuovamente al vaglio della Corte costituzionale l'uso investigativo degli strumenti di ripresa visiva*, in *Giur. cost.*, 2008, 3

CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. bras. dir. proc. pen.*, 2017, 2

CAPRIOLI, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, in AA.VV., *Dimensione tecnologica e prova penale*, Giappichelli, a cura di Luparia, Marafioti e Paolozzi, 2019

CAPRIOLI, *Intercettazioni e tutela della privacy nella cornice costituzionale*, in *Cass. pen.*, 2021, 4

CARNEVALE, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. e proc.*, 2009, 4

CARTABIA, *Le sentenze "gemelle": diritti fondamentali, fonti, giudici, in Giur. cost.,* 2007, 5

CARTABIA, *I "nuovi" diritti*, in www.statoechiese.it, 2011

CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana,* Relazione predisposta per la Conferenza trilaterale della Corti costituzionali italiana, portoghese e spagnola, Roma, Palazzo della Consulta 24-26 ottobre 2013

CASCONE, *Il sequestro informatico nel prisma del principio di proporzione*, in *Dir. pen. e proc.*, 2022, 1

CASCONE*, La Corte di Giustizia dell'Unione Europea definisce le condizioni per la legittimità delle normative nazionali in materia di acquisizione dei tabulati. Le ripercussioni sull'ordinamento italiano della sentenza del 2 marzo 2021 (c-746/18) nel caso H.K.,* in *Cass. pen.,* 2022, 2

CAVALIERE, *Questioni attuali in tema di "nuovi diritti"*, in www.dirittifondamentali.it, 2015

CESARI, *Editorial: The Impact of New Technologies on Criminal Justice: An Horizon with Unknown Implications,* in *Rev. bras. dir. proc. pen.*, vol. 5, n. 3, 2019

CISTERNA, *Sull'irrilevanza probatoria dei nastri illeciti una lettura di merito che non convince,* in *Guid. Dir*., 2006, 38

COMOGLIO, *L'inutilizzabilità "assoluta" delle prove "incostituzionali",* in *Riv. dir. proc*., 2011, 1

CONDE-PUMPIDO TOURÓN, *La reforma procesal. Registros de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informático,* in *Jornadas de especialistas en materia de criminalidad informática, Centro de estudios jurídicos,* 2016

COGNETTI, *Principio di proporzionalità. Profili di teoria generale e di analisi sistematica,* Giappichelli, 2010

CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, 2007

CONTI, *La prova scientifica*, in AA.VV., *La prova penale*, a cura di Ferrua, Marzaduri, Spangher e Rivello, Giappichelli, 2013

CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. e proc*., 2018, 9

CONTI, *Sicurezza e riservatezza*, in *Dir. pen. e proc*., 2019, 11

CORDERO, *Prove illecite nel processo penale,* in *Jus*, 1961

CORDERO, *Il procedimento probatorio,* in *Tre studi sulle prove penali*, Giuffrè, 1963

COSTANZI, *Perquisizione e sequestro informatico. L'interesse al riesame nel caso di estrazione di copie digitali e restituzione dell'originale*; in *Cass. pen*., 2016, 1

CRISAFULLI, *Incostituzionalità o abrogazione?*, in *Giur. cost.* 1957

CUOMO, *La prova digitale*, in AA.VV., *Prova scientifica e processo penale*, a cura di Lupària, Cedam, 2022

CURTOTTI, *Procedimento penale e* intelligence *in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. e giust*., 2018, 3

DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc*., 2011, 2

DANIELE, *Contrasto al terrorismo e captatori informatici*, in *Riv. dir. proc*., 2017, 2

DANIELE, *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Proc. pen e giust*. 2018, 5

DANIELE, *L'illusione di domare il captatore informatico*, in *Leg. pen*., 2020, 2

DANIELE, *Il controllo giurisdizionale sull'emissione dell'ordine europeo di indagine: la necessaria simmetria con la disciplina nazionale nei casi interni analoghi*, in *Sistema penale*, 31 marzo 2022

DE LA MATA BARRANCO e BARINAS UBIÑAS, *La protección penal de la vida privada en nuestro tiempo social: ¿necesidad de redefinir el objeto de tutela?*, in *Rev. der. pen. y crim.*, 2014, 11

DELGADO MARTÍN, *Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015*, in *Diario La Ley*, n. 8693, Sección Doctrina, 2 febbraio 2016

DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni unite*, in *Cass. pen.*, 2006, 12

DI BITONTO, *Raccolta di informazioni e attività di* intelligence, in *Contrasto al terrorismo interno e internazionale*, a cura di Kostoris e Orlandi, Giappichelli, 2006

DI BITONTO, *Lungo la strada per la riforma della disciplina delle intercettazioni*, in *Cass. pen.*, 2009

DI BITONTO e MOSCARINI, *Introduzione alla procedura penale*, Giappichelli, 2018

DI BITONTO, *La captazione di flussi telematici*, in AA.VV., *L'intercettazione di comunicazioni*, a cura di Bene, Cacucci Editori, 2018

DI BITONTO, *La regola di giudizio nei singoli riti speciali: il ragionamento probatorio*, in *Cass. pen.*, 2022

DI CHIARA, *Atipicità e sistemi probatori: linee per una fenomenologia generale*, in AA.VV., *Sicurezza e nuove frontiere tecnologiche*, a cura di Militello e Spena, Giappichelli, 2018

DI FILIPPO, *Dati esteriori delle comunicazioni e garanzie costituzionali*, in *Giur. it.*, 1993, 1

DI PAOLO, *Tecnologie del controllo e prova penale*, Cedam, 2008

DI PAOLO, *Judicial investigations and gathering of evidence in a digital online context*, in *Revue internationale de droit pénal*, 2009/1-2, vol. 80

DI TARANTO, *Nuove tecniche d'investigazione nell'era digitale: il "malware" di Stato, Ciberspazio e diritto*, 2017, Vol. 18, 57

DIDDI, *Il regime dell'utilizzabilità*, in Diddi, Filippi e Marandola, *La nuova disciplina delle intercettazioni*, Pacini Editore, 2020

DINACCI, *L'inutilizzabilità nel processo penale. Struttura e funzione del vizio*, Giuffrè, 2008

DI TARANTO, RUGGIERI e CUPELLI, *Nuove tecniche d'investigazione nell'era digitale: il* malware *di Stato,* in *Ciberspazio e dir*., 2017, vol. 18, n. 57

DOMINIONI, *La prova penale scientifica*, Giuffré, 2005

DOMINIONI, voce *Prova scientifica* (diritto processuale penale), in *Enc. dir*., *Annali*, vol. II, tomo I, Giuffrè, 2008

EASTERBROOK, *Cyberspace and the Law of the Horse*, in *Chicago Unbound*, 1996

ELIA, *Libertà personale e misure di prevenzione*, Giuffrè, 1962

ESPIN LOPEZ, *Investigacion sobre equipos informaticol y su prueba en el proceso penal*, Aranzadi, 2021

FALATO, *Sulla categoria dei mezzi atipici di ricerca della prova e le cd. intercettazioni Gps*, in *Giur. it*., 2010, 11

FANUELE, *La libertà personale*, in AA.VV., *Processo penale e Costituzione*, a cura di Dinacci, Giuffrè, 2010

FANUELE, *La localizzazione satellitare nelle investigazioni penali*, Cedam, 2019, 205

FELICIONI. *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. e giust.*, 2016, 5

FERRAJOLI, *Diritto e ragione. Teoria del garantismo penale,* 11a ed.*,* Editori Laterza, 2009

FERRUA, *Il giudizio di diritto nel processo penale,* in *Cass. pen*., 2000, 6

FERRUA, *Contraddittorio e verità nel processo penale,* in *Studi sul processo penale*, in *Studi sul processo penale, vol. II, Anamorfosi del processo accusatorio*, Giappichelli, 1992

FERRUA, *Prove illegittimamente acquisite: passato ed avvenire di un'illustre teoria*, in *Dir. pen. e proc*., 2020, 9

FERRUA, *Ammissibilità della prova e divieti probatori,* in *Rev. Bras. Dir. proc. pen*., 2021, 7

FIANDACA, *Il giudice di fronte alle controversie tecnico-scientifiche. Il diritto e il processo penale*, in *Diritto e questioni pubbliche*, 2005

FILIPPI, *L'intercettazione di comunicazioni*, Giuffrè, 1997

FILIPPI, *La consulta riconosce che l'*home watching *è una prova incostituzionale*, in *Giust. pen.*, 2008, 1

FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen*., 2016, 2

FLOR, *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente,* in *Riv. ita. dir. e proc. pen*., 2007, 2-3

FLOR, *Le indagini ad alto contenuto tecnologico fra esigenze di accertamento e repressione dei reati e tutela penale di tradizionali e nuovi beni giuridici nell'era digitale*, in Flor e Marcolini, *La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Giappichelli, 2022

FOTI, *La nuova disciplina del captatore informatico. Un disfunzionale equilibrio?*, in *Proc. pen. e giust.*, 2021, 1

GAITO e FÙRFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen.*, 2016, 2

GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Cedam, 1992

GALANTINI, voce *Inutilizzabilità*, in *Enc. dir.*, Agg. I, Giuffrè, 1997

GALANTINI, *Alla ricerca della "inutilizzabilità derivata"*, in *Sist. pen.*, 2021, 3

GALETTA, *Principio di proporzionalità*, in *Diritto* on-line, *www.treccani.it*, 2012

GALLO, *Efficacia diretta del diritto UE, procedimento pregiudiziale e Corte Costituzionale: una lettura congiunta delle sentenze n. 269/2017 e 115/2018*, in *Riv. ass. it. cost.*, 2019, 1

GALLUCCIO MEZIO, *"Intercettazioni - corpo del reato" e altre insidiose suggestioni*, in *Dir. pen. e proc.*, 2021, 3

GRAMUGLIA, *Le sezioni unite tornano sul confine dell'onere di motivazione del decreto di sequestro probatorio del* corpus delicti, in *Dir. pen. cont.*, 2018, 9

GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1973, 2

GREVI, *Libertà personale dell'imputato*, in *Enc. dir.*, XXIV, Giuffrè, 1974

GREVI, *La nuova disciplina delle intercettazioni telefoniche*, Giuffrè, 1982

GREVI, *Spunti e variazioni in tema di rapporti tra segreto di Stato e servizi di sicurezza*, in *Pol. dir.*, 1987, 1

GREVI, *I requisiti delle intercettazioni e la motivazione del provvedimento autorizzativo*, in *Cass. pen.*, 2009, 9

GRIFFO, *Perquisizione informatica… e dintorni*, in *Giur. pen. web*, 2019, 5

GRIMALDI, *Il principio di proporzionalità della pena nel disegno della Corte Costituzionale,* in *Giur. pen. web*, 2020, 5

HOBBES, *Leviathan*, Penguin Classics, 1982

HUETE NOGUERAS, *La regulación de las medidas de investigación tecnológica. Análisis de los aspectos referentes a la incorporación al proceso de datos electrónicos de tráfico o asociados*, in *Revista del Ministerio Fiscal*, n. 2, 2016

HUME, *Essays, moral, political, and literary*, Eu-gene f. Miller, 1987

IOVENE, *Pedinamento satellitare e diritti fondamentali della* persona, in *Cass. pen.*, 2012, 10

IOVENE, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont*., 2014, 3-4, 330

JIMÉNEZ CAMPO, *Artículo 53. Protección de los derechos fundamentales*, in Alzaga Villaamil, *Comentarios a la Constitución española de 1978*, Edersa, Madrid, 1996

JIMÉNEZ SEGADO e PUCHOL AIGUABELLA, *Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos* in *Diario La Ley*, n. 8676, Sección Doctrina, 7 gennaio 2016

JOHNSON e POST, *Law and borders – The rise of law in cyberspace*, in *Stanford Law Review*, 1996

KOSTORIS, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in AA.VV., *Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, a cura di Ruggieri e Picotti, Giappichelli, 2011

LAFONT NICUESA, *El agente policial encubierto*, Tirant lo Blanch, 2022

LANZAROTE MARTINÉZ, *La nueva regulación de las intervenciones telefónicas y telemáticas: algunas cuestiones claves y otras discutibles*, in *Revista del ministerio fiscal*, 2017, 3

LARONGA, *Le prove atipiche nel processo penale*, Cedam, 2002

LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *Dir. pen. cont.*, 7 ottobre 2016

LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, vol. 113, n. 2, 1999

LÓPEZ CAUSAPÉ, *Las medidas de investigación tecnológica en la ley de enjuiciamiento criminal tras la reforma de la LO 13/2015 de 5 de octubre. Referencia a las disposiciones comunes*, in *Boletín digital AJFV Penal*, 6 luglio 2016

LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, 4

LUPÁRIA, Computer crimes *e procedimento penale*, in *Trattato di procedura penale*, (diretto da) Spangher, vol. VII, a cura di Garuti, Utet giuridica

MANCUSO, *La perquisizione* on line, in *Jusonline*, 2017, 3

MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, in AA.VV., *Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura*, a cura di Giarda, Giunta e Varraso, Cedam, 2018

MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, in AA.VV., *Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura*, a cura di Giarda, Giunta e Varraso, Cedam, 2018

MANES, *Principio di proporzionalità. Scelte sanzionatorie e sindacato di legittimità*, in *Libro dell'anno del Diritto*, 2013

MANNELLA, *Giudice comune e Costituzione: il problema dell'applicazione diretta del testo costituzionale*, in *Federalismi.it*, 29 dicembre 2010

MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, 12

MARCHENA GOMEZ, *La reforma de las diligencias de investigacion limitativas de los derechos reconocidos en el art. 18 de la ce*. *Proceso penal y nuevas tecnologias*, in Marchena Gómez e González Cuéllar Serrano, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Ediciones Jurídicas Castillo de Luna, 2015

MARCOLINI, *Regole di esclusione e nuove tecnologie*, in *Criminalia*, 2006, 1

MARCOLINI, voce *Processo penale spagnolo*, in *Enc. dir., Annali*, vol. II, tomo I, 2008

MARCOLINI, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche)*, in *Cass. pen*., 2010, 7-8

MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2015, 2

MARCOLINI, *Prove atipiche (diritto processuale penale)*, in *Enc. Dir. Annali*, vol. X, Giuffrè, 2017

MARCOLINI, *La giurisprudenza della Corte di giustizia dell'Unione europea sulla data retention: il baluardo dei diritti fondamentali in Europa*, in Flor e Marcolini, in *La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Giappichelli, 2022

MAZZA, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont., Riv. Trim*., 2013, 3

MAZZA, *Legge e potere: l'irruzione delle Corti internazionali*, in AA.VV., *Legge e potere nel processo penale. Atti del Convegno. Bologna, 4 e 5 novembre 2016*, Cedam, 2017

MEG LETA JONES, *Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw*, in *Journal of Law, Technology & Policy*, Georgetown University, 2018

MELCHIONDA, *Prove illegali e prove illecite nel futuro del processo penale*, in *Riv. pen.*, 1977

MILLER e WEBBER, *Introduction*, in *Proportionality and the rule of law. Rights, Justification, Reasoning*, in *Cambridge University Press*, 2014

MERLO, *Considerazioni sul principio di proporzionalità nella giurisprudenza costituzionale in materia penale*, in *Riv. it. dir. e proc. pen.*, 2016, 3, 1427

MIRANDA ESTRAMPES, *El concepto de prueba ilícita y su tratamiento en el proceso penal* (2a. ed.), J.M. Bosch Editor, 2008

MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, Giappichelli, 1995

MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2012, 2

MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, 3

MONTES ÁLVARO, *Regulación de las medidas de investigación tecnológica y la protección de los derechos reconocidos en el art. 18 CE*, in *Revista del Ministerio fiscal*, 2017, 3

MORRONE, voce *Bilanciamento* (giustizia costituzionale), in *Enc. dir., Annali*, vol. II, t. II, Giuffrè, 2008

MORSELLI, *L'idolo del sequestro come 'atto dovuto' che impedisce la declaratoria di illegittimità in caso di perquisizione illegittima*, in *Proc. pen. giust.*, 2020, 10

NADAL GÓMEZ, *El régimen de los hallazgos casuales en la ley 13/2015, de modificación de la ley de enjuiciamiento criminal,* in *Revista General de Derecho Procesal*, 40, 2016

NAPPI, *Sull'utilizzazione extrapenale dei risultati delle intercettazioni*, in *Cass. pen.*, 2014, 1

NATALI, *Sezioni unite e "legge Bonafede": nuove regole per l'uso trasversale delle intercettazioni*, in *Cass. pen*., 2020, 5

NEGRI, *Fumus commissi delicti. La prova per le fattispecie cautelari*, Giappichelli, 2004

NEGRI, *Splendori e miserie della legalità processuale. Genealogie culturali, "èthos" delle fonti, dialettica tra le Corti*, in *Arch. pen*., 2017, 2

NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. e proc. pen.*, 2020, 1

NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Un tentativo di sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Cedam, 2020

NIEVA FENOLL e TARUFFO, *La valoración de la prueba*, Marcial Pons, 2010

NOBILI, *La nuova procedura penale*. *Lezioni agli studenti*, Clueb, 1989

NOBILI, sub *art. 191*, in *Commento al nuovo codice di procedura penale*, a cura di Chiavario, vol. II, Utet, 1990

NOBILI, *Scenari e trasformazioni del processo penale*, Cedam, 1998

NOCERINO, *Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in *Dir. pen. e proc*., 2021, 8

NOCERINO, *Il captatore informatico nelle indagini interne e transfrontaliere*, Cedam, 2022

NUVOLONE, *Le prove vietate nei paesi di diritto latino,* in *Riv. dir. proc*., 1966

ORLANDI, *Atti e informazioni dell'autorità amministrativa nel processo penale*, Giuffrè, 1992

ORLANDI, *Provvisoria esecuzione delle sentenze e presunzione di non colpevolezza*, in AA.VV., *Presunzione di non colpevolezza e disciplina delle impugnazioni (Atti del Convegno, Foggia-Mattinata, 25-27 settembre 1998)*, Giuffrè, 2000

ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, 1

ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, *in Riv. it. dir. e proc. pen.*, 2014, 3

ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici,* in *Arch. pen. web*, 25 luglio 2016

ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma,* in *Riv. it. dir. e proc. pen.*, 2018, 2

PACE, *Problematica delle libertà costituzionali, Parte generale*, Cedam, 1990

PACE, *Nuove frontiere della libertà di «comunicare riservatamente» (o, piuttosto, del diritto alla riservatezza)?,* in *Giur. it*, 1993, 1

PADUA, *L'accesso alla casella e-mail e l'acquisizione dei contenuti: un delicato inquadramento normativo,* in *Proc. pen. e giust*., 2018, 3

PANZAVOLTA, *Contributo allo studio della invalidità derivata*, Aras Edizioni, 2012, 263

PAOLOZZI, *Relazione introduttiva*, in AA.VV., *Dimensione tecnologica e prova penale*, a cura di Luparia, Marafioti e Paolozzi, Giappichelli, 2019

PARLATO, *Problemi insoluti: le perquisizioni on-line*, in AA.VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra e Orlandi, Giappichelli, 2018

PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, in *Proc. pen. e giust*., 2020, 2

PERONI, *Prova illegittima e prova illecita: una singolare nozione di inutilizzabilità ex art. 191 c.p.p. (nota a Sez. un., 30/10/02, dep. 21/5/03, n.22327, Carnevale)*, in *Cass. pen.*, 2005, 3

PICARO, *Perquisizione illegittima e limiti della inutilizzabilità*, in *Arch. pen.* 2020

PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in AA.VV*., Il diritto penale dell'informatica nell'epoca di Internet*, a cura di Picotti, Cedam, 2004

PICOTTI, *Ratifica della convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. int.*, 2008, 5

PIERRO, *Una nuova specie di invalidità: l'inutilizzabilità degli atti processuali penali*, Edizioni Scientifiche italiane, 1992

PINELLI, *Sul trattamento giurisdizionale della CEDU e delle leggi con essa confliggenti*, in Giur. cost., 2007, 5

PINELLI, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di stato"*, in *Dir. pen. cont*., 2017, 4

PINO, *Conflitto e bilanciamento tra diritti fondamentali. Una mappa dei problemi*, in *Etica & Politica*, 2006, 1

PINO, *Diritti fondamentali e principio di proporzionalità*, in *Ragion pratica*, 2014, 2

PISANI, *La custodia preventiva: profili costituzionali*, in *L'ind. pen*., 1970

PISANI, *Libertà personale e processo*, Cedam, 1974

PISANI, *Le prove. Appunti sul Titolo I, Libro III, del Progetto di un nuovo codice di procedura penale, Testo della relazione scritta presentata al Seminario sul tema: «Prospettive del nuovo processo penale»*, a cura dell'Istituto Superiore Internazionale di Scienze Criminali (Siracusa, 9-14 gennaio 1978), in *Riv. it. dir. proc. pen*., 1978

PITTIRUTI, Digital evidence *e processo penale*, 2017, Giappichelli

POLLICINO, *Diritto all'oblio e conservazione dei dati. La Corte di Giustizia a piedi uniti: verso un* digital right to privacy, in *Giur. cost.*, 2014, 3

PROCACCINO, *Piccoli equivoci senza importanza: tra intercettazioni di flussi telematici, perquisizioni e prove atipiche*, in *Cass. pen.*, 2022, 9

RAFARACI, *Ricognizione informale dell'imputato e (pretesa) fungibilità delle forme probatorie*, in *Cass. pen*, 1998, 6

RAFARACI, *Verso una* law of evidence *dei dati*, in *Dir. pen. proc.*, 2021, 7

RECCHIA, *Il principio di proporzionalità nel diritto penale. Scelte di criminalizzazione e ingerenza nei diritti fondamentali*, Giappichelli, 2020

REIMAN, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, Santa Clara computer & high tech. L. J., 27, 38, 1995

RICCI, *Le prove atipiche*, Giuffrè, 1999

RICHARD GONZÁLEZ, *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y garabación de imagen y sonido*, La Ley, 2017

RICOTTA, *Questioni sull'utilizzo della backdoor a scopo processuale*, in *Cass. pen.*, 2022, 7/8

RIVELLO, *La prova scientifica*, Giuffrè, 2014

RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio del materiale informatico*, in *Cass. pen.*, 2018, 1

RIVELLO, *Le intercettazioni mediante captatore informatico*, in AA.VV., *Le nuove intercettazioni*, a cura di Mazza, Giappichelli, 2018

RODOTÀ, voce *Riservatezza*, in *Enc. Treccani online*, in https://www.treccani.it/enciclopedia/riservatezza_res-9e2b210a-9bc7-11e2-9d1b-00271042e8d9_%28Enciclopedia-Italiana%29/

RODRÍGUEZ LAINZ, *Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción*, in *Diario La Ley*, n. 8896, 2017

RODRÍGUEZ, *Artículo 18: Derecho al honor, a la intimidad y a la propia imagen*, en Alzaga Villaamil, *Comentarios a la Constitución española de 1978*, Edersa, Madrid, 1996

ROUSSEAU, *The basic political writings*, Hackett Publishing Company, 1987

RUGGIERI, *Riprese visive e inammissibilità della prova*, in *Cass. pen.*, 2006, 12

SÁNCHEZ RUBIO, *Los registros remotos sobre equipos informáticos: la investigación del «hacker legal»*, in AA.VV., *Fodertics 6.0 los nuevos retos del derecho ante la era digital*, a cura di Bueno de Mata, Comares, 2017

SÁNCHEZ RUBIO, *El principio de proporcionalidad en las medidas de investigación tecnológicas*, in AA.VV., *Investigación y proceso penal en el siglo XXI: nuevas tecnologías y protección de datos*, a cura di Zamora, Pereira, Ordóñez Ponz, Moral García, Aranzadi, 2021

SANDULLI, *La proporzionalità dell'azione amministrativa*, Cedam, 1998

SANDULLI, voce *Proporzionalità*, in *Dizionario di diritto pubblico*, a cura di Cassese, Giuffrè, 2006

SANTORIELLO, *La legalità della prova*, in AA.VV., *Processo penale e Costituzione*, a cura di Dinacci, Giuffrè, 2010

SCACCIA, *Il bilanciamento degli interessi come tecnica di controllo costituzionale*, in *Giur. it.*, 1998, 6

SCACCIA, *Proporzionalità e bilanciamento dei diritti nella giurisprudenza delle Corti europee*, in *Rivista AIC*, 2017

SCALFATI, *Premessa*, in AA. VV., *Le Indagini Atipiche. Leggi penali tra regole e prassi*, a cura di Scalfati, 2014

SCELLA, *Prove penali e inutilizzabilità. Uno studio introduttivo*, Giappichelli, 2000

SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. ita. dir. e proc. pen.*, 2012, 2

SIGNORATO, *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra e Orlandi, Giappichelli, 2018

SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018

SILVESTRI, *L'individuazione dei diritti della persona*, in *Dir. pen. cont.*, 27 ottobre 2018, 2

SLOBOGIN, *Public privacy: camera surveillance of public places and the right to anonymity*, in *Mississippi Law Journal*, 2002, 72

SPANGHER, *Linee guida per una riforma delle intercettazioni telefoniche*, in *Dir. pen. e proc.*, 2008, 10

SPILLER, *La sentenza Tele2 Sverige: verso una* digital rule of law *europea?*, in *IANUS Dir. e fin.*, dic. 2017

STAIANO, *Diritto alla riservatezza e potere pubblico, in Federalismi.it*, 2017, 17

STONE SWEET e MATHEWS, *Proportionality balancing and global constitutionalism*, in *Columbia journal of transnational law*, 47

TAORMINA, *Narcoanalisi*, in *Enc. Dir.*, vol. XXVII, 1977

TAVASSI, *Le intercettazioni ubiquitarie fra legalità e non dispersione della prova*, in *Arch. pen*., 2018, 2

TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. pen. e proc.*, 2014, 6

TESTAGUZZA, Exitus acta probat "*Trojan" di Stato: la composizione di un conflitto*, in *Nuovo arch. pen*., 2016, 2

TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, Cedam, 2014; Pittiruti, Digital evidence e *procedimento penale*, Giappichelli, 2017

TIM WU, *Is Internet Exceptionalism Dead?, The next digital decade: essays on the future of the internet*, Berin Szoka & Adam Marcus, eds., Techfreedom, 2010 (2011)

TONINI, *Documento informatico e giusto processo*, in *Dir. pen. e proc.*, 2009, 4

TONINI e CONTI, *Il diritto delle prove penali*, Giuffrè, 2014

TORRE, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. e proc.*, 2015, 9

TORRE, *Il captatore informatico, tra riforma Orlando e sistema processuale*, in *Giur. ita*., 2018, 7

TORRE, *Il riesame del sequestro probatorio di documenti informatici*, in *Giur. ita*, 2019, 6

TORRE, *Indagini informatiche e principio di proporzionalità*, in *Proc. pen. e giust.*, 2019, 6

TREVIJANO, *La inviolabilidad del domicilio*, Tecnos, 1992

TROGU, *Le indagini svolte con l'uso di programmi spia (trojan horses),* in AA.VV., *La giustizia penale nella "rete". Le nuove sfide della società dell'informazione nell'epoca di Internet*, a cura di Flor, Falcinelli e Marcolini, ed. DipLap, 2015

TROGU, *Intrusioni segrete nel domicilio informatico,* in AA.VV., *Le indagini atipiche*, a cura di Scalfati, Giappichelli, 2019

UBERTIS, *Riflessioni sulle "prove vietate"*, in *Riv. pen.*, 1975

VACIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Giappichelli, 2012

VALIÑO CES, *Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015*, in *Diario La Ley*, n. 8731, 2016

VASSALLI, *Il diritto alla libertà morale (contributo alla teoria dei diritti della personalità)*, in AA.VV., *Studi giuridici in memoria di Filippo Vassalli*, Utet, 1960

VASSALLI, *I metodi di ricerca della verità e la loro incidenza sulla integrità della persona*, in *Riv. pen.*, 1972, 1

VIGORITI, *Prove illecite e Costituzione,* in *Riv. dir. proc.*, 1968

WARREN e BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1890

ZAPPALÀ, *Le garanzie giurisdizionali in tema di libertà personale e di ricerca della prova,* in AA.VV., *Libertà e ricerca della prova nell'attuale assetto delle indagini preliminari. Atti del Convegno dell'Associazione tra gli studiosi del processo penale*, Giuffrè, 1995

ZARAGOZA TEJADA, *La modificación operada por la ley 13/2015. El agente encubierto informático,* Curso de formación continua de fiscales, Centro de Estudios jurídicos, 2016

ZARAGOZA TEJADA, *El registro de dispositivos de almacenamiento masivo de la informacion,* in AA.VV., *Investigation tecnologica y derechos fundamentales. Comentario a las modificaciones introducidas por la Ley 13/2015*, Aranzadi, 2017

ZARAGOZA TEJADA, *El registro remoto de equipos informaticos,* in AA.VV., *Investigation tecnologica y derechos fundamentales. Comentario a las modificaciones introducidas por la Ley 13/2015*, Aranzadi, 2017

ZOCO ZABALA, *Nuevas tecnologías y control de las comunicaciones. LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de la medidas de investigación tecnológica*, Thomson Reuters, 2015