UNIVERSITÀ DEGLI STUDI DI GENOVA

SCUOLA DI SCIENZE SOCIALI
DIPARTIMENTO DI GIURISPRUDENZA

CORSO DI LAUREA IN
GIURISPRUDENZA

Tesi di laurea in Diritto Processuale Penale

"Tecnologie di controllo nel procedimento penale"

Relatore:
Chiar.mo Prof. Mitja GIALUZ

Candidato:
Stefano BANAUDI

Anno accademico 2023-2024

INDICE SOMMARIO

CAPITOLO II

LA DISCIPLINA SULLE INTERCETTAZIONI IN CHIAVE EVOLUTIVA

PARTE II

NODI CRITICI DELLA DISCIPLINA DELLE TECNOLOGIE DI CONTROLLO

CAPITOLO III

I NUOVI STRUMENTI DELLA TECNICA TRA VUOTO NORMATIVO E PROSPETTIVE *DE IURE CONDENDO*

CAPITOLO IV

LA TENSIONE TRA TUTELA DEI DIRITTI FONDAMENTALI ED ESIGENZE REPRESSIVE

INTRODUZIONE

Dal celebre modello panottico fino al mondo orwelliano dominato dal Grande Fratello, quella della sorveglianza costituisce una dimensione ineliminabile della modernità. Le tecnologie dell'informazione e della comunicazione, unitamente alla pluralità degli strumenti di monitoraggio elettronico a nostra disposizione, l'hanno resa una pratica oggi sempre più ricorrente e pervasiva della vita quotidiana. I dilemmi etici che essa pone si apprezzano inevitabilmente anche sul piano dell'accertamento penale, posto che l'autorità giudiziaria è in grado di acquisire una mole sempre più cospicua di dati e, per giunta, prima ancora che il *trial* vero e proprio abbia inizio. L'evoluzione tecnologica ha, in effetti, sortito sul procedimento penale un duplice effetto: la rapida obsolescenza della prova dichiarativa, che abdica al ruolo di prova regina, e la trasfigurazione delle indagini preliminari, che da «fase che non pesa e che non conta» divengono «gigantesca istruzione sommaria». In altri termini, il baricentro del procedimento penale sembra essersi spostato dal dibattimento e la raccolta di elementi decisivi ai fini del giudizio anticipata ad un momento in cui la garanzia del contraddittorio non opera ancora, circostanza che si pone in maniera stridente con un modello di stampo accusatorio. Strumenti sempre più sofisticati consentono di frugare nella vita delle persone come mai prima d'ora, rafforzando l'assunto di Carnelutti secondo il quale il processo è già di per sé una pena. A fronte di ciò, mentre fuori dai confini nazionali si ragiona di "domicilio informatico" e di *computer forensics*, il legislatore nostrano è rimasto inerte, sottraendosi ad una cruciale sfida di civiltà. Quello che ha fatto, anzi, è stato ripensare, ora in prospettiva "garantista" ora "giustizialista", la disciplina delle intercettazioni di conversazioni o comunicazioni, mentre, per tutto ciò che esula dall'intercettazione in senso stretto, si è prontamente trincerato dietro lo scudo dell'art. 189 c.p.p., lasciando alla giurisprudenza il delicato onere di riportare a sistema il frastagliato panorama dei mezzi di ricerca della prova di cui si avvale l'organo inquirente. Il risultato è una imbarazzante situazione di vuoto normativo, che costringe l'interprete ad un notevole sforzo ermeneutico per ritagliare una soluzione di volta in volta confacente al caso di specie. Il presente lavoro si propone quindi di illustrare, in chiave diacronica e comparatistica, la normativa concernente le tecnologie di controllo all'interno del procedimento penale, intendendosi con tale locuzione, oltre alle tradizionali intercettazioni, tutti quei mezzi atipici di ricerca della prova che rappresentano ormai una risorsa imprescindibile ai fini dell'accertamento penale.

PARTE I
FISIOLOGIA DELLE TECNOLOGIE DI CONTROLLO

CAPITOLO I
IL RAPPORTO TRA TECNOLOGIA E DIRITTO NELL'ACCERTAMENTO PENALE

Sezione I
TECNOLOGIE DEL CONTROLLO E PROVA PENALE

SOMMARIO: 1. Scienza e tecnica nell'accertamento penale. – 2. L'intersezione tra scienza, tecnica e processo nell'ordinamento statunitense: *the new surveillance technologies*. – 3. Nuove forme di *electronic surveillance*. – 4. Obsolescenza della prova dichiarativa: le indagini preliminari da "fase che non pesa e che non conta" a "gigantesca istruzione sommaria".

1. *Scienza e tecnica nell'accertamento penale*

L'ambizione al controllo sui consociati non rappresenta certo una novità. Se si pensa al celebre modello panottico, in cui la possibilità di esercitare un controllo ubiquitario e senza soluzione di continuità è sufficiente a distogliere i reclusi da comportamenti non conformi alle aspettative del sorvegliante, ci si può convincere del fatto che la sorveglianza incarna una delle più penetranti manifestazioni autoritative[1]. Senonché, l'«intima contraddizione della procedura penale»[2] risiede in ciò, che le finalità cognitive, che spingono a dilatare i confini dell'indagine, sono inesorabilmente destinate a confrontarsi con le prerogative riconosciute ai singoli, le quali impongono all'opposto di circoscrivere i margini della ricerca. Evocando l'autorità di Francesco Carrara, del resto, il rito penale come insieme di forme poste a salvaguardia dei galantuomini si contrappone al codice penale come codice dei delinquenti[3].

Oggi, però, lo scenario appare assai più complesso di quello immaginabile ai tempi di Bentham. Assume anzitutto rilievo l'incidenza del progresso tecnologico e delle sfide poste dalla «società dell'informazione»[4]: sebbene infatti la storia dell'umanità sia da sempre una

[1] J. BENTHAM, *Panopticon – Ovvero la casa di ispezione*, Venezia, III ed., 2002.

[2] Al riguardo A. CAMON, *Sfondi*, in AA. VV., *Fondamenti di procedura penale*, Padova, 202, p. 7 ss.

[3] F. CARRARA, *Il diritto e la procedura penale*, pubblicato in *Opuscoli di diritto criminale*, III ed., Prato, 1889, p. 19.

[4] Sulla quale cfr., per tutti, L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

storia di progresso, l'ultimo secolo è stato attraversato da un'evoluzione del sapere scientifico e tecnico che, senza pari in altre epoche, ha innescato profonde trasformazioni sociali. A fronte delle sempre più sofisticate tecnologie di condizionamento messe a punto dai «capitalisti della sorveglianza»[5] cresce proporzionalmente la delicatezza dell'accertamento penale. Gli strumenti attualmente diffusi consentono un monitoraggio pervasivo, che stravolge i paradigmi su cui si fondano le ormai datate, per quanto tuttora vigenti, previsioni normative in materia; applicazioni tecniche sino a qualche tempo fa del tutto sconosciute ai più vengono poste al servizio dell'inquirente. Come si legge al considerando n. 3 della direttiva 2016/680/UE[6], «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della raccolta e della condivisione di dati personali è aumentata in modo significativo. La tecnologia, come mai in precedenza, consente il trattamento di dati personali nello svolgimento di attività quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati».

Questo repentino sviluppo della tecnica ha contribuito a delineare un clima emergenziale, alimentato da istanze securitarie, che, ponendo sullo sfondo le prerogative dei singoli, minaccia di alterare gli equilibri nell'assetto dei rapporti tra poteri autoritativi e libertà fondamentali. Il pericolo paventato è stato efficacemente stigmatizzato dalla Corte e.d.u., ad avviso della quale il rischio capitale è quello di distruggere la democrazia con il pretesto di difenderla[7]. Per la sua vocazione assiologica, il procedimento penale – in quanto «ricerca ordinata (*omissis*) di verità»[8], sistema in cui «la caccia vale più della preda e cioè il modo in cui si agisce conta più del risultato»[9] – costituisce senza dubbio l'osservatorio privilegiato per valutare l'attuale consistenza dei diritti fondamentali.

Nel tracciare un quadro di sintesi dei complessi rapporti intercorrenti tra processo penale e nuovi strumenti di conoscenza a carattere tecnico e/o scientifico, nonché, più in generale,

[5] S. ZUBOFF, *Il capitalismo della sorveglianza*, Luiss University Press, Roma, 2019, p. 309 ss.

[6] Si tratta della direttiva relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

[7] Nel testo ufficiale, «*undermine or even destroy democracy under the cloak of defending it*». Così Corte e.d.u., 13 settembre 2018, *Big brother watch c. Regno Unito*, § 308.

[8] G. CAPOGRASSI, *Giudizio, processo, scienza, verità*, Milano, 1959, p. 57.

[9] F. CORDERO, *Diatribe sul processo accusatorio*, in ID, *Ideologie del processo penale*, Milano, 1966, p. 220.

del "problema del controllo" con riferimento ai nuovi *investigative tools,* viene in rilievo la dicotomia tra *liberalizing technologies* e *public protective technologies*[10], ovvero tra "tecnologie di libertà" e "tecnologie di controllo"[11]. Le prime – al cui alveo possono essere ricondotti telefoni, cellulari, *internet* e strumenti simili – vengono così definite in ragione della capacità di promuovere l'esercizio delle libertà individuali. Al tempo stesso, non se ne può cogliere il *proprium* senza tenere conto delle zone d'ombra che le stesse proiettano sulle nostre vite: icasticamente è quindi stata prospettata l'immagine «di una tecnologia bifronte, come l'antico dio Giano»[12], che enfatizza la corrispondente proporzionalità tra vantaggi e pericoli arrecati.

La diffusione delle nuove tecnologie ha prodotto specularmente effetti anche sui sistemi di *law enforcement,* cioè sulle attività delle istituzioni preposte al controllo e alla difesa sociale: in altri termini, a fronte dell'attitudine dei criminali a massimizzare l'impiego dell'offerta tecnologica a fini offensivi, si potenzia la capacità di controllo sugli individui da parte delle *law enforcement agencies,* che possono contare su ritrovati idonei a garantire performanti risultati. Esempi di questo genere sono i sistemi satellitari di controllo del posizionamento del soggetto come il GPS o la c.d. *facial recognition technology*.

Il parallelo sviluppo di *liberalizing technologies* e *public protective technologies* fa quindi sì che la nostra società sia attraversata da due vettori contrapposti, la "globalizzazione del terrore" da un lato e la "globalizzazione del controllo" dall'altro[13]. Non sorprendono dunque i timori legati all'immagine orwelliana del Grande Fratello, all'avvento in forma elettronica del *Panopticon* benthamiano, all'incubo della società della totale sorveglianza o dell'implacabile trasparenza, popolata soltanto da «uomini di vetro»[14]. Questi rapidi cenni bastano per intuire come il sistema di giustizia penale, chiamato a adempiere ad

[10] Le espressioni sono di A. ETZIONI, *Implications of selected new technologies for individual rights and public safety*, in 15, *Harvard Journal of Law and Technology*, 261 e 274 (2001-2002).

[11] Così S: RODOTÀ, *Timori, ipotesi, realtà,* in *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* 1997 p. 27.

[12] S. RODOTÀ, *Timori,* cit., p. 27.

[13] Il rilievo è di G. DI PAOLO, *"Tecnologie del controllo e prova penale"*, Padova, 2008, p. 5.

[14] S: RODOTÀ, *Timori*, cit., p. 26. Nella letteratura statunitense cfr. D. SOLOVE, *Privacy and power: computer databases and methafhors for information privacy*, in 53, *Stanford Law Review*, 1393-1398 (2001).

un'essenziale funzione cognitiva[15], incontri innanzi a sé sfide sempre più ardue, in quanto sempre più complessa è divenuta la società in cui l'illecito è radicato[16].

Come rileva Rodotà[17], «l'innovazione tecnologica ha inciso profondamente sul modo in cui la sfera della politica non solo si presenta ma si struttura»: l'insieme di queste trasformazioni viene icasticamente definito dall'Autore «tecnopolitica»[18]. Tanto radicale è il cambiamento dovuto al diffondersi delle tecnologie dell'informazione e della comunicazione, nonché all'espansione planetaria di Internet. Infatti, mentre le tecnologie precedenti, che instauravano una comunicazione verticale e unilaterale, esaltavano allo stesso modo il potere del comunicatore e la passività della platea dei destinatari del messaggio, le nuove tecnologie sembrano modificare questo quadro, determinando una comunicazione orizzontale ed esaltando i poteri individuali e collettivi, così caricati di potenzialità egualitarie.

D'altro canto, lo stesso Rodotà ha evidenziato, in molti suoi scritti, i principali problemi che un mezzo di comunicazione quale Internet presenta al giurista[19]. Secondo lo studioso, la tradizionale nozione di *privacy*, riproducente lo schema della proprietà privata, non è più in grado di comprendere una dimensione tanto profondamente mutata[20]. Nata come diritto dell'individuo borghese a escludere gli altri da ogni forma di invasione della propria sfera privata, si è strutturata nel tempo come diritto di ogni persona al mantenimento del controllo sui propri dati. Divenute entità disincarnate, le persone hanno sempre più bisogno di una tutela del loro corpo elettronico. Da ciò l'opportunità di un *habeas data* quale diritto che si

[15] Il procedimento penale è stato efficacemente definito come «un ingranaggio tutto volto al trattamento dei dati personali», che per sua stessa natura si alimenta della «raccolta», della «selezione» e del «raffronto» di informazioni: così S. CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in D. NEGRI, *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 5. In maniera non dissimile, il processo rappresenterebbe un «sistema predisposto per acquisire, formare e far interagire le informazioni utili e rilevanti per elaborare decisioni giudiziali» secondo R. ORLANDI, *Il processo penale nell'era di* internet, in *Dir. pen. proc.*, 1998, p. 140.

[16] A fare questa considerazione è G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 6.

[17] S: RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, p. 119.

[18] S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004.

[19] Su tutti S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014.

[20] *Ibidem*, p. 27-32.

sviluppa dal concetto dell'*habeas corpus*, dal quale si è evoluta storicamente la libertà personale.

Non potendocisi affidare ad un'"etica della sorveglianza", vi è la necessità, ad avviso di Rodotà, di esercitare forme di controllo sui diversi soggetti che esercitano la sorveglianza, generando un "contropotere diffuso" che contribuisca a escludere la piena legittimazione sociale e istituzionale dei sorveglianti. A questo proposito, si deve segnalare che l'Italia è stato uno dei primi Paesi ad abbozzare una sorta di *Internet Bill of Rights*, un documento d'indirizzo che richiama le dichiarazioni sui diritti di tradizione anglosassone e che si propone di tracciare alcune possibili linee-guida in vista di future riforme legislative e politiche che coinvolgano, in qualche modo, Internet[21]. Particolare rilievo ai fini dell'accertamento penale merita il punto della Dichiarazione dedicato all'inviolabilità dei sistemi e domicili informatici, in base al quale senza l'autorizzazione dell'autorità giudiziaria, nei soli casi e modi previsti dalla legge, dovrebbe essere vietato l'accesso ai dati della persona che si trovino su dispositivi personali, su elaboratori remoti accessibili tramite credenziali da qualsiasi elaboratore connesso a Internet o simultaneamente su dispositivi personali e, in copia, su elaboratori remoti, nonché l'intercettazione di qualsiasi forma di comunicazione elettronica. Come si intuisce, la disposizione si riferisce non solo al problema delle investigazioni digitali in ambito penale, ma anche alle azioni di sorveglianza indiscriminata.

Lo stretto connubio tra sviluppo tecnologico e strategie commerciali ha contribuito a creare, nel corso degli anni, quelle che Lyon definisce le "società sorvegliate", ovvero società che, per le loro procedure amministrative e di controllo, dipendono dalle tecnologie della comunicazione e dell'informazione[22]. L'azione di sorveglianza sistematica è diventata non solo una *routine*, ma ormai una parte inscindibile della vita quotidiana di chiunque. Per questo motivo, quello della sorveglianza costituisce un tema chiave nella società contemporanea: mentre espressioni come "postmoderno", "società globalizzata" o "società dell'informazione" sono state coniate per gettare luce sulle più rilevanti trasformazioni sociali del presente, il concetto di "società sorvegliata" aspira a mettere in risalto alcuni di

[21] Il testo della Dichiarazione è consultabile all'indirizzo *http://www.camera.it/application/xmanager/projects/leg17/attachments/upload_file/upload_files/000/000/187/dichiarazione_dei_diritti_internet_pubblicata.pdf>*

[22] D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2002, p. 1.

quei processi sociali che sono stati prodotti da queste trasformazioni e alle quali essi stessi hanno contribuito.

Posto che la sorveglianza rappresenti un tratto distintivo delle postmoderne società globali dell'informazione, appare difficile negare che essa sia oggi da considerarsi come il mezzo essenziale per garantire l'ordine sociale. Tuttavia, proprio la coincidenza tra "società dell'informazione" e "società sorvegliate" consente a Lyon di parlare di "morte della *privacy*". Secondo l'Autore, questa circostanza impone di studiare la sorveglianza anche dal punto di vista delle implicazioni etiche e politiche, interrogandosi circa i possibili scenari futuribili. In effetti, «nella sorveglianza contemporanea, è presente il sogno idolatrico dell'onnipercezione incarnata nel panopticon: questo è ciò che il minaccioso scintillio dell'occhio elettronico rappresenta»[23]. Se un tanto è vero, ad essere in atto non è semplicemente un miglioramento tecnico delle strategie di controllo, ma una nuova forma di regolazione sociale. Le nuove pratiche di sorveglianza, potenziando e amplificando, per mezzo dell'informatizzazione, gli apparati burocratici ai quali è affidato il controllo sociale, congiungono moderno e postmoderno.

Ma c'è di più. L'avanzare delle società sorvegliate ha determinato una vera e propria "scomparsa dei corpi"[24]. Questo fenomeno, invero già in germe a partire dagli anni Sessanta, ha assunto, con il perfezionarsi delle tecnologie di informazione e comunicazione, dimensioni tanto rilevanti da rendere possibili i rapporti a prescindere dalla copresenza. Si tratta di un punto chiave nella disamina sulla sorveglianza, in quanto indica le ragioni strutturali, storiche e sociali per le quali la stessa si è diffusa in modo capillare: proprio l'esplicito focalizzarsi dell'attenzione sulle informazioni di tipo personale – ciò che integra la sorveglianza – è uno dei mezzi principali con cui tenere insieme le relazioni incorporee. Una conseguenza dello strutturarsi di relazioni incorporee è che le nozioni moderne di "pubblico" e "privato" sono mutate e i confini divenuti incerti, «dal momento che ogni sorta di dettagli di quella che un tempo era la vita "privata" circolano entro le stesse reti telematiche "pubbliche"»[25]. Pure questo aspetto è gravido di implicazioni: infatti, come osserva il sociologo, «la riattribuzione di un corpo alle persone rappresenta un obiettivo etico

[23] *Ibidem*, p. 206.

[24] *Ibidem*, p. 19.

[25] *Ibidem*, p. 21.

che dovrebbe informare il nostro essere uomini delle società postmoderne dell'informazione»[26].

Ad avviso di Lyon, è possibile distinguere tra sorveglianza individuale e sorveglianza istituzionale: mentre la prima può essere praticata con gli oggetti che si comprano nei negozi di materiale di spionaggio, la seconda si è sviluppata come un aspetto della burocrazia. L'elemento sconvolgente risiede nel fatto che, in molti casi, la sorveglianza istituzionale non è segreta. I cittadini sanno di essere tracciati, vedono le telecamere, sono consapevoli che le ricerche effettuate in Internet e i dati di traffico sono custoditi, ma ciononostante non appaiono scoraggiati ad un impiego massivo dei telefoni cellulari. Questo fenomeno si comprende forse alla luce del delicato rapporto tra sorveglianza e paura: è infatti dalla "cultura del timore" diffusa nella società moderna, innescata, in special modo, dagli avvenimenti dell'11 settembre 2001, che possono essere motivate quelle reazioni che hanno condotto, per esempio, all'installazione di telecamere nelle strade. In questo modo, si finisce per giustificare il potere e la volontà di controllo dei cittadini innocenti in cambio della promessa di una maggiore sicurezza. La conclusione alla quale si può così pervenire[27] è che l'attività di controllo capillare non è più una prerogativa di quei regimi che si suole definire "autoritari", ma può avvenire in pressoché qualsiasi cornice politica o costituzionale. La tendenza diffusa, in definitiva, è quella di uno Stato che sorveglia le comunicazioni elettroniche con ogni mezzo possibile.

La sorveglianza mirata ha, pertanto, ceduto il posto, almeno nella fase iniziale della raccolta delle informazioni, alla sorveglianza indiscriminata. Si assiste, in particolare, ad un'inversione dialettica delle modalità di prelievo delle informazioni: mentre, prima dell'era digitale, l'attività di sorveglianza prendeva le mosse da un soggetto ben preciso e identificato, oggi si tende a raccogliere le informazioni di tutti, indiscriminatamente e senza un obiettivo preciso, cosicché l'estrazione di quelle d'interesse su un certo individuo avviene soltanto *ex post*. Questo sistema evoca un'attività di pesca a strascico, in cui la rete non cattura soltanto i pesci desiderati ma anche altri di contorno, per il solo fatto che si trovano lì in quel momento[28]. Siamo in presenza di un'azione che riesce a scavare in profondità come

[26] *Ibidem*, p. 212.

[27] A queste conclusioni, in una prospettiva che trascende l'ambito della procedura penale, perviene G. ZICCARDI, Internet, *controllo e libertà*, Milano, 2015, p. 224 ss.

[28] *Ibidem*, p. 226.

mai era successo prima, penetrando nell'area più intima della personalità dei cittadini. Ad essere mutato non è, quindi, solo il modo in cui si effettuano i controlli, ma anche la facilità con cui si possono ottenere i dati sensibili riferiti a una persona.

Del tema della sorveglianza si è occupato anche uno dei più autorevoli intellettuali del secondo Novecento, Zygmunt Bauman[29]. A lui si deve la folgorante definizione della «modernità liquida», la quale presenta innegabili ricadute sul piano della sorveglianza, a sua volta scivolata a poco a poco in uno "stato liquido". In realtà, l'espressione «sorveglianza liquida», più che una definizione esauriente della sorveglianza, è soprattutto un orientamento, un modo di contestualizzarne gli sviluppi nella modernità tanto fluida quanto inquietante di oggi. La sorveglianza, che un tempo appariva solida e stabile, è divenuta flessibile e mobile, diffondendosi e penetrando in molti ambiti della vita in cui in passato aveva un'influenza marginale. La liquefazione delle forme sociali e la separazione tra potere e politica sono due caratteristiche chiave della modernità liquida che hanno evidenti attinenze con la sorveglianza.

Il mondo di oggi è post-panottico, perché gli ispettori possono essere sfuggenti e rifugiarsi in ambiti irraggiungibili. Più in particolare, il diagramma panottico appare inadeguato a raffigurare efficacemente l'odierna meccanica della sorveglianza: per quanto Foucault abbia visto nella struttura panottica di Bentham la chiave per comprendere l'ascesa delle moderne società dotate di autodisciplina, il *Panopticon*, relegato ormai ai margini della società, non costituisce più il modello o la strategia di dominio universale. Inoltre, nella transizione dal moderno al liquido-moderno, si registra un mutamento della sorveglianza indotta dalla sicurezza. In una società imperniata sull'ubiquità dei pericoli, l'idea che una convivenza sicura possa essere concepita solo come risultato di una costante vigilanza ingenera una dipendenza dalla sorveglianza. Secondo Bauman, però, il paradosso del mondo ipersecuritario è che la generazione post-elettronica, pur essendo protetta dall'insicurezza più di qualsiasi altra passata, avverte ogni giorno un crescente ed inusitato senso di insicurezza.

Tutte queste considerazioni postulano la necessità di un'etica per la "nuova sorveglianza". Dato che l'adiaforizzazione, ossia l'affrancamento delle azioni da una valutazione etica reso possibile dall'uso di strumenti tecnici, si riverbera in maniera preponderante anche sulla sorveglianza, appare quant'altri mai opportuna una riscoperta della persona umana e, segnatamente, dell'Altro, inteso quale titolare autonomo di diritti e

[29] Z. BAUMAN-D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, Bari, 2013.

oggetto dell'altrui responsabilità. Vero è, del resto, che, se la relazionalità umana si rivela solo al cospetto dell'Altro, vi è qualcosa di profondamente inquietante in sistemi di sorveglianza che sembrano demolire tale relazionalità[30]

A questo punto, il problema che si pone in via principale è quello di capire come la nuova epistemologia scientifica si coniughi con gli istituti preordinati dalla legge per assicurare al processo le conoscenze affidabili da impiegare nella ricostruzione del fatto. Come correttamente ricorda Dominioni, «la cultura della conoscenza giudiziaria ha registrato e, in misura non irrilevante, sta ancora registrando un sensibile ritardo nel farsi carico del rinnovamento delle concezioni epistemologiche in ambito scientifico e tecnologico»[31]. L'incapacità del legislatore di tenere il passo dell'evoluzione tecnico-scientifica si registra anche nel ritardo a predisporre i congegni processuali utili a rendere praticabili le nuove risorse cognitive nella funzione probatoria con la dovuta affidabilità: è ciò che si dice distinguere la "vera scienza" dalla *junk science*.

Molteplici e peculiari sono, come si capisce, le questioni alle quali pone di fronte la "nuova prova scientifica". In prospettiva definitoria, è questa un'espressione ellittica, che designa un complesso di operazioni probatorie per le quali si adoperano strumenti di conoscenza attinenti alla scienza e alla tecnica. Lo studio della nuova prova scientifica, oltre a mettere a fuoco le specificità originanti dalla natura controversa e dall'elevata specializzazione degli strumenti tecnico-scientifici che si utilizzano, deve farsi carico di chiarirne il rapporto con l'atipicità probatoria. Per quanto in Italia il ricorso a questi mezzi sia sempre stato ricondotto al grimaldello dell'art. 189 c.p.p. nella duplice prospettiva di non precluderne e controllarne l'impiego, è utile osservare che gli strumenti probatori tecnico-scientifici sono per natura estranei alle previsioni del catalogo legale: essi esorbitano dalla normazione di "competenza" della legge[32], quasi come un "giardino proibito" alla legge [33]. Se la legge è chiamata a regolare i presupposti del loro impiego, non può che affidarsi alla scienza e alla tecnica quanto allo statuto epistemologico degli stessi. Quello della riconduzione della nuova prova scientifica al fenomeno dell'atipicità probatoria è dunque un

[30] *Ibidem*, p. 126 ss.

[31] O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005, p. 7.

[32] *Ibidem*, p. 15.

[33] L'espressione è mutuata da P. FERRUA, *Un giardino proibito per il legislatore: la valutazione delle prove*, in *Quest. giust.*, 1998, p. 587 ss., che la riferisce alle regole di valutazione dei risultati probatori.

vero e proprio equivoco: l'atipicità probatoria poggia, infatti, su un concetto di relazione, il cui termine di riferimento sono le previsioni del catalogo legale[34]. La relatività della natura atipica di determinati mezzi probatori trova riscontro nella circostanza per la quale taluni esemplari erano qualificati come atipici nella previgente legislazione perché in essa non erano previsti, mentre oggi figurano come tipici in quanto contemplati dalla vigente normativa[35]. Per intendere come un tale fraintendimento abbia inciso anche nel corpo legislativo, basti pensare al tenore letterale dell'art. 189 c.p.p., il quale, ponendo il suo oggetto in correlazione negativa con le previsioni del repertorio legale[36], male si adatta alla nuova prova scientifica[37]. La conclusione alla quale si può forse pervenire è che proprio dal vuoto normativo, cioè dal difetto di regole specifiche per l'ammissione della prova scientifica, discenda l'esigenza, nel vigente ordinamento italiano, di riferirsi all'art. 189 c.p.p.

Sebbene negli ultimi decenni l'accertamento penale si sia arricchito di inediti apporti tecnologici e contributi scientifici, solo oggi si avverte, con imperdonabile ritardo, l'enorme impatto che il proliferare della *scientific evidence* ha sortito sul processo penale[38], al punto che sorge l'interrogativo se la prova orale rappresenti ancora la chiave di volta del modello accusatorio[39]. Sempre più evidenze scientifiche, formatesi nella prima fase del procedimento e veicolate in quella dibattimentale, riducono il "contraddittorio per la prova" a mero esercizio dialettico su materiali già "preconfezionati" in sede di indagini preliminari, con

[34] Accenna al fatto che la tipicità-atipicità è riferibile solo alle componenti dei mezzi di prova disciplinati dalla legge e non anche allo strumento di prova G. F. RICCI, *Le prove atipiche*, Milano, 1999, p. 570.

[35] Cfr. la notazione di P. TONINI, *Manuale di procedura penale*, V ed., p. 214.

[36] La norma parla di "prova non disciplinata dalla legge".

[37] Al riguardo cfr. ancora O. DOMINIONI, *La prova penale scientifica*, cit., p. 33. Secondo l'Autore, risalendo alle origini di questa aporia, si approderebbe probabilmente al sistema delle prove legali, che, oltre a predeterminare la valutazione dei risultati delle operazioni probatorie, tipizzava anche gli strumenti di conoscenza che in queste si dovessero impiegare. La rottura del sistema delle prove legali ha operato sulla duplice direttrice di sottrarre i risultati probatori a valutazioni precostituite dal legislatore e di eliminare dalla normazione legale gli strumenti scientifico-tecnici di ricostruzione processuale del fatto, lasciando che nel concreto delle singole operazioni probatorie si attingesse, quando necessario e possibile, alle potenzialità della scienza e della tecnica.

[38] Si vedano G. CANZIO, *Prova scientifica, ricerca della «verità» e decisione giudiziaria nel processo penale*, in *Decisione giudiziaria e verità scientifica*, Quaderni della rivista trimestrale di diritto e procedura civile, n. 3, Milano, 2005, p. 55; O. DOMINIONI, *In tema di nuova prova scientifica*, in *Dir. pen. proc.*, 2001, p. 1061; P. TONINI, *Prova scientifica e contraddittorio*, in *Dir. pen. proc.*, 2003, p. 1459.

[39] Cfr. L. LUPARIA, *L'inchiesta penale tra echi del passato e risvolti della modernità*, Intervento al convegno *"Inchiesta penale e pregiudizio. Una riflessione interdisciplinare"*, Teramo, 4 maggio 2006.

buona pace, fra l'altro, dei principi del libero convincimento e della centralità del giudice[40]. Se la scienza forense, intesa come la scienza che studia il valore processuale di determinati accadimenti ai fini della costituzione di possibili fonti di prova, si è già confrontata in passato con gli ostacoli delineati dal progresso, appare oggi più che mai chiamata ad accostarsi al mondo del *computer*, nonché alle fonti di prova da esso generate: ciò viene naturalmente a configurarsi come un banco di prova per i principi tradizionali, operando una *summa divisio* tra quelli destinati a rimanere immutati e quelli costretti ad adeguarsi ai cambiamenti che il "mondo digitale" impone.

Assume rilievo, in tale prospettiva, la c.d. *computer forensics*, vale a dire «l'estensione di teorie, principi e prassi, proprie della scienza forense generalmente intesa, al mondo dell'informatica e delle nuove tecnologie»[41]. Non è difficile, del resto, constatare come sempre più il diritto si stia muovendo nella direzione della digitalizzazione, cosicché, anche nel corso di indagini correlate a reati tradizionali, vengono in essere, quasi ogni volta, aspetti tecnologici[42]. Appare quindi del tutto ragionevole la previsione secondo la quale, nel prossimo futuro, qualsiasi tipo di fonte di prova sarà "digitale", in quanto «il processo di informatizzazione e digitalizzazione della nostra società condizionerà direttamente il mondo giuridico e, soprattutto, il suo aspetto processuale»[43].

Questa circostanza è utile a chiarire il carattere multidisciplinare della *computer forensics*: nell'ambito di tale disciplina si possono infatti distinguere un aspetto informatico, uno giuridico e uno investigativo. Per quanto concerne i profili legali, si deve sottolineare come le conoscenze di diritto processuale e, segnatamente, quelle sulle corrette modalità di acquisizione della prova debbano giustapporsi alle conoscenze dei limiti e dei diritti previsti dalla legge[44]. Accanto a queste distinzioni preliminari, la *forensics* congiunge un aspetto prettamente teorico (basi teoriche informatiche e giuridiche) ad uno eminentemente pratico

[40] Sul punto, si veda L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, p. 128.

[41] *Ibidem*, p. 6.

[42] Si vedano le interessanti osservazioni in A. GHIRARDINI-G. FAGGIOLI, *Computer forensics*, Milano, 2007 (p. XIV), dove gli Autori notano come «Riservare la *computer forensics* ai soli reati informatici, quelli per intenderci connessi con la violazione delle reti, è riduttivo. Analisi informatiche di natura forense sono state utili nelle più svariate situazioni, dal traffico di droga ai movimenti eversivi, dall'evasione fiscale a frodi avvenute nel settore dell'allevamento del bestiame».

[43] L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica*, cit., p. 9.

[44] *Ibidem*, p. 14.

(conoscenza della prassi e degli strumenti): l'unione di questi aspetti consente di delineare il panorama attuale della *computer and network forensics*. Resta, sullo sfondo, l'interrogativo sul futuro di questa disciplina, che non potrà prescindere da una seria valorizzazione degli aspetti etici a essa sottesi: l'auspicio pare, allora, quello che alla *computer ethics* venga affiancata una *forensic ethics*, ovvero un esame puntuale dei principi etici che devono animare ogni soggetto chiamato ad analizzare dati a fini investigativi[45].

2. *L'intersezione tra scienza, tecnica e processo nell'ordinamento statunitense:* the new surveillance technologies

L'analisi della *computer forensics* si è sempre basata, anche in Italia, su parametri nordamericani. Tre sono i profili di maggiore criticità sui quali ha posto l'accento la dottrina nordamericana[46]. Il primo punto concerne la corretta definizione delle aree di specializzazione per chi si trova a dover operare nel settore della *computer and network forensics*: in particolare, sarebbe opportuna una prima distinzione di base tra *digital crime scene technicians* (o *first responders*) e *digital evidence examiners*. Un secondo punto critico riguarda i metodi adoperati dagli investigatori per assicurare l'affidabilità della prova digitale, nonché la possibilità che venga a mancare un metodo sistematico che presenti la prova, al termine dell'*iter* investigativo, come affidabile e idonea a corroborare le conclusioni correlate a quella prova. Infine, il terzo punto di dibattito investe la necessità di una standardizzazione: la mancanza di standard accettati a livello generale si concretizza sovente in una raccolta delle prove, documentazione e custodia incompleta, in errori di analisi e interpretazione della fonte di prova digitale. Da ultimo, un auspicabile momento di approfondimento, all'interno della *forensics*, potrebbe riguardare, come già osservato, gli aspetti etici: in altri termini, si pone l'opportunità di una *forensics ethics*, ovvero un'analisi dei principi etici che devono ispirare i soggetti chiamati ad analizzare dati a fini investigativi[47].

[45] *Ibidem*, p. 25.

[46] Si veda, in particolare, lo studio di E. CASEY, *Digital Evidence and Computer Crime. Forensic science, computer and the Internet*, Second Edition, Elsevier, 2004, p. 1 ss.

[47] A questo proposito, si veda L. LUPARIA-G. ZICCARDI, *Investigazione penale e tecnologia informatica*, cit., p. 25.

Diversamente da quanto avvenuto in Italia, nell'ordinamento statunitense il tema della *scientific evidence* e, più in generale, dell'impatto del progresso scientifico-tecnologico sul processo è stato indagato approfonditamente. Negli ultimi decenni, in particolare, si è assistito, anche a seguito di alcune importanti pronunce della Corte Suprema[48], allo sviluppo di un vivace dibattito attorno al tema della *scientific evidence* e della *technological surveillance*[49]. È stato messo in luce come «qualunque sia il motivo sotteso alla diversità di approccio, la cultura giuridica statunitense sembra connotarsi rispetto a quella italiana per una marcata e precoce consapevolezza di come le nuove tecnologie e conoscenze scientifiche abbiano significative ricadute sul fenomeno processuale, in tutti i suoi snodi essenziali»[50]. Emblematiche del connubio tra giustizia penale statunitense e progresso tecnologico-scientifico sono le c.d. *criminal investigations*: com'è noto, infatti, l'ultimo trentennio si è caratterizzato per l'impiego sempre più massiccio delle nuove tecnologie del controllo per la ricerca della prova[51]. Una vera e propria esplosione ha riguardato, in particolare, la sorveglianza elettronica, al punto che la varietà dei mezzi utilizzabili a fini di monitoraggio pare oggi essere praticamente illimitata. Si impone, pertanto, una preliminare rassegna delle *new surveillance technologies*.

Adottando anzitutto un approccio descrittivo, si può constare come la letteratura statunitense classifichi i nuovi strumenti investigativi, a seconda del livello di invasività sul diritto alla *privacy*, in tre categorie[52].

---

[48] Il riferimento è a *Daubert v. Merrell-Dow Pharmaceuticals, Inc.*, 509 *U.S.* 579 (1993) e *Kyllo v. United States*, 533 *U.S.* 27 (2001). Nella dottrina italiana per un commento alla prima cfr. O. DOMINIONI, *La prova penale scientifica*, cit., p. 137 ss.; sulla seconda v. M. MIRAGLIA, *Il IV emendamento alla rincorsa del progresso: perquisizioni e lotta alla droga nel diritto U.S.A.*, in *Dir. pen. proc.*, 2002, p. 105.

[49] Il tema è al centro di molti convegni. Si vedano, per esempio, E. CHENG, S. KREIMER, R. SIMMONS, F. LEDERER, *Symposium: the powers and pitfall of technology*, in 60, N.Y.U. *Annual Survey of American Law*, 675 (2002) nonché T. CLANCY, A. M. CLOUD, T. MACLIN, D. SKLANSKY, C. SLOBOGIN, J. TOMKOVICZ, K. URBONYA, *Symposium: The effect of technology on Fourth Amendment analysis and individual rights*, in 72, *Miss. Law Journal*, 1-564 (2002-2003). Cfr. anche AA. VV., *Electronic evidence*, a cura di MASON, London, LexisNexis, Butterworths, 2007.

[50] G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 11.

[51] A titolo di esempio, si possono segnalare *pen registers & track and trap devices, gun detectors, thermal imaging devices, Key Logger Systems* (KLS), la *Magic lantern* e il c.d. FBI *Carnivore system*, la *facial recognition technology* e gli altri sistemi di identificazione biometriche (tra cui la DNA *identification* e la *retinal recognition*), la *video surveillance*, la *satellite surveillance* e tutte le differenti forme di *covert surveillance* che la tecnologia può produrre.

[52] Così R. SIMMONS, *The powers and pitfalls of technology, Technology enhanced surveillance by law enforcement officials*, in 60, *NYU Ann. Survey of American Law*, 711 (2005).

Al livello più elevato troviamo le c.d. *hyper-intrusive searches*, categoria nella quale sono ricompresi «tutti quei mezzi di indagine che danno accesso a informazioni estremamente riservate»[53]. In ragione della spiccata attitudine intrusiva all'interno della sfera privata, tali strumenti consentono di controllare gli aspetti più intimi della vita delle persone, all'insaputa degli interessati e in tempo reale. L'esempio paradigmatico è rappresentato dalle intercettazioni di comunicazioni, da tempo ricondotte all'alveo delle *search* ai sensi del IV Emendamento e oggetto di puntuale disciplina legislativa, sebbene, in tempi più recenti, siano venuti alla ribalta anche le c.d. video-intercettazioni e congegni come la Lanterna Magica e i *Key Logger Systems*[54].

La seconda categoria è quella della c.d. *virtual surveillance*, ricomprendente quelle tecnologie dotate di una minore capacità intrusiva rispetto alle precedenti in ragione della diversa natura del dato captato: è il caso dei *pen registers & trap and trace devices*[55], dei *thermal imagers*[56] o dei c.d. *see-through devices*[57]. Queste tecnologie consentono agli investigatori di acquisire conoscenze non accessibili senza l'ausilio tecnologico, ma si tratta pur sempre di informazioni meno sensibili di quelle che costituiscono l'oggetto della prima categoria[58]. Come nel caso delle *hyper-intrusive searches*, anche per la *virtual surveillance*

[53] G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 19.

[54] Per *keylogger system* si intende un programma che monitora i caratteri digitati su tastiera del personal computer, così permettendo di carpire le *passwords* di accesso al sistema informatico o di forzare la c.d. *strong encryption* (cioè la protezione dei dati realizzata tramite crittografia). La lanterna magica è una tecnologia recentemente sviluppata dell'FBI. Come i *keyloggers*, essa consente di rilevare i caratteri digitati, ma la sua installazione non costringe gli investigatori ad accedere fisicamente al sistema informatico. Può infatti essere invitata via *e-mail*, approfittando delle falle dei sistemi antivirus. In argomento cfr. C. WOO, M. SO, *The case for Magic Lantern: September 11 highlights the need for increased surveillance*, in 15, *Harvard Journal of Law and* Technology, 521 (2002).

[55] Queste tecnologie non il contenuto della comunicazione telefonica o telematica, ma solo i dati esterni della medesima.

[56] Essi si limitano ad una sorta di mappatura del calore emanato dall'edificio, per evidenziare la differenza di temperature tra le varie zone del medesimo, senza svelare alcunché su ciò che vi accade. Sulle questioni poste dall'impiego del *thermal imager* e di tecnologie similari cfr. S. SALTZBURG, D. CAPRA, *American criminal procedure. Cases and commentary*, VII ed., 2004, p. 64-72, nonché e soprattutto T. CLANCY, A. M. CLOUD, T. MACLIN, D. SKLANSKY, C. SLOBOGIN, J. TOMKOVICZ, K. URBONYA, *op. cit.*

[57] Si tratta di tecnologie binarie che, pur essendo in grado di scrutare attraverso barriere opache come indumenti o borse, possono rivelare soltanto la presenza o l'assenza dell'oggetto ricercato (armi o sostanze stupefacenti), senza dire nulla circa gli altri effetti personali contenuti sotto o all'interno di tali involucri.

[58] La sorveglianza virtuale consente per lo più di ricostruire relazioni personali intrattenute dal sospettato, i suoi movimenti e attività. Queste informazioni possono essere ottenute tramite l'acquisizione dei dati esterni delle comunicazioni telefoniche ed elettroniche (in tempo reale, con *pen registers* e *trap and trace devices*; *ex post*, attraverso i tabulati telefonici), mediante l'impiego di dispositivi in grado di localizzare il soggetto e/o tracciarne elettronicamente i movimenti (come *beepers* e telecamere di sorveglianza), nonché con l'acquisizione di documentazione presso enti pubblici e/o privati. Per una sintesi delle varie forme di

il problema che si pone è se, in assenza di una specifica disciplina legislativa, il loro impiego possa essere qualificato come *search*, ovvero se possa essere riconosciuta in capo ai soggetti monitorati una legittima aspettativa alla *privacy*.

Infine, la terza e ultima categoria è quella delle c.d. *high volume collection technologies*. Si tratta di quei ritrovati «che procedono alla raccolta di massa di informazioni provenienti da varie fonti e, successivamente, passano al setaccio i dati così raccolti per individuare quell'esigua percentuale che potrebbe essere rilevante per le indagini»[59]. Questi dispositivi «vengono impiegati per lo più in aree pubbliche o aperte al pubblico, dove transita una gran quantità di soggetti, al fine di controllarne gli spostamenti o di identificare persone ricercate o sospettate»[60]. Esempi di questo genere di tecnologie sono il sistema di identificazione biometrico noto come *facial recognition technology*[61] e il c.d. *Carnivore System*, utilizzato dall'FBI per il controllo delle comunicazioni via *internet*[62]. Posto che in entrambi i casi si discute di strumenti di indagine che consentono di captare informazioni "esposte al pubblico", rispetto alle quali si sarebbe indotti ad escludere l'esistenza di una legittima aspettativa di *privacy*, il problema di fondo è se lo *screening* di massa che li connota sia idoneo ad alterarne la natura, cioè se il salto qualitativo e quantitativo innescato dal supporto tecnologico trasformi in *search* la "sorveglianza rafforzata" che essi consentono di condurre.

"*surveillance of relationship and movements*" cfr. W. LAFAVE, *Search and seizure: A treatise on the Fourth Amendment*, IV ed., vol. I, 2004, p. 729-785.

[59] G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 21.

[60] *Ibidem*.

[61] Tale sistema si basa sull'intreccio delle immagini raccolte dagli inquirenti con i dati biometrici della persona ricercata. In proposito, si veda J. BROGAN, *Facing the music: the dubious constitutionality of facial recognition technology*, in 25, *Hasting Comm. & Ent. Law Journal*, 65 (2002-2003); C. MILLIGAN, *Facial recognition technology, video surveillance and privacy*, in 9, *Southern California Interdisciplinary Law Journal*, 295 (1999).

[62] Il *Carnivore System* consiste in un *software* sviluppato per la ricerca di *e-mails* sospette attraverso dei filtri preimpostati. Una volta applicato all'*Internet Server Provider* (ISP), esso setaccia tutte le trasmissioni in entrata e in uscita alla ricerca delle comunicazioni etichettate come "sospette" dai programmatori. Il filtro può operare ricercando tutte le *e-mail* indirizzate a (o provenienti da) un certo individuo, oppure quelle che contengono determinate parole chiave o che hanno specifici oggetti. Successivamente all'individuazione delle comunicazioni sospette, queste vengono conservate per gli inquirenti, i quali possono acquisirne i dati esterni oppure il contenuto, a seconda che il *Carnivore System* sia stato usato nel *pen mode* o nel *full mode*. In argomento cfr. A. ETZIONI, *op. cit.*, p. 275; S. SALTZBURG, D. CAPRA, *op. cit.*, p. 53; W. LAFAVE, *op. cit.*, p. 740.

3. *Nuove forme di* electronic surveillance

Come si è visto, il paradigma della sorveglianza pervade attualmente ogni momento della vita individuale e la sfera privata risulta sempre più erosa dalla possibilità di accesso da parte dei pubblici poteri ad una massa ingente di informazioni personali. Le *surveillance technologies* consentono agli investigatori l'equivalente funzionale delle attività investigative tradizionali come pedinamenti, perquisizioni e sequestri, ma con risultati quantitativamente e qualitativamente superiori. Mentre il carattere occulto e continuo del monitoraggio elettronico rende particolarmente efficace la sorveglianza, l'ausilio tecnologico permette il controllo simultaneo di un gran numero di persone con costi certamente più contenuti di quelli che occorrerebbero se le medesime attività venissero svolte direttamente dagli investigatori. Senonché, lo strutturale ritardo del diritto rispetto all'evoluzione tecnico-scientifica ha determinato l'impiego dei nuovi *high-tech investigative tools* in un contesto di vuoto normativo: è così toccato agli operatori del diritto e, segnatamente, alla giurisprudenza il delicato onere di individuare il regime giuridico applicabile, come, del resto, già in passato era avvenuto per le intercettazioni.

Nell'ordinamento americano, una volta verificata la possibilità di inquadrare gli inediti strumenti di indagine nell'ambito della disciplina legale prevista per le attività istruttorie tipiche, si è posta l'esigenza di un raffronto con il IV Emendamento, allo scopo di accertare la riconducibilità degli stessi alla nozione costituzionale di *search and seizure*. Proprio questa seconda è l'operazione più delicata, in quanto la categoria della prova incostituzionale e la correlata regola di esclusione probatoria rappresenterebbero l'unico baluardo contro illegittime interferenze dei poteri pubblici nella sfera privata, a fronte di una disciplina legislativa lacunosa, quando non del tutto inesistente. Se, fino agli anni Sessanta, la giurisprudenza, ispirata da una logica eminentemente proprietaria, offriva una lettura restrittiva del precetto costituzionale evocato, dopo il caso *Katz*[63] il baricentro della tutela si

[63] La storica pronuncia *Katz v. United States* del 1967 ha rappresentato il punto di svolta decisivo nell'esegesi del IV Emendamento, segnando l'abbandono della *trespass doctrine* in favore di una concezione più ampia e moderna del diritto al rispetto della vita privata. Il caso da cui è scaturito tale arresto concerneva l'intercettazione di conversazioni telefoniche realizzate da una cabina pubblica, cioè un luogo rispetto al quale non era concepibile una violazione dei *property rights* degli occupanti. In particolare, le dichiarazioni incriminanti erano state captate dagli agenti federali grazie all'installazione, all'esterno della cabina telefonica, di un congegno elettronico che contemporaneamente captava e registrava i suoni. In quella vicenda la Corte concluse che la portata del IV Emendamento non poteva più essere ricostruita in base alla presenza o meno di una *physical intrusion* in un ambito privato, quanto piuttosto in base all'esistenza o meno di una ragionevole aspettativa di *privacy*. Alla pronuncia si deve l'individuazione dei criteri in base ai quali effettuare la verifica circa la sussistenza o meno della *reasonable expectation of privacy* (il c.d. *Katz test*): per quanto nella prassi si siano riscontrate non poche difficoltà nell'applicazione del *Katz test*, innegabile merito della *Katz decision* è quello di avere riconosciuto la necessità di estendere la tutela costituzionale del IV Emendamento anche nei

è spostato dalla proprietà privata alla dignità personale: da quel momento il vaglio giurisdizionale sulla legittimità o meno dei nuovi strumenti investigativi è venuto a dipendere non più dalla presenza di un *physical trespass*, bensì dalla *reasonable expectation of privacy*. A partire dal caso *Katz*, tuttavia, nel delicato giudizio di valore diretto a determinare oltre quale soglia le attività investigative che sfruttano i ritrovati tecnologici possano essere ricondotti alla nozione costituzionale di *search*, la Corte Suprema ha fatto ricorso a varie tecniche argomentative, le quali hanno complessivamente sortito l'effetto di negare la tutela garantita dal IV Emendamento.

Da una sintetica ricognizione degli espedienti interpretativi enucleati per delimitare l'ambito di operatività delle garanzie costituzionali poste a tutela del «*right to be secure*» sembrano potersi distinguere quattro argomenti principali[64]. Anzitutto, viene preso in considerazione il c.d. *revelatory behaviour*, locuzione con la quale si allude alla condotta del soggetto che, consapevolmente, porta a conoscenza di un terzo o del pubblico un'informazione confidenziale. Per quanto sussistano diverse varianti del *revelatory behaviour*, si afferma che la condotta rivelatrice esclude la violazione del IV Emendamento, perfino laddove l'autorità ne tragga vantaggio dalla scelta individuale grazie agli strumenti tecnologici. Un'altra tecnica argomentativa utilizzata per delimitare il raggio di operatività delle garanzie costituzionali previste nel IV Emendamento è quella che dà rilievo al c.d. *informational content*, cioè al contenuto dell'informazione acquisita. Anche in questo caso si riscontra la presenza di varianti, ma il nucleo essenziale di tale argomento risiede nell'impossibilità di ricondurre al concetto costituzionale di *search* quelle forme di sfruttamento del progresso tecnologico che si traducono in attività inidonee, di per sé, a fornire alcuna informazione all'autorità procedente. Il terzo modello argomentativo pone l'accento sulla natura e sul carattere della tecnologia. Dall'analisi di molteplici pronunce emerge come il vaglio di compatibilità delle nuove tecniche investigative con i principi costituzionali venga eseguito sulla base di vari parametri, quali il grado di sofisticazione della tecnologia, la circostanza che il dispositivo tecnologico si limiti a potenziare i sensi umani o li soppianti, il tipo di senso potenziato e l'entità del potenziamento, il fatto che la strumentazione utilizzata sia *generally available to the public* oppure *in general public use*. Infine, un'ulteriore strategia argomentativa sovente impiegata è quella che accorda rilevanza

confronti di tecniche investigative fisicamente non intrusive e che permettono l'apprensione di beni intangibili come le comunicazioni.

[64] Tale ricostruzione è di G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 101 ss.

alla *location of the privacy interest*, ossia al carattere dei luoghi in cui si riconosce l'esistenza di un interesse alla riservatezza. In materia si suole distinguere tra domicilio in senso stretto (*the home*), altri luoghi privati (*other private domains*) e spazi pubblici: l'intensità della protezione dell'interesse alla *privacy* è stata perciò graduata secondo una scala che vede al massimo livello il domicilio strettamente inteso, al mimino i *public places* e, in posizione intermedia, i luoghi privati diversi dal domicilio.

Un notevole passo in avanti nel percorso interpretativo del IV Emendamento è stato compiuto, in epoca più recente, con la pronuncia *Kyllo v. United States* del 2001[65]. In quella occasione la Corte Suprema ha tentato di adeguare il concetto di *search* alle insidie provenienti dalle più recenti tecnologie. Il caso *Kyllo* trae origine da una vicenda piuttosto semplice: la polizia sospetta che l'indagato coltivi marijuana all'interno della sua abitazione, ma, non disponendo di elementi sufficienti per ottenere un mandato di perquisizione, decide di mettere sotto controllo l'edificio mediante un *thermal imager* del tipo *Agema Thermovision 210*[66]. Emerso che il tetto sopra il garage e un muro laterale dell'abitazione presentano una temperatura più elevata delle altre parti, gli agenti ottengono un mandato di perquisizione, arrivando alla scoperta di una coltivazione di circa cento piante. La corte d'appello, investita del gravame, esclude una legittima aspettativa alla *privacy* in capo all'imputato, non avendo questi compiuto alcuno sforzo per nascondere il calore fuoriuscente dall'abitazione; inoltre, ad avviso dello stesso collegio, il *thermal imager* non è idoneo a rivelare alcun dettaglio intimo, bensì soltanto amorfe macchie di calore. Nel 2001 il caso approda davanti alla Corte Suprema, la quale, al contrario, afferma che l'utilizzo del *thermal imager* costituisce una perquisizione ai sensi del IV Emendamento e può, pertanto, avvenire solo in presenza di un mandato. Il una prospettiva che parte dal passato ma guarda al futuro, «il portato di tale operazione esegetica è il principio generale secondo cui, ogni qual volta l'autorità sfrutti dispositivi tecnologici di uso non comune al fine di scoprire dettagli su un'abitazione non altrimenti ottenibili se non mediante un'intrusione fisica nei

[65] *Kyllo v. United States*, 533 *U.S.* 27 (2001). Cfr., in proposito, M. MIRAGLIA, *Garanzie costituzionali nel processo penale statunitense. Tendenze e riflessioni*, Torino, 2008.

[66] Il *thermal imager* è uno strumento che rileva il calore emanato da ogni oggetto sotto forma di radiazioni infrarosse, non percepibili a occhio nudo. Il dispositivo traduce le radiazioni captate in immagini a colori, dove le diverse tonalità cromatiche indicano appunto le differenze di temperatura tra le varie parti dell'oggetto o rispetto agli oggetti circostanti.

predetti luoghi, allora tale forma di sorveglianza costituisce un'attività qualificabile come *search* e si deve presumere "irragionevole" se effettuata in assenza di un mandato»[67].

La pronuncia della Corte Suprema nel caso *Kyllo* costituisce una pietra miliare nel processo interpretativo del IV Emendamento: se il caso *Katz* ha comportato il superamento della tradizionale definizione di *search*, imperniata su una logica proprietaria, il caso *Kyllo* compie un passo in avanti verso l'adattamento dell'esegesi del precetto costituzionale alle nuove forme di aggressione alla *privacy* prodotte dall'evoluzione tecnologica. La dottrina più autorevole[68] ha osservato come, in armonia con il caso *Katz*, la Corte Suprema abbia inteso, nel caso *Kyllo*, ribadire che ciò che rileva ai fini dell'operatività del IV Emendamento non è l'intrusione in senso fisico entro un'area costituzionalmente protetta, ma la violazione di una legittima aspettativa di *privacy*; si può inoltre cogliere, nella vicenda da ultimo esaminata, la volontà della Corte di prendere posizione, *hic et nunc*, contro la crescente invasività delle nuove tecnologie, senza attendere lo sviluppo di strumenti più sofisticati e insidiosi del *thermal imager*. Infine, si segnala la capacità del *decisum* relativo al caso *Kyllo* di superare gli *escamotages* esegetici elaborati dalla giurisprudenza per sminuire la protezione della *privacy* accordata con il caso *Katz*. In merito a questo profilo, va dato rilievo alla circostanza per la quale, mentre la *Katz progenity* avrebbe ricostruito il paradigma delle attività qualificabili come *search* valorizzando soltanto il metodo impiegato per la ricerca – vale a dire, la presenza di un'intrusione fisicamente apprezzabile – la pronuncia *Kyllo* parrebbe focalizzare l'attenzione sul tipo di attività o di informazione che costituisce l'oggetto dell'attività di sorveglianza. Di conseguenza, il *discrimen* tra attività investigative riconducibili o meno alla nozione di *search* andrebbe individuato non tanto nel grado di intrusione fisica, quanto piuttosto nei risultati conseguiti, cioè nel carattere riservato dell'informazione acquisita.

Un'altra tecnologia particolarmente intrusiva nella vita privata delle persone è rappresentata dalle telecamere di sorveglianza, sempre più utilizzate dagli inquirenti sia nei luoghi di privata dimora sia negli spazi pubblici, tanto nel corso del procedimento penale quanto fuori. Ancora una volta, l'ordinamento statunitense si segnala per la sua propensione pionieristica, che lo ha portato ad affrontare il problema della disciplina processuale applicabile alle "riprese visive" già a partire dagli anni Ottanta. Limitando il discorso alle

[67] G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 114.

[68] W. LAFAVE, *op. cit.*, p. 494 ss.

videoriprese investigative eseguite in luoghi di privata dimora[69], va sottolineato come la presenza di un vuoto normativo non abbia affatto comportato l'inutilizzabilità dei dati conoscitivi acquisiti mediante questa tecnica investigativa, ma la giurisprudenza federale si sia piuttosto espressa nel senso dell'ammissibilità di siffatta prova atipica, estendendo la *warrant procedure* prevista dal *Title III* per le intercettazioni alla *silent video surveillance* effettuata in ambito domiciliare[70]: in ragione di ciò, la polizia giudiziaria dovrà sempre munirsi di un'autorizzazione giurisdizionale, legittimamente conseguibile in presenza di determinati requisiti specifici.

Le argomentazioni che hanno condotto all'applicazione del regime normativo del *Title III* possono essere desunte da un esame sommario del *leading case Torres del 1984*. La vicenda trae origine da una presunta violazione delle norme in materia di armi ed esplosivi, che aveva portato gli inquirenti a domandare e ottenere l'autorizzazione all'installazione di microfoni e telecamere equipaggiate per la trasmissione a distanza nel rifugio dell'organizzazione, in cui operavano i quattro imputati: la *television surveillance* così disposta consentì di filmare alcuni degli appartenenti alla banda mentre in silenzio assemblavano bombe. Proprio l'utilizzabilità di questi risultati costituì questione controversa durante il giudizio di primo grado, all'esito del quale il *trial judge* affermò che le videoregistrazioni non erano ammissibili come prova ai fini del giudizio, in quanto non esisteva alcuna norma che attribuisse al giudice federale il potere di autorizzare l'esecuzione di riprese visive in luoghi di privata dimora. Gli argomenti del giudice di prime cure e della difesa non convinsero però i giudici d'appello, i quali pervennero ad un verdetto opposto. Secondo la corte d'appello, infatti, il ricorso alle videoriprese di condotte non comunicative all'interno di luoghi di privata dimora, per quanto non sempre legittimo, non è di per sé incostituzionale, risultando tale tecnica investigativa ammissibile allorché vengano rispettate alcune garanzie minime, desumibili dal IV Emendamento e dalla disciplina del *Title III*. In particolare, la corte individua nel principio di proporzionalità il punto cruciale della questione relativa alla compatibilità delle riprese visive intradomiciliari con le garanzie

[69] L'espressione si riferisce a una tecnica investigativa specifica, ossia all'uso di telecamere da parte degli inquirenti al fine di captare immagini attestanti l'attività, spostamenti, relazioni personali o altre notizie relative ai soggetti spiati con l'occhio elettronico. Solitamente tale forma di sorveglianza è effettuata in modo occulto e si protrae nel tempo; può essere fissa o mobile e spesso implica l'installazione dello strumento di ripresa nel medesimo luogo in cui sono situate le persone messe sotto controllo.

[70] L'assimilazione sotto il profilo delle garanzie procedimentali tra captazione occulta di immagini e apprensione clandestina del contenuto di comunicazioni altrui è stata affermata per la prima volta dalla corte d'appello del settimo circuito con il caso *United States v. Torres* del 1984 ed è stata successivamente ribadita dalle corti d'appello degli altri *circuits*.

costituzionali. In ragione dei diversi gradi di invasività che possiedono le attività qualificabili come *search*, non si può in astratto escludere un divieto di utilizzazione della *television surveillance* nei procedimenti per reati di minore gravità, al fine di addivenire ad un corretto bilanciamento tra esigenze pubbliche e interessi individuali. In definitiva, la sola via per valutare la ragionevolezza o meno dell'intrusione consiste nell'eseguire un bilanciamento tra *the need to search* e il grado d'invasione che essa comporta nella sfera individuale. La vicenda processuale in esame costituisce un esempio di ragionevole impiego della *television surveillance*. In merito alle ragioni che hanno indotto a estendere la procedura autorizzativa prevista dal *Title III* per le intercettazioni alle riprese visive di comportamenti non comunicativi, rileva la forte analogia tra i due strumenti investigativi sotto il profilo della capacità intrusiva e del carattere non selettivo, nonché della necessità di un'interpretazione adeguatrice del precetto costituzionale che tenga conto del nuovo contesto storico-sociale in cui si trova ad operare. Si segnala, infine, il monito al fine dell'elaborazione di una più precisa disciplina, rivolto dalla giurisprudenza al legislatore e rimasto ad oggi lettera morta, in quanto, a distanza di oltre vent'anni, non risulta che il Congresso sia intervenuto per colmare il vuoto normativo.

Altro discorso è quello della videosorveglianza negli spazi pubblici o esposti al pubblico. Mentre per la captazione di immagini in ambito domiciliare la giurisprudenza ha svolto, come si è visto, un ruolo di supplente, rispetto a questo tema l'atteggiamento dei giudici si è improntato al principio del *laissez-faire,* a prescindere dalla forma del monitoraggio, fissa o mobile[71]. Così, in relazione alla *covert surveillance*, varie corti di merito hanno negato che sia qualificabile come *search* l'esecuzione di fotografie o riprese video al fine di acquisire elementi conoscitivi riguardanti incontri avvenuti sulla pubblica via oppure in aree esposte al pubblico[72], mentre analoghe considerazioni sono state svolte a proposito della *mass videosurveillance,* cioè della videosorveglianza di determinate aree

[71] In merito alla distinzione tra monitoraggio fisso e mobile, cfr. W. LAFAVE, *op. cit.*, p. 776. Secondo tale ricostruzione, la sorveglianza mobile è impiegata al fine di verificare se la persona indagata è coinvolta in attività criminose: solitamente è mirata su un soggetto specifico, individuato a priori, e comporta il pedinamento e l'impiego di macchine fotografiche e/o telecamere per documentare quanto osservato dagli investigatori. La sorveglianza fissa, invece, riguarda ambienti specifici, i quali vengono messi sotto controllo per acquisire la prova di attività criminose in essi realizzate: si possono fare gli esempi delle video-riprese eseguite all'esterno di un edificio per immortalare tutti coloro che vi entrano e/o escono, ovvero della videosorveglianza realizzata mediante l'installazione di telecamere a circuito chiuso (CCTV).

[72] Si veda soprattutto W. LAFAVE, *op. cit.*, p. 779; M. J. BLITZ, *Video surveillance and the constitutional public space: fitting the fourth Amendment to a world that tracks image and identify*, in 82, *Texas Law Review*, p. 1378; C. SLOBOGIN, *Public privacy: camera surveillance of public spaces*, cit., p. 236.

cittadine per finalità di prevenzione, repressione e accertamento dei reati[73]. Ciò dimostra chiaramente come né il legislatore né le corti statunitensi siano inclini a porre limitazioni sull'operato della polizia giudiziaria con riguardo all'esecuzione di riprese video in contesti pubblici[74]. Per quanto larga parte della dottrina e della giurisprudenza[75] abbia sostenuto l'estraneità dalla sfera di applicazione dei c.d. *Fourth Amendments requirements* di qualunque forma di monitoraggio elettronico di attività svolte in pubblico, quest'impostazione non è condivisa da tutti. Secondo alcuni, infatti, «la "centralità" della tecnologia nella società moderna ha avuto forti ricadute anche sull'architettura dello spazio pubblico, ponendo problemi di fronte ai quali le "vecchie" categorie concettuali appaiono improponibili»[76]. Questa prospettiva «muove dal presupposto che la diffusione capillare di telecamere nelle aree urbane abbia trasformato lo spazio pubblico in una sorta di "conduttore" che reca traccia di buona parte degli spostamenti e delle attività individuali»[77], circostanza per la quale si pone la necessità di un nuovo modo di impostare la questione. In una società aperta e democratica pare difficile accettare un impiego massivo e deregolamentato del monitoraggio compiuto attraverso telecamere e/o *tracking devices*, il quale rappresenterebbe l'equivalente di migliaia di poliziotti intenti a spiare le persone in ogni singolo attimo della vita quotidiana: effettivo o potenziale che sia, il monitoraggio generalizzato e continuo degli individui esercita infatti sulla psiche umana una sottile forma di coercizione, incidente in modo negativo sui *privacy interests* e sulle libertà fondamentali[78]. Come icasticamente raffigurato già dal *Panopticon* benthamiano[79] e, in

[73] Il riferimento è all'impiego, principalmente in chiave preventiva, di impianti di videosorveglianza a circuito chiuso per monitorare aree pubbliche o aperte al pubblico come strade, edifici, sistemi pubblici di trasporto urbano considerati a rischio di criminalità. In argomento v. BLITZ, *op. cit.*, p. 1357, p. 1381; C. SLOBOGIN, *Public privacy: camera surveillance of public spaces*, cit., p. 236.

[74] L'atteggiamento "permissivo" riscontrabile tanto nel formante legale quanto nel *case law* è ascrivibile essenzialmente alla difficoltà di immaginare che si possano presentare *privacy rights* in ambito pubblico: in questo senso: C. SLOBOGIN, *Public privacy: camera surveillance of public spaces*, cit., 217.

[75] Si veda, su tutti, il caso *Knotts*, in cui la Corte Suprema si è confrontata con il problema della compatibilità con il IV Emendamento dell'impiego di *beepers* elettronici per seguire gli spostamenti di un'automobile, statuendo che, quando una persona viaggia in auto sulla pubblica via non ha una *reasonable expectation of privacy* relativamente ai suoi spostamenti da un posto ad un altro.

[76] G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 145-146.

[77] *Ibidem*, p. 146.

[78] G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 146.

[79] J. BENTHAM, *Panopticon – Ovvero la casa di ispezione*, Venezia, III ed., 2002.

chiave moderna, da Foucault[80], anche alla sorveglianza effettuata mediante l'occhio elettronico conseguono quella perdita di spontaneità e la sensazione di inquietudine derivanti dall'impressione di essere fissati.

Quanto alla base giuridica per la costruzione di una disciplina costituzionalmente orientata delle riprese visive, la migliore dottrina[81] tende ad individuarla nel c.d. *right to public anonimity*. Se i "vecchi diritti" appaiono ormai inadatti a proteggere la persona dalle aggressioni tecnologiche, il mondo giuridico risponde alla modernità attraverso la creazione di "nuovi diritti". Secondo l'elaborazione più risalente, *the public anonimity* corrisponderebbe ad una delle quattro dimensioni della *privacy – solitude, intimacy, anonimity, repose* – e, segnatamente, consisterebbe nella condizione «che si realizza quando l'individuo è in un luogo pubblico o compie azioni pubbliche ma cerca, ed ottiene, di sfuggire all'identificazione e al controllo (*omissis*) egli è tra la gente e sa di essere osservato; ma salvo che non sia una celebrità, non si aspetta di essere identificato e di dover rispettare quelle regole di comportamento e quel ruolo che osserverebbe se fosse riconosciuto dalle persone che lo stanno osservando. In questa condizione egli può confondersi nel *situational landscape*»[82]. In punto di ricadute di tale "nuovo diritto" su tecniche investigative come la videosorveglianza, il riconoscimento di una simile posizione giuridica viene fatto dipendere dal *balancing test*, cosicché, come già per i "vecchi diritti", si ammette che anche il diritto all'anonimato possa soccombere, purché nel rispetto di alcune garanzie procedurali prestabilite dalla legge. Superfluo sottolineare come proprio quella legislativa sia la sede in cui dovrebbe compiersi questa delicata operazione di bilanciamento, trattandosi di scelte di natura squisitamente politica.

L'ossessione tecnologica emersa nel "secolo breve" per il proliferare di sistemi di controllo a distanza si apprezza non soltanto sul piano della sorveglianza statica convenzionale – la videosorveglianza o altri sistemi di acquisizione di immagini – ma anche su quello della c.d. sorveglianza dinamica, la quale è in grado di rilevare in tempo reale gli spostamenti di persone o cose, nonché la loro ubicazione. Accanto al "pedinamento", che costituisce la modalità operativa tradizionale con la quale la polizia giudiziaria esegue il

[80] M. FOUCAULT, *Sorvegliare e punire*, Torino, 2005.

[81] L'analisi volta a ricostruire il fondamento costituzionale del diritto all'anonimato è di S. SLOBOGIN, *Public privacy: camera surveillance of public spaces,* cit., p. 237-286.

[82] Cfr. A. F. WESTIN, *Privacy and freedom,* London, 1967, p. 31, cit. da S. SLOBOGIN, *Public privacy: camera surveillance of public spaces,* cit., p. 239.

tracciamento dei movimenti di un soggetto rilevanti per il procedimento penale, negli ultimi anni sono stati sviluppati sistemi di localizzazione a distanza, di persone o cose, che possono essere agevolmente impiegati a fini investigativi[83]: si parla, a tale proposito, di "pedinamento elettronico", a voler rimarcare l'intreccio tra la funzione originaria, rimasta inalterata, e le nuove modalità esecutive, ad alto contenuto tecnologico. Senonché, anche in questo caso il contributo offerto dalle nuove tecnologie non presenta una valenza soltanto semantica, avendo piuttosto determinato un salto di qualità del monitoraggio, implementandone l'efficacia. Come accaduto per la captazione di immagini in ambiti pubblici o aperti al pubblico, anche la diffusione degli strumenti che consentono un controllo sistematico degli spostamenti delle persone ha acceso un vivace dibattito in seno al mondo giuridico statunitense, ponendo l'interrogativo se sia coerente con una società aperta e democratica lasciare sprovvisti di disciplina i dispositivi di tracciamento in questione. A ben vedere, infatti, essi integrano una modalità investigativa autonoma e ontologicamente differente dal pedinamento, che richiede l'assistenza di un livello minimo di garanzie. Come riconosciuto anche nel caso *United States v. Bobinsky*, il monitoraggio di un *beeper* elettronico va ben oltre le normali capacità di osservazione dell'uomo medio, in quanto permette la realizzazione di una sorveglianza più estesa e minuziosa, altrimenti non possibile[84]. Così, ancora una volta, il dibattito si è polarizzato su due estremi opposti, rappresentanti da un fronte "conservatore", poco incline a porre restrizioni alla polizia giudiziaria in relazione al pedinamento realizzato con *beepers* elettronici o tramite GPS, e, dall'altro lato, un fronte "innovatore", più propenso a richiedere sempre per tali forme di sorveglianza elettronica l'emissione di un *court order*, idoneo ad assicurare il vaglio di un giudice terzo e imparziale.

Le considerazioni sin qui svolte consentono di trarre alcune conclusioni. Anzitutto, l'evoluzione, alla quale si è assistito nell'ordinamento statunitense, dal concetto di *privacy* a quella attuale di *privacy-dignity* riflette un processo giuridico-sociale caratterizzato dal passaggio da una gerarchia di valori dominata dagli interessi proprietari ad un'altra imperniata sul riconoscimento e la preminenza della persona umana. Tale rinnovata concezione ha inciso in maniera preponderante sulla ricostruzione del IV Emendamento, norma chiave in tema di rapporti fra libertà del singolo e intervento dei pubblici poteri,

[83] A titolo esemplificativo, si possono menzionare i *beepers* elettronici, i sistemi di rilevamento satellitare come il GPS, nonché il sistema di localizzazione per celle su cui si basa la telefonia mobile.

[84] Così W. LAFAVE, *op. cit.*, p. 762, che richiama *United States v. Bobinsky*, 415 F. supp. 1334 (D. Mass. 1976). Per analoghe considerazioni cfr. J. TOMKOVICZ, *op. cit.*, p. 364 e 371.

espandendo l'ambito di protezione da essa garantito al punto che il rilievo di un *physical trespass* cede il passo al criterio della *reasonable expectation of privacy*. Di conseguenza, se la libertà personale non può più essere identificata con la pura libertà da intromissioni di carattere fisico ma traguarda la libertà di autodeterminazione, il IV Emendamento non è posto solo a tutela dell'*habeas corpus* ma anche e soprattutto dell'*habeas mentem*[85].

Ad onta di ciò, l'ordinamento nordamericano ha omesso di approntare un elevato livello di protezione delle libertà fondamentali a fronte della crescente pervasività delle recenti tecnologie di controllo. Più in particolare, le linee di tendenza emerse nel periodo successivo alla *Katz decision* possono sintetizzarsi secondo due direttrici. In primo luogo, come emerge dal caso *Kyllo*, il regime di garanzia accordato dal IV Emendamento deve scattare anche se il controllo viene effettuato fuori dal domicilio in senso stretto e l'ausilio tecnologico permette di prendere conoscenza di frammenti di vita che si svolgono al suo interno, ma, laddove venga in rilievo la c.d. *silent video surveillance* – ossia la ripresa visiva di condotte non comunicative –, non opera, in difetto di una specifica disciplina legislativa, l'intero regime di garanzia di cui al *Title III* ma solo la *warrant procedure* ex § 2158 *U.S.C.*: il risultato è, in questo modo, che ad uno strumento investigativo più insidioso e lesivo della dignità delle persone corrisponde un livello di tutela più tenue di quello previsto per aggressioni di minore intensità. La seconda linea di tendenza attiene alla sorveglianza elettronica realizzata in spazi pubblici o aperti al pubblico. A tal proposito, emerge come, pur a fronte di una rinnovata concezione di *privacy*, giurisprudenza e legislazione federale non siano inclini a ricondurre le nuove tecniche investigative all'alveo del IV Emendamento, in quanto si ritiene che le persone, nel momento in cui scelgono liberamente di esporsi al pubblico, abdichino alla propria *privacy*.

A fronte della pervasività delle nuove tecnologie del controllo, «l'atteggiamento più opportuno non è vietarne *tout court* l'uso, ma neppure lasciarle nel limbo dell'indifferenza giuridica»[86], trattandosi piuttosto di individuare un equo bilanciamento tra i contrapposti interessi in gioco, se non si vuole che lo "svuotamento" dei diritti fondamentali avvenga direttamente dal loro interno. Deve quindi salutarsi con favore l'emergere di un *right to public anonimity*, che, dietro all'immobilismo dell'approccio tradizionale, impone di reimpostare il problema anzitutto a livello costituzionale e postula la necessità di una

[85] Così A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974, p. 397 ss e 468.

[86] G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 175.

disciplina legislativa "costituzionalmente orientata" delle varie forme di sorveglianza tecnologicamente assistita. In prospettiva *de iure condendo*, la prima operazione da compiere pare quindi essere quella di una ricognizione di tutti i dispositivi tecnologici che possono contribuire a creare una sorta di *panopticon effect*, per scegliere quali consentire e quali vietare; una volta compiuto questo passo, si tratterà di regolamentare in maniera puntuale le varie tecnologie della sorveglianza non bandite, a partire dall'individuazione dei presupposti legittimanti (c.d. *justification requirements*)[87].

4. *Obsolescenza della prova dichiarativa: le indagini preliminari da "fase che non pesa e che non conta" a "gigantesca istruzione sommaria"*

Dopo avere ripercorso, anzitutto in chiave comparatistica, gli snodi più significativi del progresso tecnologico, si tratta ora di verificare come, in concreto, i nuovi ritrovati della tecnica abbiano inciso sulla dinamica processuale, modificandone la fisionomia. A questo riguardo, è opportuno ricostruire, in prospettiva diacronica, l'evoluzione delle indagini preliminari nella nostra esperienza giuridica, per constatare il ruolo ormai predominante che esse hanno assunto ai fini dell'esito del giudizio.

Nell'impianto originario del codice Vassalli, le indagini preliminari erano concepite come una «fase che non conta e che non pesa», per dirla con Nobili[88]. In particolare, il pubblico ministero era il *dominus* incontrastato di questo segmento procedimentale, strutturato alla stregua di un'indagine interna al suo ufficio. Si trattava di una fase non giurisdizionale e caratterizzata dall'unilateralità, dalla tendenziale incompletezza, dalla deformalizzazione e dalla durata circoscritta. Secondo Nobili, proprio la limitata finalizzazione delle indagini preliminari costituiva uno dei punti salienti della riforma. A conferma che le attività investigative non avevano un connotato di completezza era la

[87] Si veda, in proposito, G. DI PAOLO, *Tecnologie del controllo e prova penale*, cit., p. 176-177. Secondo l'Autrice, si dovrebbe avere riguardo ai seguenti elementi: la titolarità del potere dispositivo, il catalogo dei reati per cui sono consentite, lo *standard* probatorio necessario, il contenuto del provvedimento autorizzativo, il tipo di *law enforcement objective* perseguito, le modalità esecutive della sorveglianza elettronica, gli avvisi *post-surveillance*, le modalità di conservazione e divulgazione delle risultanze investigative e dei rimedi posti a presidio della legalità del procedere.

[88] M. NOBILI, *Diritti per la fase che "non conta e non pesa"*, in *Scenari e trasformazioni del processo penale*, Padova, 1998, p. 35 ss.

circostanza che l'attività di indagine non si concludeva con la richiesta di rinvio a giudizio, ma si consentiva al pubblico ministero di svolgere un'indagine suppletiva, ai sensi dell'art. 419, c. 3 c.p.p., tra l'esercizio dell'azione penale e l'udienza preliminare, e poi un'indagine integrativa, ai sensi dell'art. 430 c.p.p., dopo il rinvio a giudizio. L'idea di fondo era, in altri termini, quella di superare l'idea del giudice istruttore e assicurare la corrispondenza tra atti d'indagine e prove. Questo modello di indagini "leggere" entra in crisi negli anni Novanta a seguito della c.d. "svolta inquisitoria" e della conseguente caduta della barriera tra indagini e giudizio. In questo modo, l'assunzione di informazioni dalla persona informata sui fatti comincia a pesare come nel caso delle dichiarazioni rese durante l'esame testimoniale, compiendosi, sul piano delle garanzie dell'indagato, un passo indietro. Nel 1991 la Corte costituzionale[89], sulla scorta di alcune disposizioni del codice, enuncia il principio della tendenziale completezza delle indagini, il quale assolve, nella struttura del nuovo processo, una duplice e fondamentale funzione: la completa individuazione dei mezzi di prova è necessaria, da un lato, per consentire al pubblico ministero di esercitare le varie opzioni possibili e indurre l'imputato ad accettare i riti alternativi, mentre, dall'altro lato, funge da argine contro eventuali prassi di esercizio "apparente" dell'azione penale, destinate a risolversi in un ingiustificato aggravio del carico dibattimentale.

Si possono menzionare diverse ragioni che stanno a fondamento di questo cambio di paradigma. Oltre alla ricordata "svolta inquisitoria" e al principio di tendenziale completezza delle indagini, svolgono un ruolo cruciale l'introduzione delle investigazioni difensive, figlia del principio di parità delle parti, e la diffusione della prova scientifica e tecnologica. L'ultimo aspetto appare decisivo. Il progresso scientifico e tecnologico rende centrale nella ricostruzione dei fatti del passato, più che i segni lasciati dal fatto di reato sulle persone e colti attraverso i sensi, quelli lasciati sulle cose (tracce di DNA, impronte, messaggi, passaggi davanti a telecamere) e rievocati attraverso la tecnologia: prove tecnologiche vengono così assunte durante le indagini preliminari attraverso gli atti di indagine (analisi della scena del crimine, accertamenti tecnici) o i mezzi di ricerca della prova (intercettazioni di conversazioni, sequestro del telefonino, mezzi atipici). Si approda, quindi, a quella concezione delle indagini preliminari che Ferrua ha icasticamente definito una «gigantesca istruzione sommaria». Esse vengono ibridandosi e assumono progressivamente una funzione "preparatoria" del processo, per molti aspetti simile a quella che caratterizzava la fase istruttoria del previgente codice di rito: dall'indagine che prepara unicamente all'azione si

[89] Corte cost. 15 febbraio 1991, n. 88.

passa ad un'indagine completa che prepara il processo. Alcuni interventi legislativi emblematizzano questa evoluzione. Per un verso, l'introduzione dell'art. 415-bis c.p.p., che porta alla previsione di una *discovery* degli atti di indagine prima dell'esercizio dell'azione penale, viene ad assicurare una fase di contraddittorio tra indagato e pubblico ministero in ordine alla completezza delle indagini; per altro verso, l'introduzione dell'art. 421-bis, sempre ad opera della stessa legge Carotti[90], riconosce al g.u.p. il potere di disporre un'integrazione in caso di indagini incomplete e laddove il materiale cognitivo eventualmente acquisito *ex post* non sia idoneo a eliminare le lacune. Sebbene alcuni Autori abbiano invocato una "resurrezione del vecchio", la Corte costituzionale[91] ha chiarito come «l'esigenza di completezza delle indagini preliminari è ora significativamente valutabile anche in sede di udienza preliminare», essendo al giudice attribuito il potere di disporre l'integrazione delle indagini stesse *ex* art. 421-bis c.p.p.

Il vero punto di svolta, tuttavia, è rappresentato dalla riforma del giudizio di abbreviato, che viene trasformato da giudizio subordinato al necessario consenso di entrambe le parti (c.d. patteggiamento sul rito) a diritto dell'imputato: a partire dalla legge Carotti, infatti, il pubblico ministero deve tenere conto, nello svolgere le indagini preliminari, che, sulla base degli elementi raccolti, l'imputato può chiedere ed ottenere di essere giudicato con tale rito, non potendo quindi esimersi dal predisporre un esaustivo quadro probatorio in vista dell'esercizio dell'azione penale. La stessa Corte costituzionale[92], nel 2001, afferma che «l'esigenza di completezza delle indagini preliminari (*omissis*) risulta rafforzata dal riconoscimento del diritto dell'imputato ad essere giudicato, ove ne faccia richiesta, con il rito abbreviato». In conseguenza di ciò, quello che si richiede è la presenza di una piattaforma cognitiva il più possibile esaustiva e idonea a giudicare l'imputato "allo stato degli atti". Il precipitato di tutte queste innovazioni è la polifunzionalità delle indagini preliminari, tale per cui gli elementi di prova raccolti possono essere impiegati a diversi scopi: decidere se chiedere il rinvio a giudizio o l'archiviazione, fondare alcune richieste fatte al g.i.p., vagliare la fondatezza dell'accusa.

La centralità del dibattimento come luogo deputato alla formazione della prova è oggi in aperta crisi. L'evoluzione della fisionomia delle indagini preliminari ha forse costituito la

[90] L. 16 dicembre 1999, n. 479.

[91] Corte cost. 6 luglio 2001, n. 224.

[92] Corte cost. 9 maggio 2001, n. 115.

premessa di questa trasfigurazione del processo, ma, per avere un quadro più completo, è necessaria qualche considerazione ulteriore. Anzitutto, appare opportuna la preliminare disamina di una disposizione costituzionale che disciplina lo "statuto epistemologico" della prova penale. L'art. 111 Cost., dopo avere affermato al c. 2 che «ogni processo si svolge nel contraddittorio tra le parti», statuisce al c. 4 che «il processo penale è regolato dal principio del contraddittorio nella formazione della prova». Da queste norme emerge la convinzione secondo la quale il contraddittorio è il metodo migliore di ricostruzione della verità; tuttavia, come è stato efficacemente messo in luce da Siracusano, il vero salto qualitativo si compie quando dal contraddittorio retorico-argomentativo si passa al contraddittorio "poietico", ovvero quando si passa dal contraddittorio sulla prova (c. 2) al contraddittorio per la prova (c. 4). Questa scelta esprime una precisa opzione assiologica, sintetizzabile con le parole di Giostra: «viene abbandonato l'orientamento epistemologico che, presumendo neutro il momento dell'acquisizione delle conoscenze, riserva coerentemente l'intervento dialettico alla loro valutazione, per abbracciarne un altro che, invece, ritiene utili per ben decidere soltanto le conoscenze scaturite dal confronto dialettico»[93]. In altri termini, la realizzazione del contraddittorio denota un processo penale assiologicamente orientato, cioè una concezione della giustizia in cui il metodo di accertamento della verità rappresenta di per sé un valore, considerato che, come già si era intuito, «la giustizia della sentenza sta nel cammino seguito pel risultato»[94]. Appare emblematico che il principio del contraddittorio in senso "forte" sia stato codificato proprio all'indomani della c.d. "svolta inquisitoria", quando la Corte costituzionale, con un trittico di sentenze[95], enuclea il principio di non dispersione della prova: in risposta alla magistratura, il legislatore adotta una legge costituzionale[96] che riscrive, di fatto, l'art. 111 Cost. in senso maggiormente garantistico.

Se un tanto è vero, quella dichiarativa si presenta come la prova più coerente con il principio del contraddittorio, che trova attuazione nell'assunzione della prova stessa attraverso il meccanismo della *cross examination*. Senonché, questo assetto, oltre ad essere derogato in una serie di casi previsti per via legislativa, si pone in maniera stridente con la *law in action*, ovvero con il concreto modo di essere del processo oggi. In effetti, la natura

[93] G. GIOSTRA, *Prima lezione sulla giustizia penale*, Bari, 2020, p. 45.

[94] T. ASCARELLI, *Processo e democrazia*, in *Riv. trim. dir. proc.*, 1958, p. 858.

[95] Si tratta delle sentenze del 1992 n. 24, 254 e 255.

[96] L. cost. 23 novembre 1999, n. 2

tendenzialmente irripetibile dei controlli, resi possibili dal progresso della tecnica, finisce per consentire l'acquisizione di vere e proprie prove utilizzabili in giudizio, sebbene, sul piano teorico, una simile soluzione non potrebbe trovare spazio all'interno di un sistema ad ispirazione accusatoria come il nostro[97]. In altri termini, il *punctum dolens* della questione risiede nel fatto che i controlli *de quibus* postulano l'acquisizione di elementi idonei ad integrare la piattaforma probatoria su cui dovrà basarsi la decisione del giudice in ordine alla responsabilità dell'imputato. Questa attitudine si pone in contrasto anche con la regola generale di impermeabilità tra le distinte fasi del procedimento, ponendo in discussione l'esistenza di una rigida separazione tra indagini preliminari e dibattimento ed esaltando, al contempo, i caratteri di strumentalità delle prime rispetto al secondo. Per quanto le ambasce inerenti ad una simile fisionomia del procedimento penale possano essere attenuate valorizzando il ruolo meramente propulsivo delle ricerche rispetto al proficuo sviluppo delle indagini, esse confermano la ormai innegabile obsolescenza della prova dichiarativa, rimpiazzata dai più affidabili contributi cognitivi offerti dall'evoluzione tecnologica, i quali si sottraggono però al principio del contraddittorio.

Questa circostanza non è priva di effetti. Il pubblico ministero si ritrova infatti ad affrontare l'alternativa tra formulazione dell'accusa e archiviazione della notizia di reato basandosi, essenzialmente, su materiale investigativo che egli stesso ha raccolto: ciò pone la necessità di arginare gli effetti di quella legge psicologica in base alla quale «il pubblico ministero formula ipotesi per cercare la verità, ma, sovente, finisce per cercare la verità delle proprie ipotesi»[98]. Come osservato in dottrina[99], pur non essendo «un grimaldello per aprire i segreti della realtà», la dialettica riveste, da questo punto di vista, un ruolo cruciale, in ragione della sua funzione di naturale «antidoto alla pigrizia dell'intelletto» e della sua attitudine a «predispo[rre] a cercare l'altro lato di ogni questione». In altri termini, il confronto con soggetti portatori di istanze autonome ed eterogenee risulta decisivo per le determinazioni del pubblico ministero in ordine all'esercizio dell'azione penale, in quanto idoneo a mandare in crisi un assunto in origine considerato sicuro. Pertanto, se nella dialettica si trova il punto di equilibrio tra "ragioni dell'accusa" e "ragioni della difesa", pare

[97] Si veda, in questo senso, F. NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, Milano, 2020, pp. 124 e 125.

[98] S. CIAMPI, *La riforma delle intercettazioni e le sue ricadute sulla conclusione delle indagini preliminari*, in *Arch. pen. 2020, n. 2*., p. 3.

[99] F. CORDERO, *Gli osservanti. Fenomenologia delle norme*, Milano, 1967, p. 327.

senz'altro opportuno che «il sistema garantisca un confronto effettivo tra pubblico ministero e persona sottoposta alle indagini preliminari, quantomeno nei momenti che immediatamente precedono la decisione del magistrato circa l'esercizio dell'azione penale»[100].

Alla luce di questi rilievi, è possibile ravvisare nella fisionomia dell'avviso di conclusione delle indagini preliminari, «con i poliedrici risvolti che lo caratterizzano in termini di contestazione di una cripto-imputazione»[101], lo strumento per un recupero del contraddittorio. Il meccanismo forgiato nel 1999 assicura infatti che le determinazioni del pubblico ministero in merito all'esercizio dell'azione penale si formino tenendo conto del contributo documentale e dialettico del diretto interessato. Ciò che si determina in base all'istituto di cui all'art. 415-bis c.p.p. è la *discovery* dell'intero *dossier* investigativo e, soprattutto, l'apertura di una finestra di dialogo fra imputato *in fieri* e pubblico ministero, che può sfociare nell'eventuale pretesa dell'interessato di essere interrogato dal magistrato inquirente, piuttosto che nella richiesta di nuove indagini. È appena il caso di precisare che, sebbene l'operatività dell'avviso di conclusione delle indagini preliminari risponda a esigenze di buon funzionamento del sistema processuale, non pochi problemi si sono posti nella prassi, legati, in particolar modo, alla mole di elementi raccolti dal pubblico ministero.

Contestualmente alla notificazione dell'avviso *ex* art. 415-bis c.p.p., il legislatore ha altresì previsto la *discovery* delle intercettazioni telefoniche nei casi in cui non si sia dato luogo alla c.d. udienza stralcio[102]. Questa previsione costituisce «il *clou*»[103] della novella del 2020[104]: si tratta di una modifica d'impatto, in quanto istituzionalizza un *modus operandi* germogliato nel sottobosco della prassi, seguito quindi dalle procure della Repubblica e

[100] S. CIAMPI, *La riforma delle intercettazioni e le sue ricadute sulla conclusione delle indagini preliminari*, in *Arch. pen.*, 2020, p. 4.

[101] *Ibidem*.

[102] In base all'art. 415-bis, c. 2-bis c.p.p., «qualora non si sia proceduto ai sensi dell'articolo 268, commi 4, 5 e 6, l'avviso contiene inoltre l'avvertimento che l'indagato e il suo difensore hanno facoltà di esaminare per via telematica gli atti depositati relativi ad intercettazioni ed ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche e che hanno la facoltà di estrarre copia delle registrazioni o dei flussi indicati come rilevanti dal pubblico ministero (*omissis*)».

[103] F. CAPRIOLI, *La procedura di filtro delle comunicazioni rilevanti nella legge di riforma della disciplina delle intercettazioni*, in *Cass. pen.*, 2020, p. 1396.

[104] L. 28 febbraio 2020, n. 20.

regolamentato, da ultimo, con strumenti di *soft law*[105]. Per la prima volta dalla sua creazione, l'art. 415-bis c.p.p. viene così interpolato con un esplicito riferimento alla disciplina delle intercettazioni. In particolare, si prevede una *discovery* del materiale captato «incubata dalle più complesse dinamiche partecipative e di *disclosure* "a tutto tondo" che caratterizzano la notifica dell'avviso ex art. 415-bis c.p.p.»[106]. In questo modo, il legislatore ha inteso consacrare *ex lege* il connubio tra intercettazioni telefoniche e avviso di conclusione delle indagini preliminari, contribuendo a chiarificare la funzionalizzazione di questo istituto rispetto all'attuazione del principio del contraddittorio, così anticipato già al delicato momento della scelta circa l'esercizio dell'azione penale.

Si può quindi concludere, anche alla luce della riforma evocata, che la disciplina recata dall'art. 415-bis c.p.p. costituisce la «matrice di un vero e proprio micro-procedimento, di "una fase tra le fasi", caratterizzata da autonomia strutturale e funzionale»[107]: l'evoluzione dalla quale è stata interessata ne ha enfatizzato il ruolo, «segnando una progressiva erosione dell'iconografia dell'istituto quale semplice garanzia difensiva, a tutto vantaggio di una dimensione olistica, incentrata su un confronto articolato, sfaccettato, poliedrico tra pubblico ministero e persona sottoposta alle indagini preliminari, funzionale e prodromico all'assunzione, da parte del magistrato inquirente, di determinazioni la cui rilevanza è strategica per il seguito del procedimento»[108].

Nel denunciare il ritardo del nostro legislatore rispetto alla regolamentazione dei nuovi strumenti della tecnica, si è trattato della relatività dell'atipicità probatoria con riferimento all'art. 189 c.p.p.[109]. Questa disposizione pone, fra i requisiti per i mezzi atipici di prova, oltre all'idoneità rispetto all'accertamento e alla mancanza di pregiudizio per la libertà morale della persona, il previo contraddittorio davanti al giudice al quale è imposto il compito di regolare le specifiche modalità di assunzione della prova. I dubbi che l'hanno riguardata sono sorti proprio perché l'art. 189 c.p.p., pur collocato tra i princìpi generali della prova, appare difficilmente conciliabile con le caratteristiche dei mezzi di ricerca della

[105] In tema, più in generale, P. TONINI-F. CAVALLI, *Le intercettazioni nelle circolari delle procure della Repubblica*, in *Dir. pen. proc.*, 2017, 705.

[106] S. CIAMPI, *La riforma delle intercettazioni*, cit., p. 5-6.

[107] *Ibidem*, p. 6.

[108] *Ibidem*.

[109] Si veda cap. 1, sez. I, § 1, p. 9, 10.

prova, i quali, compiuti in segreto durante le indagini, sono incompatibili con un previo contraddittorio davanti al giudice. Il nodo è stato sciolto dalla giurisprudenza costituzionale e di legittimità, la quale ha affermato che il contraddittorio può essere operato nel momento in cui i risultati dei mezzi atipici di ricerca della prova vengono ammessi dal giudice, chiamato a valutare *ex post* la presenza dei requisiti previsti dall'art. 189 c.p.p.

Si è, tuttavia, palesato un ulteriore profilo di criticità, rappresentato dalla natura invasiva dei mezzi atipici di ricerca della prova rispetto alle libertà fondamentali. A fronte dell'inerzia del legislatore, la giurisprudenza, ancora una volta, si è fatta carico di tracciare le linee guida che permettono di valutare l'ammissibilità dei nuovi mezzi atipici di ricerca della prova. In base al principio di non sostituibilità, è necessario accertare, in primo luogo, se il mezzo atipico sia inquadrabile in un mezzo tipico di ricerca della prova e trovi in esso la sua regolamentazione: in altri termini, il mezzo atipico non deve eludere fraudolentemente le regole sostanziali previste per l'atto tipico[110]. Una volta appurata l'effettiva atipicità dello strumento, è necessaria un'ulteriore valutazione in ordine all'intensità di limitazione delle libertà fondamentali prodotta dall'attività atipica. A questo proposito, si distingue tra mezzi atipici di ricerca che non limitano diritti fondamentali e mezzi atipici di ricerca che limitano diritti fondamentali. Nella prima ipotesi, i mezzi atipici possono essere disposti direttamente dalla polizia giudiziaria, purché compiuti ai legittimi fini dell'accertamento penale. Più complessa la seconda ipotesi, che impone di distinguere a seconda che i diritti fondamentali oggetto di limitazione siano o meno protetti da riserva di legge: la giurisprudenza, in proposito, equipara l'ultimo caso a quello in cui, pur in presenza di una riserva di legge, il mezzo atipico non lede il nucleo essenziale del diritto, richiedendo l'autorizzazione motivata del pubblico ministero; invece, nel caso di un mezzo atipico che lede il nucleo essenziale di un diritto protetto dalla riserva di legge, la conseguenza, più radicale, è quella dell'inutilizzabilità.

[110] Per una più compiuta disamina del principio di non sostituibilità, si veda C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007.

Sezione II

LA CATEGORIA PROBATORIA DEI "CONTROLLI OCCULTI E CONTINUATIVI"

SOMMARIO: 1. Profili di una nuova sistematizzazione probatoria. – 2. Il metodo della proporzionalità nella disciplina dei controlli occulti. – 3. I controlli occulti e lo spazio giudiziario europeo.

1. *Profili di una nuova sistematizzazione probatoria*

Come si è visto, la sorveglianza incarna una delle più vive manifestazioni autoritative, anche in quanto dotata di una significativa attitudine "disciplinante" rispetto alle condotte sociali del soggetto passivo del controllo. Tuttavia, nella prospettiva dell'attuale scenario, profondamente innovato dall'irrompere del fattore tecnologico, è necessario interrogarsi in ordine alla tecnica da prediligere per la regolamentazione dei controlli occulti di ultima generazione (apparati di videosorveglianza, dispositivi di localizzazione G.P.S., *software* di accesso da remoto a sistemi informatici, *IMSI catcher*, …). In particolare, si pone il quesito se sia più opportuno disciplinare singolarmente la singola attività di sorveglianza attraverso una "codificazione" di dettaglio oppure seguire una tecnica differente. Per quanto possa apparire difficile tipizzare in maniera esaustiva i plurimi utilizzi di cui sono suscettibili gli strumenti di monitoraggio oggi diffusi, la dottrina ha, in maniera unanime, denunciato le improprie forzature dell'ambito di applicabilità delle previsioni esistenti alle quali rischiano di condurre le lacune, come nel caso del *virus* informatico[111]. Vi è, poi, un altro problema, rappresentato dal rischio di una normativa destinata a diventare ben presto obsoleta e incapace di tenere il passo dell'evoluzione tecnica: per quanto lungimirante, infatti, difficilmente il legislatore potrebbe prevedere ogni futura applicazione tecnologica facendo tempestivamente fronte alla verosimile comparsa in scena di nuove modalità di controllo. Non pare allora fuor di luogo riflettere sull'opportunità di un approccio alternativo, che si

[111] L'intervento additivo realizzato dal d.lgs. n. 216 del 2017 e dalle successive interpolazioni in relazione all'impiego del *virus* informatico quale strumento per le c.d. intercettazioni ambientali è stato oggetto di critiche da parte della dottrina, che ha segnalato come, omettendo di regolamentare alcuni utilizzi del mezzo in questione, si continui a relegare nell'area dell'atipicità operazioni diverse dall'intercettazione di dialoghi *inter praesentes*, ancorché non meno invasive: basti pensare alla copia della memoria statica del dispositivo infettato, ovvero al monitoraggio in tempo reale dell'attività non comunicativa compiuta dall'utilizzatore. Sul punto, tra gli altri, E. M. MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, in A. GIARDA-F. GIUNTA-G. VARRASO (a cura di), *Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura*, Padova, 2018, p. 193 ss; L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, in G. GIOSTRA – R. ORLANDI (a cura di), *Nuove norme in tema di intercettazioni: tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, 2018, p. 289 ss.

proponga di disciplinare le moderne ricerche anche prescindendo da una puntuale e analitica regolamentazione dei diversi controlli.

In base all'art. 8, § 2 CEDU, è esclusa ogni ingerenza di un'autorità pubblica nell'esercizio del diritto al rispetto della propria vita privata e familiare se non per espressa previsione di legge e, comunque, purché questa sia necessaria «alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale o alla protezione dei diritti e delle libertà altrui». Per quanto la giurisprudenza di Strasburgo escluda la violazione di questa norma in presenza di una base legale priva dell'analitica individuazione delle singole operazioni di controllo concretamente esperibili, «ciò che risulta imprescindibile ai fini del rispetto della riserva di legge di cui all'art. 8, § 2 CEDU è un'adeguata tipizzazione dei casi in cui l'interferenza può essere realizzata e dei soggetti contro cui può essere diretta, accompagnata da apposite garanzie volte a contenere il pregiudizio arrecato al diritto al rispetto della vita privata»[112]. La compatibilità con la riserva di legge di una regolamentazione che assuma come riferimento una categoria di attività accomunate da determinate caratteristiche trova conforto nelle disposizioni della Carta fondamentale, la quale sembra a sua volta accontentarsi dell'individuazione dei presupposti che giustificano la limitazione dei diritti da essa contemplati (i casi), nonché della specificazione dell'oggetto della sorveglianza e delle garanzie previste a tutela della prerogativa incisa (i modi), senza richiedere una precisazione degli strumenti materialmente impiegati ai fini dell'intrusione. Da questi rilievi pare potersi desumere un principio di "neutralità tecnica", postulante l'irrilevanza del mezzo concretamente impiegato ai fini del rispetto della riserva di legge. Pertanto, «in presenza di una base legale che ammette la deroga al diritto fondamentale delineandone presupposti, oggetto e prescrizioni esecutive, il principio in esame potrebbe dirsi soddisfatto a prescindere dall'analitica specificazione delle modalità del controllo»[113].

Si è visto come, grazie all'ausilio dei nuovi strumenti tecnici, le ricerche oggi esperibili siano dotate di una inedita potenzialità intrusiva, tale da qualificare in maniera singolarmente afflittiva la sorveglianza. Proprio l'attributo tecnologico possiede, quindi, un rilievo decisivo ai fini di una più precisa delimitazione del perimetro della categoria dei controlli occulti e continuativi. In ragione dell'ampiezza dei dati che è possibile acquisire per il tramite dei nuovi ritrovati della tecnica, si è proposto, in altre esperienze ordinamentali, di valutare

[112] F. NICOLICCHIA, *I controlli occulti e continuativi*, cit., p. 65.

[113] *Ibidem*, p. 69.

l'intrusività del controllo avendo riguardo, più che alla tipologia delle informazioni acquisite, proprio ai mezzi tecnici impiegati, secondo quello che è stato definito come un *technology-centered approach*[114]. Problemi non trascurabili si sono posti con riferimento al contesto spaziale di esecuzione delle ricerche: appurato che non è facile prevedere *ex ante* gli spazi in cui verrà materialmente effettuato il controllo alla luce della mobilità di molti degli strumenti di sorveglianza attualmente in uso, rileva il dato che i nuovi ambienti virtuali risultano sprovvisti di quelle tutele stabilite in favore del domicilio, sebbene nello spazio digitale sia possibile rinvenire una quantità di informazioni riservate assai maggiore rispetto a quelle conservate nella realtà fisica. Questa considerazione rafforza l'idea secondo la quale sarebbe opportuno prediligere un'interpretazione che parametri le garanzie assicurate dalla legge non già alla tipologia del dato suscettibile di essere captato, bensì all'invasività intrinseca della ricerca[115].

Focalizzando l'attenzione sull'invasività intrinseca dei controlli occulti, si osserva come «l'occultezza del controllo non deve essere intesa come inerente alla c.d. segretezza "interna" degli atti compiuti durante le indagini preliminari»[116], in quanto «il connotato in discussione intende piuttosto designare quelle operazioni caratterizzate da un *quid pluris* di clandestinità, che assurge a peculiarità fisiologica ed ineliminabile della ricerca»[117]. Si possono individuare almeno due tratti caratteristici inerenti a questo genere di controlli. In primo luogo, rileva la posizione di svantaggio del soggetto passivo della sorveglianza, che è completamente inconsapevole di costituire il bersaglio dell'accertamento compiuto in segreto dall'organo inquirente; in secondo luogo, i rimedi garantiti allo stesso soggetto passivo risultano posticipati al termine delle operazioni, quando la lesione delle aspettative di intimità è ormai stata perpetrata. Ciò conduce a considerare i controlli occulti come misure investigative *lato sensu* coercitive, a prescindere dall'uso di una coazione fisica[118]. Questa soluzione è condivisa anche dalla Corte e.d.u., la quale ha posto l'accento sulla speciale

[114] In questo senso, nel contesto nordamericano, D. GRAY, *The Fourth Amendment in an Age of Surveillance*, Cambridge University Press, 2017, p. 124 ss.

[115] Illustra le due alternative, riconoscendo la maggiore sensibilità della seconda prospettiva rispetto alla necessità di tutela dei diritti fondamentali, C. CONTI, *Sicurezza e riservatezza*, in *Dir. pen. proc.*, 2019, p. 1585.

[116] F. NICOLICCHIA, *op. cit.*, p. 76.

[117] *Ibidem*.

[118] Cfr. sul tema F. RUGGIERI, *La giurisdizione di garanzia nelle indagini preliminari*, Milano, 1996, p. 38 ss.

invasività degli accertamenti volti a carpire clandestinamente informazioni della più diversa natura[119]. Malgrado l'indubbia insidiosità dei controlli occulti, il carattere clandestino dell'acquisizione continua ad essere considerato, all'interno del panorama nazionale, alla stregua di un fattore neutro al fine di stabilire il trattamento normativo delle ricerche, circostanza che ha incoraggiato un atteggiamento renitente rispetto alla necessità di prevedere cautele *ad hoc*. Al pari della clandestinità, anche l'elemento temporale è idoneo ad innalzare il tasso di afflittività della sorveglianza. Tale aspetto rileva in una duplice accezione: accanto all'attributo sincronico, in forza del quale la continuatività viene a designare un'acquisizione effettuata in tempo reale, questa presuppone, infatti, l'esistenza di una significativa estensione temporale delle operazioni. Pure questo profilo continua ad essere ingiustificatamente trascurato dal legislatore, non solo con riguardo alle operazioni atipiche, ma anche rispetto alle intercettazioni, ad oggi unico controllo occulto preso in considerazione dal codice di rito[120].

In base a queste considerazioni, non si vedono ragioni contrarie ad includere nella categoria dei controlli occulti e continuativi anche le attività volte all'acquisizione clandestina di informazioni non assolutamente sottratte all'altrui conoscenza ove effettuate in tempo reale e per un periodo di tempo prolungato. Ciò vale tanto per la registrazione di condotte "materiali" che hanno luogo in ambienti pubblici quanto in relazione ai controlli digitali in spazi virtuali non privati. A quest'ultimo riguardo, stante l'idoneità del contesto digitale ad aumentare in maniera esponenziale il novero delle informazioni oggetto di potenziale captazione[121], si segnalano le più mature elaborazioni interpretative, che riconoscono all'utente informatico "nuove" prerogative meritevoli di apposita protezione specificamente inerenti al contesto digitale. In particolare, si deve porre l'accento sull'individuazione di un diritto all'integrità e alla riservatezza dei sistemi informatici, che

[119] Si veda, a riguardo, Corte e.d.u., 6 settembre 1978, *Klass c. Germania*, § 68.

[120] Pur essendo istituiti limiti temporali per l'esecuzione delle intercettazioni, esso sono infatti prorogabili con successivo provvedimento senza che venga fissata una durata massima complessiva delle operazioni. Sul punto, cfr. G. ILLUMINATI, *La tutela della segretezza delle comunicazioni tra vecchio e nuovo codice*, in *Processo penale e valori costituzionali nell'insegnamento di Vittorio Grevi*, Padova, 2013, p. 107.

[121] A tale riguardo, è opportuno richiamare il passaggio di una nota sentenza della Corte di Lussemburgo, in cui i giudici affermarono che «l'inclusione nell'elenco dei risultati – che appare a seguito di una ricerca effettuata a partire dal nome di una persona – di una pagina web e delle informazioni in essa contenute relative a questa persona, poiché facilita notevolmente l'accessibilità di tali informazioni a qualsiasi utente di Internet che effettui una ricerca sulla persona di cui trattasi e può svolgere un ruolo decisivo per la diffusione di dette informazioni, è idonea a costituire un'ingerenza più rilevante nel diritto fondamentale al diritto della vita privata della persona interessata che non la pubblicazione da parte dell'editore della suddetta pagina web». Così Corte giust., sent. 13 maggio 2014, C-131/12, Google Spain SL, § 87.

postula la facoltà di servirsi dello strumento digitale senza patire indebite intrusioni e a prescindere dal profilo inerente alla natura riservata delle informazioni oggetto del controllo. A ben vedere, pure il c.d. *screening* di massa di informazioni non segrete dovrebbe essere circondato da apposite garanzie, in quanto suscettibile di provocare un *vulnus* alle prerogative individuali, nella misura in cui finisce per coartare il diritto all'autodeterminazione delle persone. Non è comunque revocabile in dubbio che, laddove il controllo occulto e continuativo risulti orientato verso un determinato soggetto, l'istituzione di apposite garanzie sia direttamente imposta dal diritto al rispetto della vita privata, a nulla rilevando in senso contrario la natura pubblica o semi-pubblica del dato. Nonostante ciò, troppo tenui appaiono le cautele previste in relazione alle ricerche riconducibili al paradigma delle operazioni in rilievo: volendo riportare l'esempio delle investigazioni digitali "sotto copertura"[122], non è certo trascurabile la necessarietà di una prodromica perlustrazione dello spazio virtuale, se non altro allo scopo di identificare gli "ambienti" nei quali si rende opportuno dar luogo alle operazioni previste dalle disposizioni di legge.

Un ultimo aspetto da prendere in considerazione, al fine di delineare compiutamente il perimetro della categoria dei controlli occulti e continuativi, è quello relativo alla paternità soggettiva della ricerca[123]. Occorre infatti domandarsi «se (*omissis*) possa influenzare l'estensione del *genus* o se, al contrario, essa debba considerarsi un fattore in tal senso assolutamente neutro»[124]. In via di principio, pare opportuno «affermare la necessità di istituire uno statuto di regole comuni per le operazioni di sorveglianza, indipendente dalla qualifica soggettiva pubblica o privata del controllante»[125]. Ciò senza voler disconoscere l'esistenza di ragioni che giustificano, in astratto, un trattamento più rigoroso per i controlli effettuati dall'autorità pubblica. Certo è che, qualora l'alternativa derivante dalla paternità pubblica o privata della ricerca permanga, come oggi avviene, da individuare nella dicotomia tra prova documentale ed atto investigativo atipico, ben poco rilevanti potrebbero apparire le conseguenze derivanti dalla differente qualificazione. Quello che sarebbe piuttosto auspicabile è la scelta di subordinare il controllo realizzato dall'attore pubblico al rispetto di

[122] Esempio paradigmatico è quello delle attività di contrasto *ex* art. 14 della l. 3 agosto 1998, n. 269, in materia di delitti di pedopornografia commessi mediante l'impiego di sistemi informatici o mezzi di comunicazione telematica ovvero utilizzando reti di telecomunicazione accessibili al pubblico.

[123] F. NICOLICCHIA, *op. cit.*, p. 103.

[124] *Ibidem*.

[125] *Ibidem*.

apposite garanzie, a seguito della sussunzione all'interno del *genus* dei controlli occulti e continuativi[126].

2. *Il metodo della proporzionalità nella disciplina dei controlli occulti*

Una volta tracciato il perimetro della categoria oggetto di esame, si tratta di entrare nel merito della regolamentazione da riservare ai controlli occulti e continuativi. Nel tentare un bilanciamento tra finalità cognitive dell'accertamento e spazi di libertà, un ruolo cardine dev'essere riconosciuto al principio di proporzionalità. Attributo dotato di una valenza ormai trasversale all'interno dei rapporti tra autorità e individuo, il suo ruolo nel contesto delle indagini penali e, segnatamente, nel contesto delle operazioni di sorveglianza segreta non costituisce certo una soluzione inedita[127]. Malgrado ciò, sul principio di proporzionalità si sono destate alcune perplessità: «accanto a chi ne riconosce infatti l'importanza e la vitalità nell'attuale panorama interpretativo (*omissis*), altri denunciano i pericoli insiti nella logica *flou* che governerebbe lo scrutinio di proporzione»[128]. Ben più allarmanti sono, tuttavia, alcune prese di posizione capaci di distorcerne la vocazione garantista. Si segnala, al riguardo, l'orientamento assunto dalla Corte costituzionale, che, nel rigettare la questione di legittimità costituzionale riferita agli artt. 266 c.p.p., 18 e 18-ter o.p.[129], ha inteso il principio

[126] L'ipotesi è caldeggiata sempre da F. NICOLICCHIA, *op. cit.*, p. 106.

[127] Tanto per fare alcuni esempi, si può pensare alla Convenzione di Budapest – fonte internazionale di riferimento per le investigazioni tecnologicamente assistite –, che, al § 146, è esplicita nel designare questo criterio quale generale parametro interpretativo delle proprie disposizioni in funzione di salvaguardia dei diritti fondamentali. In maniera analoga, la Carta dei diritti fondamentali dell'Unione europea subordina, all'art. 52, le eventuali limitazioni dei diritti sanciti dalla Carta medesima al rispetto del principio di proporzionalità. Quanto al diritto derivato dell'Unione, la direttiva 2016/680/UE impone di procedere in maniera proporzionata alle attività di trattamento dei dati personali finalizzate a prevenzione, indagine, accertamento e perseguimento dei reati; tale principio informa altresì l'intera architettura della direttiva 2014/41/UE in materia di ordine europeo di indagine penale. Il valore trova poi riscontro all'art. 8 della CEDU, in base al quale, in tanto sono ammesse deroghe al divieto di interferenze da parte delle autorità nazionali nella vita privata, in quanto esse necessarie in una società democratica. Ancorché non espressamente menzionato nel testo della Costituzione, il principio viene infine accreditato anche a livello nazionale quale criterio attraverso cui vagliare la legittimità delle limitazioni imposte alle prerogative sancite dalla Carta fondamentale.

[128] F. NICOLICCHIA, *op. cit.*, p. 112.

[129] Corte cost., sent. n. 20 del 2017, annotata da E. APRILE, *Per la Consulta resta illegittima l'acquisizione del contenuto della corrispondenza epistolare dei detenuti effettuata senza le formalità dell'art. 18-ter ord. penit.*, in *Cass. pen.*, 2017, p. 1877 ss.

di proporzionalità alla stregua di un parametro neutrale, invocabile per riscontrare l'eventuale sproporzione delle intrusioni dell'autorità nella sfera privata del singolo, ma, al contempo, idoneo a stigmatizzare un assetto normativo ritenuto troppo sbilanciato a favore delle prerogative di riservatezza. Questa impostazione, forse influenzata dal difetto di una solida costruzione teorica riferita al principio di proporzionalità nel nostro ordinamento, conduce all'effetto paradossale di un'applicazione *in malam partem* del principio stesso, interpretazione incompatibile con la stessa natura del canone[130]. Da una più ortodossa lettura del valore sembrerebbe invece potersi inferire che eventuali limitazioni delle prerogative del singolo siano da ammettersi solo ove indefettibili per il raggiungimento di uno scopo statuale dotato almeno di pari rango del diritto inciso[131]. In definitiva, deve pacificamente escludersi che il principio di proporzionalità possa essere invocato a giustificazione "in positivo" di ingerenze nella sfera privata, a maggior ragione in materia di controlli occulti. Pur nel permanere di una significativa componente relativistica del principio, specialmente nella fase del c.d. vaglio di proporzionalità, il giudizio di bilanciamento costituisce in realtà solo una parte di un articolato scrutinio, che si declina ulteriormente nella verifica di idoneità e necessità della misura. Inoltre, il carattere intrinsecamente discrezionale della valutazione di proporzionalità incontra il limite rappresentato da quella porzione essenziale delle prerogative individuali insuscettibile di essere posta in bilanciamento con le pretese dell'autorità[132].

Veniamo al contenuto precettivo della proporzionalità nel campo dei controlli occulti e continuativi. Come è noto, il test di proporzionalità si caratterizza per la struttura triadica, che consente di distinguere tre momenti valutativi[133]: lo scrutinio di idoneità, la verifica di necessità e, da ultimo, il bilanciamento degli opposti interessi in conflitto.

---

[130] Il rilievo è di F. NICOLICCHIA, *op. cit.*, p. 116.

[131] Diffusamente sul punto D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, p. 55 ss., ove si sottolinea «la vocazione di genuina garanzia liberale» propria del canone in discorso. Desume invece questa necessità dal carattere di inviolabilità riconosciuto alle libertà costituzionali F. ALONZI, *L'*escalation *dei mezzi di intrusione nella sfera privata*, in *Rev. Bras. de Direito Processual Penal*, 2019, p. 1425 ss.

[132] Cfr. R. ORLANDI, *Rito penale e salvaguardia dei galantuomini*, relazione svolta a Lucca (dicembre 2004- bicentenario della nascita di Francesco Carrara), in *Criminalia. Annuario di scienze* penalistiche, 2007, p. 304, che evidenzia la fondamentale valenza del concetto di «dignità umana» in chiave delimitativa di un «nucleo incomprimibile» delle prerogative del singolo in ambito processualpenalistico.

[133] Lo ricordano, tra gli altri, A. SANDULLI, voce *Proporzionalità*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, p. 4644-4645; R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. pen. proc.*, 2014, p. 1157.

Prendendo le mosse dal requisito di idoneità, esso consiste in un giudizio di astratta adeguatezza della misura al raggiungimento dello scopo per cui la stessa è consentita, ovvero – nel caso di specie – l'acquisizione di elementi rilevanti ai fini dell'accertamento penale. Secondo una fortunata definizione, «l'idoneità è il criterio di razionalità tecnica basato sul nesso di ragionevole strumentalità del mezzo rispetto al fine perseguito. La misura è inidonea se non ha alcun effetto utile oppure rende difficile il raggiungimento dello scopo, mentre anche la semplice possibilità di ottenere il risultato, di facilitarlo in qualche caso, basta a soddisfare il requisito»[134]. Ne consegue che, ai fini del giudizio di idoneità, rileva anzitutto una valutazione di pertinenza tra controllo ed oggetto dell'indagine, giacché una ricerca avulsa dal tema dell'accertamento si risolverebbe in un «flagello nelle mani di un pazzo»[135]. Appare dirompente la circostanza per la quale, essendo sin dalla loro genesi questi controlli irripetibili, essi appaiono fisiologicamente preordinati alla raccolta di elementi da impiegare nel futuro giudizio di responsabilità, cosicché la loro idoneità andrà giocoforza vagliata anche alla luce di tale orientamento finalistico. Sono infine inidonee al raggiungimento dello scopo le misure che permettono l'acquisizione di informazioni sprovviste dei connotati di affidabilità e verificabilità postuma.

Quanto al vaglio di necessità, «da intendersi quale espressione di una logica del minimo sacrificio necessario in forza della quale eventuali limitazioni alle prerogative fondamentali devono in primo luogo essere circoscritte ad ipotesi eccezionali in cui l'ingerenza risulti davvero imprescindibile al raggiungimento dello scopo che la legittima»[136], va escluso che possano considerarsi necessarie intrusioni investigative dirette ad arricchire *ad abundantiam* un quadro probatorio già compiutamente delineato. Secondo corollario di questo principio consiste nell'obbligo di prediligere, a parità di attitudine documentative, le modalità meno impattanti sull'esercizio delle libertà fondamentali. Si può, quindi, istituire un rapporto di genere a specie tra idoneità e necessità, in quanto «la misura inidonea non potrà a maggior ragione dirsi mai necessaria, mentre tra le attività astrattamente idonee occorrerà pur sempre

[134] Così D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità*, in *Riv. it. dir. proc. pen.*, 2020, p. 62 ss.

[135] Questa efficace espressione è di M. NOBILI, *Diritti per la fase che "non conta e non pesa"*, cit., p. 40. Con particolare riguardo alle intercettazioni, insiste sulla necessità di assicurare la rigida pertinenzialità tra campo della ricerca ed oggetto dell'indagine M. L. DI BITONTO, *Lungo la strada per la riforma delle intercettazioni*, in *Cass. pen.*, 2009, p. 18.

[136] F. NICOLICCHIA, *op. cit.*, p. 125.

isolare quelle effettivamente necessarie al perseguimento dell'esigenza che le giustifica»[137]. Se la verifica di necessità dev'essere parametrata all'oggetto della ricerca, irrilevanti appaiono invece le considerazioni legate alla gravità del reato per cui si procede[138], che potranno invece venire in questione esclusivamente al fine di orientare il bilanciamento tra gli opposti interessi in conflitto.

In merito a quest'ultimo, la disciplina legislativa dovrebbe garantire un rapporto di proporzionalità diretta fra il grado di intrusività della misura ed il livello di intensità delle garanzie. Sul punto, però, è dato riscontrare un atteggiamento di profonda chiusura del nostro ordinamento, come conferma la vicenda relativa al c.d. captatore informatico quale mezzo per l'intercettazione di comunicazioni o conversazioni[139]: in prospettiva *de iure condendo*, la corretta applicazione del giudizio di proporzionalità dovrebbe porre capo ad una regolamentazione più analitica e restrittiva rispetto a quella generalmente dettata dagli artt. 266 ss. c.p.p.[140].

Sulla controversa questione della titolarità soggettiva del potere di disporre il controllo clandestino, la soluzione maggiormente garantista è rappresentata dalla previsione di una riserva di giurisdizione, che attribuisca al giudice – in quanto organo terzo ed imparziale – la legittimazione esclusiva ad autorizzare le attività di monitoraggio in discorso. Si discute, tuttavia, se ciò possa inferirsi dalle prescrizioni costituzionali persino con riguardo agli atti di indagine che implicano una limitazione del diritto a comunicare segretamente. Più in particolare, la disputa attiene all'interpretazione della locuzione «autorità giudiziaria» contenuta agli artt. 13 ss. Cost.: con specifico riguardo alle intercettazioni, vi è infatti chi attribuisce carattere restrittivo al disposto costituzionale dell'art. 15 Cost., desumendo da ciò

[137] *Ibidem*, p. 126.

[138] Segnala criticamente la tendenza di un arretramento della verifica circa l'effettiva necessità della misura in presenza di «delitti per cui l'intercettazione è strumento di ricerca particolarmente utile», A. CAMON, *Le intercettazioni nel processo penale*, Bologna, 1996, p. 112-113.

[139] Dapprima, nelle more dell'adozione di una disciplina di legge appositamente dedicata allo strumento, la giurisprudenza aveva consentito il ricorso al c.d. *trojan* in forza della disciplina già esistente per le captazioni mediante strumenti tradizionali *sic et simpliciter*; per quanto la riforma delle intercettazioni abbia introdotto un onere di motivazione rafforzato in sede di autorizzazione all'impiego del captatore, prescrivendo di specificare le ragioni che rendono necessario l'utilizzo di tale tecnica e di predeterminare luoghi e tempi dell'intercettazione al fine di prevenire acquisizioni indiscriminate almeno nell'ambito di procedimenti per reati c.d. comuni, la ricerca risulta ammissibile per tutte le fattispecie di reato che legittimano l'intercettazione tradizionale, così ampliandosi il catalogo delle violazioni che consentono l'impiego dello strumento a tutte quelle contemplate dall'art. 266 c.p.p.

[140] Così F. NICOLICCHIA, *op. cit.*, p. 131.

il potere esclusivo in capo al giudice di autorizzare il ricorso al mezzo di ricerca della prova[141]. Certo è che un monopolio del giudice in fase autorizzativa non sussiste rispetto a quelle operazioni idonee a pregiudicare il mero interesse alla riservatezza: in quest'ultima ipotesi non si rinviene infatti alcuna norma di rango costituzionale istitutiva di una riserva di giurisdizione[142]. In chiave preventiva, «è comunque difficile non riconoscere l'illegittimità di un sistema che affidi al pubblico ministero il monopolio delle valutazioni inerenti all'opportunità di ricorrere a misure di controllo occulto senza alcuna verifica successiva»[143]. Sebbene, cionondimeno, questa sia la situazione attualmente sussistente all'interno del nostro ordinamento, anche alla luce degli orientamenti espressi dai legislatori di altri contesti ordinamentali, parrebbe in ogni caso preferibile mantenere in capo al giudice l'esclusiva competenza ad autorizzare le forme di sorveglianza maggiormente invasive.

Vi è quindi, sempre nella fase antecedente al controllo, la questione delle fattispecie abilitanti: un corretto bilanciamento tra gli interessi in gioco impedisce infatti di prescindere dalla predeterminazione delle ipotesi di reato per le quali è astrattamente ammissibile il ricorso alla ricerca clandestina. Sulla base della necessaria relazione di proporzionalità diretta tra tasso di invasività dell'ingerenza ed intensità delle garanzie legali, le misure maggiormente invasive dovrebbero essere riservate alle indagini relative alle più gravi violazioni, mentre, secondo la Corte di giustizia, si potrebbe addirittura prescindere dalla previa individuazione delle fattispecie di reato che ammettono l'ingerenza per i controlli meno incisivi[144]. Restano, in ogni caso, censurabili le locuzioni normative carenti in punto di tassatività, in quanto incapaci di circoscrivere entro margini di adeguata prevedibilità le fattispecie sostanziali in cui è possibile attivare le ricerche[145].

---

[141] In questo senso P. BALDUCCI, *Le garanzie nelle intercettazioni tra costituzione e legge ordinaria*, Milano, 2002, p. 45. Analogamente, L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, p. 61 ss. In senso contrario, però, richiamando anche il *dictum* di Corte cost., sent. n. 81 del 1993, A. CAMON, *Le intercettazioni nel processo penale*, Bologna, 1996, p. 110.

[142] Conformemente, anche con riguardo al disposto degli artt. 13 e 14 Cost., F. ALONZI, *Le attività del giudice nelle indagini preliminari. Tra giurisdizione e controllo giudiziale*, Padova, 2011, p. 130 ss.

[143] F. NICOLICCHIA, *op. cit.*, p. 134.

[144] Si veda, in proposito, Corte giust., sent. 2 ottobre 2018, C-207/16, *Ministerio Fiscal*, annotata da G. FORMICI, *Tutela della riservatezza delle comunicazioni elettroniche*, in *Osservatorio costituzionale*, 2018, p 453 ss.

[145] Un esempio paradigmatico di tale difetto può essere rintracciato nel disposto dell'art. 266-bis c.p.p. che, permettendo l'intercettazione di comunicazioni informatiche o telematiche per tutti i reati «commessi mediante l'impiego di tecnologie informatiche o telematiche», opera un riferimento ad una pluralità indeterminata di reati.

Da ultimo, si pone la questione della necessità dell'ingerenza. Atteso che la disciplina dovrebbe farsi carico di limitare il ricorso alla sorveglianza ai casi in cui essa risulti imprescindibile al fine di soddisfare le esigenze cognitive dell'accertamento, si impone una verifica di natura empirica circa la presenza di elementi sintomatici della effettiva sussistenza di una violazione del tipo di quelle che abilitano il controllo. Il presupposto del c.d. *fumus delicti* viene quindi delineandosi «quale strutturato compendio indiziario ragionevolmente riferibile ad una precisa e circostanziata ipotesi di reato»[146]. In tale prospettiva, pare allora condivisibile l'opinione di chi stigmatizza alcune prese di posizione della giurisprudenza di legittimità, che interpreta la nozione di gravi indizi di reato *ex* art. 267 c.p.p. alla stregua di un vaglio genericamente riferito «alla effettiva serietà del progetto investigativo»[147], dovendo piuttosto la verifica assumere direttamente come oggetto la consistenza della specifica ipotesi di accusa ascritta all'indagato, in armonia col corretto operare del principio di proporzionalità. Sul versante soggettivo, questione tutt'altro che secondaria è quella relativa al coefficiente di attribuibilità soggettiva degli elementi comprovanti la verificazione dell'illecito. In base all'opinione prevalente, la locuzione «indizi di reato» di cui all'art. 267, comma 1 c.p.p. designa «una piattaforma conoscitiva riferibile alla mera esistenza di una violazione penalmente rilevante, sebbene non ancora soggettivamente orientata verso una determinata persona»[148]. In questo modo, si giunge ad ammettere l'intercettazione nell'ambito di procedimenti contro ignoti, nonché nei confronti di persone diverse dall'indagato. Se ciò appare necessario onde evitare di pregiudicare l'attitudine euristica del mezzo di ricerca della prova, è innegabile che, nel contesto dei controlli di ultima generazione, particolarmente elevato risulti il rischio di venire a conoscenza di contributi riconducibili a soggetti estranei all'indagine. Opportunamente si è quindi sostenuto in dottrina che «all'aumento della frequenza statistica delle ipotesi in cui può ottenersi la contestuale documentazione di dati dalla provenienza soggettiva diversificata dovrebbe (*omissis*) corrispondere un innalzamento della soglia delle tutele»[149].

[146] F. NICOLICCHIA, *op. cit.*, p. 141.

[147] Cass., Sez. Un., 17 novembre 2004, Esposito, in *Cass. pen*., 2005, p. 343.

[148] F. NICOLICCHIA, *op. cit.*, p. 143.

[149] *Ibidem*, p. 147. In questa direzione si è mosso il legislatore con riferimento all'art. 267, comma 1 c.p.p., nel momento in cui, in sede di autorizzazione all'uso del captatore quale strumento per l'intercettazione ambientale nell'ambito di procedimenti per reati che non consentono l'intrusione domiciliare in assenza del requisito dell'attualità criminosa, prescrive di specificare «i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono».

3. *I controlli occulti e lo spazio giudiziario europeo*

La contrapposizione tra l'interesse cognitivo manifestato dall'autorità pubblica e le libertà dei singoli tende oggi a superare i confini delle singole realtà statuali, collocandosi piuttosto nel contesto di più complesse attività di indagine che si sviluppano su scala internazionale. Se, da un lato, i più evoluti strumenti di sorveglianza clandestina rendono possibile una ricerca "mobile", che dà luogo a sconfinamenti al di fuori dello Stato in cui la stessa ha avuto origine, la mobilità del dato digitale, dall'altro lato, induce a prescindere dalle delimitazioni spaziali imposte a livello geografico. Il "problema del controllo", pertanto, manifesta oggi una dimensione inter-ordinamentale, che si declina nell'esigenza di realizzare un'opera di mediazione tra le diverse tradizioni giuridiche dei paesi europei. In altri termini, la mobilità delle ricerche impone di confrontarsi con questioni legate sia alle pretese di sovranità degli Stati sia alla necessità di garantire una soglia minima di tutela condivisa dei diritti fondamentali all'interno del panorama giuridico europeo[150].

Un accurato esame di queste tematiche impone di cominciare da una sommaria ricognizione delle fonti normative di riferimento. In primo luogo, si deve menzionare la Convenzione europea di assistenza giudiziaria in materia penale di Strasburgo del 20 aprile 1959, elaborata in seno al Consiglio d'Europa: questo documento costituisce l'antecedente della più recente Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea, siglata a Bruxelles il 29 maggio 2000. Alla cooperazione di polizia ed all'assistenza giudiziaria in materia penale è poi dedicata la Convenzione applicativa dell'Accordo di Schengen, mentre ulteriore strumento pattizio dotato di specifica importanza nel settore oggetto di indagine è la Convenzione sulla criminalità informatica di Budapest del 23 novembre 2000. Venendo al diritto derivato dell'Unione, si segnala la direttiva 2014/41/UE in materia di ordine europeo di indagine penale (OEI), costituente il più evoluto sistema di circolazione della prova nell'eurozona e dotato di carattere preminente rispetto alle disposizioni convenzionali di assistenza giudiziaria eventualmente in essere tra gli Stati vincolati all'applicazione della direttiva. L'ordine europeo di indagine, «strumento ibrido che assomma in sé i caratteri della mutua assistenza giudiziaria, del reciproco riconoscimento e l'embrione di un'armonizzazione probatoria»[151], si differenzia dal suo

[150] F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" tra innovazione e tradizione*, in *Proc. pen. giust.*, 2017, p. 179. Queste due concorrenti dimensioni vengono identificate dalla dottrina quali componenti essenziali di una «prospettiva "internazionalista"» dell'assistenza giudiziaria. Cfr. al riguardo A. CIAMPI, *L'assunzione di prove all'estero in materia penale*, Padova, 2003, p. 8 ss.

[151] Così F. NICOLICCHIA, *op. cit.*, p. 180.

predecessore rappresentato dal mandato di ricerca della prova di cui alla decisione quadro 2008/978/GAI[152], in quanto aspira a dare vita ad un meccanismo acquisito a carattere tendenzialmente onnicomprensivo, cioè riferibile sia a veri e propri elementi di prova sia al compimento di «tutti gli atti di indagine finalizzati all'acquisizione di prove»[153]. La dottrina ha salutato con favore l'assoggettamento delle investigazioni transfrontaliere alle formalità proprie dell'assistenza giudiziaria, valutandolo come un risultato positivo nell'ottica della tutela delle prerogative dei singoli. Mediante la loro riconduzione al settore dell'assistenza giudiziaria, le attività c.d. operative, cioè compiute a fini di indagini e non di acquisizione probatoria in senso strettoòò, vengono regolamentate attraverso un apparato di regole e prescrizioni ben più strutturato rispetto a quello esistente nel contesto della cooperazione di polizia, governato per lo più da logiche di collaborazione spontanea e deformalizzata.

Questione di grande rilievo è quella della tipicità degli atti di indagine nel sistema OEI. Nell'interrogarsi sulle previsioni della direttiva 2014/41/UE applicabili alle attività qualificate come controlli occulti e continuativi, occorre infatti prendere in esame le conseguenze della riserva di legge di cui all'art. 8 § 2 della CEDU. Il quesito è, in altri termini, se siano ammissibili misure acquisitive innominate, ovvero ulteriori a quelle espressamente previste dagli ordinamenti degli Stati. Una risposta parrebbe rinvenirsi nell'art. 10 § 5 della direttiva, che consente di omettere l'esecuzione dell'OEI, qualora l'atto richiesto «non sia previsto dal diritto dello Stato di esecuzione». A fugare ogni dubbio è, tuttavia, l'art. 11 § 1 lett. *f*, che consente di rifiutare l'esecuzione dell'ordine qualora essa risulti incompatibile con gli obblighi derivanti dall'art. 6 TUE[154]: essendo ricomprese fra questi le prescrizioni contenute nella CEDU così come interpretate dalla giurisprudenza, appare indiscutibile che il compimento di attività lesive del diritto alla riservatezza in assenza di una base legale sufficientemente analitica rientri nell'ambito di operatività del motivo di rifiuto. Secondo la dottrina[155], deve così ritenersi che, laddove lo Stato di esecuzione constati

---

[152] L'art. 4 § 2 lett. *c* della decisione quadro escludeva espressamente dal suo ambito di operatività proprio l'acquisizione di «informazioni in tempo reale, ad esempio attraverso l'intercettazione di comunicazioni, la sorveglianza discreta dell'indiziato o il controllo dei movimenti su conti bancari».

[153] Così il considerando n. 8 della direttiva.

[154] Questa ipotesi di non riconoscimento, originariamente assente nel testo della proposta di direttiva, veniva successivamente introdotta su sollecitazione dell'Agenzia dell'Unione europea per i diritti fondamentali.

[155] Cfr. F. NICOLICCHIA, *op. cit.*, p. 192. Secondo questo Autore, «la lesione al diritto tutelato si produce infatti materialmente nello Stato di esecuzione, ed è dunque anche con riferimento al suo assetto ordinamentale che andrà verificato il rispetto delle condizioni dettate per eventuali limitazioni dell'interesse al riserbo».

l'assenza nel proprio diritto di una previsione normativa nazionale che consenta l'esecuzione della ricerca, esso potrebbe eccepire il motivo di non riconoscimento in questione.

Senonché, questo regime, teso a riconoscere la preminenza della tutela dei diritti fondamentali rispetto alla circolazione probatoria, non è esente da equivoci: l'art. 10 § 2, infatti, concernente il catalogo delle misure destinatarie di un regime di trattamento "semplificato", vi include, con un riferimento alquanto generico, tutti gli «atti d'indagine non coercitivi definiti dal diritto dello Stato di esecuzione». Appare evidente come di una clausola simile i legislatori nazionali potrebbero agevolmente profittare, al fine di ricondurvi anche operazioni da cui derivano tutt'altro che trascurabili limitazioni delle prerogative fondamentali[156].

Quid iuris nel caso in cui il controllo risulti compiutamente regolamentato solo dal diritto dello Stato di esecuzione? In questo caso, non sembrano condivisibili gli argomenti secondo i quali dovrebbe dubitarsi dell'operatività del motivo di non riconoscimento *ex* art. 11 § 1 lett. *f*, in quanto si verrebbe qui a delineare proprio «quella sorta di responsabilità "concorsuale" tra gli Stati che il motivo di non riconoscimento in esame mira a prevenire»[157]. Come conferma la giurisprudenza della Corte europea dei diritti dell'uomo[158], infatti, l'esecuzione dell'ordine di esecuzione, avente ad oggetto misure restrittive del diritto al rispetto della vita privata atipiche, anche solo in base all'ordinamento dello Stato di emissione della richiesta, finirebbe per esporre a responsabilità anche lo Stato di esecuzione. Non si può, per altro verso, neppure constatare la piena idoneità del sistema istituito dalla direttiva OEI a prevenire violazioni delle libertà affermate dalle stesse fonti europee: per quanto la direttiva stessa prescriva all'autorità "emittente" un autonomo onere di verifica specificamente inerente al rispetto dei diritti fondamentali[159], appare remota l'ipotesi che la

[156] Si sofferma sull'assenza di una nozione condivisa della coercitività della misura e sul conseguente rischio di interpretazioni difformi all'interno dei singoli ordinamenti S. RUGGERI, *Introduction to the Proposal of a European Investigation Order: Due Process Concerns and Open Issues*, in ID., *Transnational Evidence and Multicultural Inquiries in Europe*, 2014, p. 18 ss. Quanto paventato è, in effetti, ciò che si è realizzato, nel nostro ordinamento, con il d.lgs. n. 108/2017, che ha istituito un regime di tipicità investigativa temperata nella procedura di esecuzione passiva dell'ordine in forza del quale – a fronte della generale impossibilità di dare corso alla richiesta nel caso in cui l'atto «non è previsto dalla legge italiana» – deve comunque procedersi, in ogni caso, al compimento di «tutti gli atti di indagine che non incidono sulla libertà personale e sul diritto all'inviolabilità del domicilio» (così appunto l'art. 9 lett. *d* del d.lgs. n. 108/2017).

[157] F. NICOLICCHIA, *op. cit.*, p. 195.

[158] Cfr. Corte e.d.u., 7 luglio 1989, *Soering c. Regno Unito*, § 91 ss.

[159] Si allude, in particolare, al disposto dell'art. 6 § 1 lett. *a* della direttiva, nonché ai considerando n. 11 e 12.

ridetta autorità arrivi ad autocensurarsi, riconoscendo l'illegittimità della propria richiesta in ragione dell'assenza di un'adeguata copertura legale nazionale a giustificazione dei controlli[160].

Per quanto concerne lo scrutinio di proporzionalità dei controlli richiesti mediante OEI, viene in rilievo l'art. 28 della direttiva, che contempla uno specifico motivo di rifiuto dell'ordine, rappresentato dal caso in cui risulti impossibile ricorrere alla misura in un «caso interno analogo». In questo modo, si assoggetta l'atto investigativo ad una verifica di proporzionalità operata, fra l'altro, alla luce del regime giuridico imposto dalla *lex fori* in analoga fattispecie puramente interna. Malgrado l'apparente inequivocità della disposizione, si contendono il campo due diverse letture della locuzione in discorso. Da una parte, secondo un'interpretazione restrittiva ed ispirata al principio del mutuo riconoscimento, non sarebbe necessario l'accertamento di tutti i requisiti sostanziali imposti dal diritto dello Stato di esecuzione, dovendosi più semplicemente verificare l'inclusione della fattispecie di reato per cui si procede all'interno del catalogo delle ipotesi legittimanti il controllo in base alla *lex loci*[161]; dall'altro lato, vi sono i fautori di un'interpretazione più ampia, avente ad oggetto l'insieme delle circostanze necessarie ai fini dell'attivazione della misura, attraverso un'integrale rivalutazione della proporzionalità dell'intrusione conformemente ai canoni del diritto dello Stato di esecuzione[162].

La seconda soluzione è indubbiamente quella più attenta al rispetto dei diritti fondamentali incisi dai controlli, ma, allo stesso tempo, mal si concilia con il principio del mutuo riconoscimento, in quanto «affermare la necessità di uno scrutinio secondo lo *standard* della *lex loci* contraddice (*omissis*) apertamente la reciproca fiducia alla base del funzionamento dello strumento di cooperazione»[163]. Resta in ogni caso fermo il rispetto della

[160] La considerazione è di F. NICOLICCHIA, *op. cit.*, p. 197.

[161] Di questo avviso M. PANZAVOLTA, *Ordine di indagine europeo e indagini bancarie: spunti di riflessione sul concetto di caso interno analogo e atto di indagine alternativo*, in A. DIPIETRO-M. CAIANIELLO (a cura di), *Indagini penali e amministrative in materia di frodi IVA e di imposte doganali. L'impatto dell'*European Investigation Order *sulla cooperazione*, Bari, 2016, p. 380. Sulla stessa linea, con specifico riferimento all'ordine riguardante l'attività di intercettazione, G. DE AMICIS, *Dalle rogatorie all'ordine europeo di indagine: verso un nuovo diritto della cooperazione giudiziaria penale*, in *Cass. pen.*, 2018, p. 37.

[162] Con particolare riferimento all'ordinamento italiano e, segnatamente, alla materia delle intercettazioni, cfr., diffusamente, A. NOCERA, *Il sindacato giurisdizionale interno in tema di ordine europeo di intercettazione*, in *Dir. pen. cont.*, 2018, p. 164. Si veda, altresì, A. MANGIARACINA, *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale*, in *Dir. pen. proc.*, 2018, n. 2, p. 177.

[163] F. NICOLICCHIA, *op. cit.*, p. 199.

proporzionalità dell'ingerenza in virtù dell'art. 11 § 1 lett. *f*, in quanto, a pena di configurare una responsabilità dello Stato di esecuzione sulla base dell'art. 6 TUE, l'esecuzione di ogni richiesta avente ad oggetto operazioni limitative del diritto al rispetto della vita privata va sempre subordinata alle condizioni dettate in proposito dalla CEDU e dalla Carta di Nizza[164].

È appena il caso di precisare che l'eventuale sproporzione della misura secondo i canoni delle fonti da ultimo richiamate assume comunque rilievo, quantomeno nei limiti dell'art. 11 § 1 lett. *f* della direttiva, anche in occasione del compimento di controlli diversi da quelli descritti dall'art. 28, ivi inclusi quelli contemplati nell'elenco di misure "non coercitive" *ex* art. 10 § 2[165]. In quest'ultimo caso, però, si esclude la possibilità di rifiutare l'esecuzione dell'ordine qualora il reato oggetto dell'OEI non figuri tra le violazioni abilitanti l'attivazione della misura richiesta secondo la *lex loci*; peraltro, lo Stato richiesto del compimento di una delle attività descritte dall'art. 10 § 2 dovrebbe procedervi anche laddove la condotta per la quale è stato emesso l'ordine non costituisca reato in base al proprio diritto nazionale. Sembra quindi potersi concludere che vi sia un'incoerenza di fondo, oltre che una probabile violazione degli obblighi derivanti dall'art. 6 TUE, nel prevedere che uno Stato possa essere obbligato ad una restrizione dei diritti fondamentali dei cittadini al fine di accertare un fatto che neppure costituisce reato secondo il diritto nazionale[166].

Legittime sono, infine, le perplessità in ordine allo stesso metodo tipico del mutuo riconoscimento, che affida la tutela dei diritti a clausole flessibili, passibili di interpretazioni anche assai diverse: in questo modo, il delicato bilanciamento tra esigenze repressive e tutela delle libertà fondamentali viene infatti traslato, in maniera sempre più evidente, dal piano legislativo a quello dell'interpretazione giurisprudenziale, con tutto quanto ne consegue in punto di discrezionalità dell'interprete[167]. Alla luce di ciò, sarebbe forse stata auspicabile una più puntuale definizione del contenuto precettivo delle clausole normative poste a salvaguardia dei diritti fondamentali nella fase acquisitiva, anche considerato che non esiste in oggi una definizione condivisa a livello europeo di proporzionalità[168].

---

[164] Tra le quali, appunto, rientra la proporzionalità della misura.

[165] Impone questa conclusione la clausola di salvezza contenuta in apertura dell'art. 10 § 2 della direttiva.

[166] Si veda, in questo senso, F. NICOLICCHIA, *op. cit.*, p. 201.

[167] Per tutti, P. FERRUA, *Il contraddittorio tra declino della legge e tirannia del diritto vivente*, in D. NEGRI-R. ORLANDI (a cura di), *Le erosioni silenziose del contraddittorio*, Torino, 2017, p. 15 ss.

[168] Questo aspetto è messo in luce da L. BACHMAIER WINTER, *Transnational Evidence. Towards the Transposition of Directive 2014/41*, p. 52.

Un ultimo profilo da sondare è quello relativo alla circolazione transfrontaliera del prodotto dei controlli, fattispecie nella quale viene in rilievo il trasferimento di informazioni già nella disponibilità dello Stato d'esecuzione. Sul punto, la direttiva OEI relega l'acquisizione di informazioni o prove già in possesso dell'autorità di esecuzione dell'ordine nel ricordato elenco di richieste alle quali occorre dare sempre corso, a prescindere dalla loro disponibilità in analogo caso interno e dalla stessa previsione della misura nel diritto della *lex loci*[169]. Questo assetto manifesta una certa coerenza con la più generale tendenza esistente a livello europeo, incline a considerare la condivisione transnazionale di informazioni alla stregua di un'attività sciolta dalle regole dell'assistenza giudiziaria e, per questa ragione, risulta particolarmente appetibile per le autorità interessate alla cooperazione[170]. È altresì vero, per contro, che gli Stati potrebbero così essere indotti a scavalcare le formalità imposte dalle procedure di assistenza giudiziaria per l'acquisizione di prove costituende per il tramite di canali di cooperazione "non ufficiale", salvo poi richiedere *ex post* il trasferimento delle informazioni di interesse attraverso regole più permissive.

Per quanto poi taluno abbia valorizzato l'implicito divieto probatorio istituito dal sistema OEI, che, nell'annoverare tra le attività ricomprese nel campo di applicazione dello strumento proprio lo scambio di elementi già in possesso dello Stato estero, porrebbe capo ad una forma di inutilizzabilità delle forme di acquisizione diverse da quelle contemplate dalla direttiva[171], resta fermo il disposto dell'art. 10, in forza del quale non è possibile rifiutare l'esecuzione dell'ordine avente ad oggetto il trasferimento di informazioni "precostituite" in ragione dei motivi inerenti alla natura del reato oggetto del procedimento all'interno dello Stato di emissione. Il quadro illustrato si complica, infine, alla luce delle più recenti iniziative legislative in essere a livello europeo: il riferimento è, in particolare,

[169] Rileva qui il disposto dell'art. 10 § 2 lett. *a* e *b*.

[170] Lo evidenzia G. DE AMICIS, *Organismi europei di cooperazione e coordinamento investigativo*, p. 120 ss. Più in generale, sulla cooperazione mediante scambio di informazioni tra Stati cfr., fra gli altri, M. GIALUZ, *La cooperazione informativa quale motore del sistema europeo di sicurezza*, in *Cooperazione informativa e giustizia penale nell'Unione* europea, Trieste, 2009, p. 15 ss.; S. RUGGERI, *Transnational Inquiries and the Protection of Fundamental Rights in Comparative Law*, in *Criminal Proceedings. A study in memory of Vittorio Grevi and Giovanni Tranchina*, 2013, p. 559 ss.; P. TROISI, *La circolazione di informazioni per le investigazioni penali nello spazio giuridico europeo*, Padova, 2012; ID, *Il potenziamento della cooperazione transfrontaliera. Lo scambio di informazioni*, in AA. VV., *"Spazio europeo di giustizia" e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali*, 2012, p. 195 ss.

[171] In questo senso M. DANIELE, *La sfera d'uso delle prove raccolte*, in M. DANIELE-R. E. KOSTORIS (a cura di), *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, Torino, 2018, p. 184 ss. Per contro, la richiesta acquisitiva dovrebbe essere vagliata alla luce dell'artt. 11 § 1 lett. *f*, il quale autorizza lo Stato di esecuzione a rifiutare di dare corso all'ordine in presenza di incompatibilità con gli obblighi derivanti dall'art. 6 TUE, ivi inclusi, pertanto, quelli sanciti dall'art. 8 § 2 CEDU.

alla proposta di regolamento relativa all'ordine europeo di produzione e conservazione delle prove elettroniche[172], tacciato di eccessiva farraginosità a pochi anni appena dalla sua entrata in vigore[173]. Finalità di questa proposta è la creazione di un più efficace strumento di cooperazione per l'acquisizione transfrontaliera della c.d. prova digitale precostituita, nozione entro cui vengono espressamente ricomprese le informazioni di carattere personale detenute dai gestori dei servizi di telecomunicazione stranieri[174]. L'aspetto più allarmante del nuovo strumento è indubbiamente rappresentato dalla possibilità di operare un trasferimento transnazionale di dati senza il filtro preventivo di un'autorità giudiziaria dello Stato in cui si trova il destinatario della richiesta: in questo modo, il delicato compito di vagliare la legalità e la proporzionalità di attività impattanti sui diritti fondamentali resta così demandato al destinatario dell'ordine di produzione, il quale non è certo l'interlocutore più idoneo a scongiurare ingerenze illegittime[175].

Neppure dev'essere trascurato, infine, come il coinvolgimento strutturale di entità private nelle dinamiche investigative renda quanto mai attuali i rischi connessi ad una "privatizzazione" dell'indagine[176]. L'auspicio pare dunque essere quello di un impegno al contrasto della tendenza delineatasi a livello europeo con riguardo allo scambio di informazioni riservate precostituite. A questo proposito, si possono segnalare ulteriori iniziative normative attualmente in essere, come la partecipazione dell'Unione ai negoziati per la predisposizione di un II Protocollo aggiuntivo alla Convenzione di Budapest, riguardante anche «*direct cooperation with service providers in other jurisdiction with regard to requests for subscriber information*»[177], ovvero i «negoziati in vista della conclusione di un accordo tra l'Unione e gli Stati Uniti d'America sull'accesso

[172] «Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale» COM (2018) 225 final.

[173] Lo evidenziano, richiamandosi al testo dell'*Impact Assessment* che accompagna l'iniziativa legislativa, M. GIALUZ-J. DELLA TORRE, *Lotta alla criminalità nel* cyberspazio*: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont.*, 2018, p. 281.

[174] Per una specifica dettagliata delle informazioni acquisibili mediante l'ordine europeo di produzione cfr. l'art. 2 § 7 della proposta di regolamento.

[175] Cfr., in tal senso, F. NICOLICCHIA, *op. cit.*, p. 214.

[176] In senso analogo, M. DANIELE, *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Riv. dir. proc.*, 2011, p. 1288 ss.

[177] Sui contenuti della proposta cfr. F. GRAZIANI, *L'acquisizione della prova digitale all'estero: verso un secondo Protocollo addizionale alla Convenzione di Budapest sul* cybercrime, in *Rev. Bras. de Direito Processual Penal*, 2019, p. 55 ss.

transfrontaliero, da parte delle autorità giudiziarie nell'ambito di un procedimento penale, alle prove elettroniche detenute da un prestatore di servizi»[178].

[178] In questi termini la decisione del Consiglio n. 9114/19 che autorizza l'avvio dei suddetti negoziati.

CAPITOLO II
LA DISCIPLINA SULLE INTERCETTAZIONI IN CHIAVE EVOLUTIVA

SOMMARIO: 1. I principi costituzionali e convenzionali sulle intercettazioni. – 2. I presupposti per intercettare. – 3. La normativa previgente sulle intercettazioni. – 4. La l. n. 103/2017 (c.d. riforma Orlando). – 5. Il d.l. n. 161/2019 e la l. n. 3/2019 (c.d. riforma Bonafede). – 6. Le intercettazioni nei confronti dei parlamentari e del Presidente della Repubblica. – 7. Le intercettazioni preventive.

5. *I principi costituzionali e convenzionali sulle intercettazioni*

Le intercettazioni di conversazioni o comunicazioni, disciplinate agli artt. 266-271 c.p.p., costituiscono uno strumento molto efficace e, allo stesso tempo, insidioso di ricerca della prova, nella misura in cui coinvolgono confliggenti valori di rilevanza costituzionale. Ad entrare in tensione sono, in particolare, l'esigenza di accertamento dei reati e di repressione del crimine (artt. 25, 101 e 112 Cost.) con il principio della segretezza delle comunicazioni (art. 15 Cost.). Per quanto nel codice di rito non si trovi alcuna definizione di intercettazione, il vuoto è stato colmato dalla giurisprudenza, che la qualifica come un «atto del procedimento che si effettua mediante strumenti tecnici e si traduce nell'apprensione occulta, in tempo reale, del contenuto di comunicazioni riservate da parte di un soggetto estraneo al colloquio»[179].

Da questa nozione è possibile desumere i connotati fondamentali delle intercettazioni[180]. In primo luogo, rileva il carattere segreto della comunicazione o conversazione. È necessario, infatti, che i soggetti comunichino tra loro con il preciso intento di escludere estranei dal contenuto della comunicazione e secondo modalità tali da mantenere quest'ultima segreta. Inoltre, il soggetto che intercetta deve usare strumenti di captazione (elettro-meccanici, elettronici o digitali) idonei a superare le cautele elementari che dovrebbero garantire la libertà e segretezza del colloquio. Da ultimo, gli attributi della terzietà e clandestinità impongono che il soggetto captante sia assolutamente estraneo al colloquio: non si può così qualificare come intercettazione la registrazione di un colloquio

[179] Cass., sez. un., 28 maggio 2003, Torcasio, in *Guida dir*., 2003, 42, 49.

[180] In merito ai requisiti delle intercettazioni si veda, su tutti, P. TONINI, *Manuale di procedura penale*, XXI ed., Milano, 2020, p. 384-385. Cfr., inoltre, A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, nonché L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997.

effettuata da una delle persone che vi partecipano attivamente o da una persona comunque ammessa ad assistervi.

Come si diceva, la particolare delicatezza di questo mezzo di ricerca della prova è insita nelle limitazioni che reca alla segretezza delle comunicazioni, diritto fondamentale e inviolabile. Se, infatti, il domicilio rappresenta la «proiezione spaziale della persona», la libertà di comunicazione costituisce la sua «proiezione spirituale»[181], per dirla con Bricola. Per questa ragione, la Costituzione stabilisce garanzie più stringenti rispetto alla libertà personale e all'inviolabilità del domicilio: ai sensi dell'art. 15 Cost., «la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono involabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge». Così, mentre per ispezioni, perquisizioni e sequestri l'art. 13 Cost. consente che, nei casi di urgenza, possano essere compiuti su iniziativa della polizia giudiziaria, l'art. 15 Cost. non contempla analoga ipotesi, prevedendo invece l'art. 267, c. 2 c.p.p. una possibile iniziativa del pubblico ministero, salva convalida da parte del g.i.p. Con riferimento alla segretezza delle comunicazioni, la Carta fondamentale contiene, più in particolare, una vera e propria riserva di giurisdizione, che trova nell'art. 267, c. 1 c.p.p. il suo *coté* legislativo: «il pubblico ministero richiede al giudice per le indagini preliminari l'autorizzazione a disporre le operazioni previste dall'art. 266». In altri termini, soltanto con un provvedimento del giudice può essere autorizzata l'intercettazione[182] e, in adempimento della riserva di legge, il legislatore prevede i requisiti necessari per procedere all'intercettazione. Lo stesso art. 15 Cost. pone una riserva di legge rinforzata, in quanto prevede che, comunque, debbano essere stabilite "garanzie" con le norme che limitano la libertà e segretezza della corrispondenza e delle comunicazioni.

[181] F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. e proc. pen.*, 1967, p. 112.

[182] Si veda, in proposito, Corte cost., 6 aprile 1973, n. 34, la quale ha statuito che «l'art. 15 della Costituzione non si limita a proclamare l'inviolabilità della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione (comma primo), ma enuncia anche espressamente che "la loro limitazione puo' avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge": nel precetto costituzionale trovano quindi protezione sia l'interesse inerente alla libertà e segretezza delle comunicazioni, riconosciuto come connaturale ai diritti della personalità definiti inviolabili dall'art. 2 Cost., sia l'interesse connesso all'esigenza di prevenire e reprimere i reati, che è bene anch'esso oggetto di protezione costituzionale. Nel valutare la richiesta di provvedimenti autorizzativi dell'intercettazione il giudice deve procedere con cautela scrupolosa tendendo al contemperamento dei due interessi costituzionalmente protetti onde impedire che il diritto alla riservatezza delle comunicazioni venga ad essere sproporzionatamente sacrificato dalla necessità di garantire una efficace repressione degli illeciti penali: a tal fine è indispensabile che accerti se ricorrano effettive esigenze, proprie dell'amministrazione della giustizia, che realmente legittimino simile forma di indagine e se sussistano fondati motivi per ritenere che mediante la stessa possano essere acquisiti positivi risultati per le indagini in corso».

Peraltro, la constatazione che il progresso tecnologico può portare a forme di limitazione dei diritti di libertà diverse da quelle prevedibili nel 1948 ha da più parti indotto a ragionare di "domicilio informatico". Per quanto possa apparire paradossale utilizzare una categoria che dipende dalla nozione di luogo proprio in un momento in cui la dimensione spaziale, oltre a quella temporale, ha subito una contrazione per gli «effetti di deterritorializzazione» operati dalle tecnologie e dall'avvento della rete[183], la stessa Corte costituzionale[184] ha affermato che, «strettamente collegata alla libertà personale», la libertà di cui all'art. 14 Cost. tutela il domicilio «come proiezione spaziale della persona, nella prospettiva di preservare da interferenze esterne comportamenti tenuti in un determinato ambiente: prospettiva che vale, per altro verso, ad accomunare la libertà in parola a quella di comunicazione (art. 15 Cost.), quali espressioni salienti di un più ampio diritto alla riservatezza della persona». La Corte, in altri termini, sembra valorizzare entrambi i profili di tutela costituzionale del domicilio «come diritto di ammettere o escludere altre persone da determinati luoghi, in cui si svolge la vita intima di ciascun individuo; e come diritto alla riservatezza su quanto si compie nei medesimi luoghi»[185]. In questa prospettiva, anche il c.d. domicilio informatico potrebbe essere inquadrato come un'estrinsecazione ulteriore dell'oggetto di tutela dell'art. 14 Cost., che viene in rilievo in ragione delle nuove opportunità di manifestazione della personalità offerte dall'evoluzione tecnologica, nonché della proiezione virtuale degli stessi valori che stanno alla base della libertà di domicilio[186].

Particolare eco ha avuto, in questa direzione, una pronuncia resa dal *Bundesverfassungsgericht* nel 2008[187], il quale, posto di fronte alle peculiarità del monitoraggio occulto di un sistema informatico, ha ritenuto insufficiente un'interpretazione evolutiva delle garanzie offerte dalle norme costituzionali a tutela della segretezza delle telecomunicazioni e dell'inviolabilità del domicilio, riconoscendo *expressis verbis* un nuovo

[183] P. COSTANZO, *Il ruolo del fattore tecnologico e le trasformazioni del costituzionalismo*, in *Associazione italiana dei costituzionalisti. Costituzionalismo e globalizzazione. Atti del XXVII Convegno annuale. Salerno, 22-24 novembre 2012*, Napoli, 2014, p. 43.

[184] Corte cost., n. 135 del 2002.

[185] Corte cost., n. 149 del 2008.

[186] Cfr. A. BARBERA, *I principi costituzionali della libertà personale*, Milano, 1971, p. 104.

[187] BVerfG, 27 febbraio 2008, su cui v. R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. ec.*, 3/2009, p. 705. In quella occasione, il Tribunale era chiamato a valutare la legittimità di una norma della legge sulla protezione della Costituzione del Nord Reno-Westfalia, che consentiva ad un organismo di *intelligence* di derivazione governativa il monitoraggio e l'accesso segreto ai sistemi informatici collegati in rete.

diritto costituzionale «all'integrità e alla riservatezza dei sistemi informatici», fondato sulla dignità dell'uomo e dell'utente informatico, e garantendo così il «cittadino digitale» nell'uso delle tecnologie di informazione e di comunicazione in rete[188]. Come si è osservato, la decisione teutonica integra un «chiaro esempio dell'impatto tecnologico ai fini della configurazione di un diritto fondamentale»[189]. In realtà, una nozione dematerializzata di domicilio, in quanto riferita al sistema informatico o telematico, si era già fatta strada nel panorama italiano nel 1993[190] attraverso la previsione del reato di cui all'art. 615-ter c.p., che punisce con la reclusione fino a tre anni «chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo». A seguito delle divergenti posizioni espresse in dottrina circa la corretta individuazione del bene giuridico e della *ratio* sottesi a tale ipotesi di incriminazione[191], si è espressa la Cassazione[192], affermando che intenzione del legislatore era quella di assicurare protezione alla «estensione del domicilio materiale e spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, al quale estendere la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto (art. 14 Cost.)».

L'allargamento della nozione penale di domicilio, avallata dalla giurisprudenza di legittimità, ha destato l'interrogativo circa il corrispondente allargamento del concetto di cui all'art. 14 Cost.[193]: sul punto, si sono levate posizioni anche del tutto contrarie a tale copertura costituzionale per i nuovi "luoghi" informatici, da includere, piuttosto, nel diritto alla *privacy* o nella più ampia libertà e segretezza delle comunicazioni. La Corte costituzionale, per parte sua, non ha mai espressamente accolto una nozione autonoma di

[188] M. TORRE, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. e proc.*, 2015, p. 1168.

[189] P. COSTANZO, *L'impatto della tecnologia sui diritti fondamentali,* in P. COSTANZO-T. E. FROSINI-O. POLLICINO-E. APA-M. BASSINI (a cura di), *Diritti e libertà in internet*, Milano, 2017, p. 11.

[190] L. n. 547 del 1993.

[191] V., fra gli altri, R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo* jus excludendi alios, in *Dir. pen. proc.*, 2005, p. 81; L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 80.

[192] Cass., Sez. VI, 4 ottobre 1999, n. 3067; ancora, Sez. V, 26 ottobre 2012, n. 42021; Sez. V, 31 marzo 2016, n. 13057.

[193] In questo senso P. VERONESI, *Per un'interpretazione costituzionale del concetto di "domicilio",* in *Ann. Univ. Ferrara, XVII*, Ferrara, 2003, p. 125.

domicilio, adagiandosi, di fatto, su altre definizioni, «il cui senso ha a che fare certamente con un concetto che si avvicina a quello attinto dall'ordinamento penale e che si è evoluto con l'evolversi della società»[194]. Sebbene i giudici della Consulta non abbiano mai affrontato il tema del domicilio informatico, dalle sue richiamate pronunce pare, nondimeno, potersi desumere un'indiretta apertura verso nuove dimensioni del domicilio meritevoli di tutela, anche considerato che «il rapporto tra la persona e il luogo nel quale essa proietta la propria individualità, nella società dell'informazione, vale anche per i luoghi virtuali nei quali, a ben vedere, si concretano le medesime esigenze di tutela»[195]. In questo modo, l'estensione della tradizionale nozione fisica di domicilio, recepita dall'art. 615-ter c.p., viene a coincidere con il diritto «all'integrità e alla riservatezza dei sistemi informatici» di cui ha parlato il Tribunale Costituzionale tedesco e risponde all'impostazione della Corte Suprema americana, secondo la quale il IV Emendamento «*protects people, not places*» da perquisizioni e sequestri ingiustificati[196]. In definitiva, posto che «nei dispositivi tecnologici di uso comune – e, in particolare, in quello "strumento degli strumenti" che, per i filosofi antichi era la mano e per i contemporanei è lo *smartphone* – c'è l'intera nostra vita e che essi rappresentano una vera estensione della nostra mente»[197], il diritto all'*habeas data*[198] appare sempre più l'«indispensabile sviluppo contemporaneo del classico *habeas corpus*»[199].

Ciò detto, dal carattere multiforme delle intercettazioni discende che queste possano avere ad oggetto:

a) ai sensi dell'art. 266, c. 1 c.p.p., conversazioni o comunicazioni telefoniche e altre forme di telecomunicazione (c.d. intercettazioni telefoniche);
b) ai sensi dell'art. 266, c. 2 c.p.p., comunicazioni o conversazioni tra presenti (c.d. intercettazioni ambientali);

[194] C. DOMENICALI, *Tutela della persona negli spazi virtuali: la strada del "domicilio informatico"*, in *federalismi*.it, n. 7/2018, p. 13.

[195] *Ibidem*, p. 16.

[196] *Katz v. United States* (1967).

[197] M. GIALUZ, *Premessa*, in ID. (a cura di), *Le nuove intercettazioni*, in *Diritto di Internet*, 2020, p. 7.

[198] Sul quale cfr. B. GALGANI, Habeas data *e garanzie fondamentali*, in *Arch. pen.* web., 2019, p. 1, nonché L. LUPARIA, Privacy, *diritti della persona e processo penale*, in *Riv. dir. proc.*, 2019, p. 1464 ss.

[199] M. GIALUZ, *Premessa*, cit., p. 7.

c) ai sensi dell'art. 266-bis c.p.p., il flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi (c.d. intercettazioni telematiche).

È appena il caso di precisare che non costituiscono intercettazione il pedinamento elettronico tramite GPS[200], che può essere disposto dalla polizia giudiziaria come mera attività atipica, e l'acquisizione dei tabulati del traffico telefonico. Parimenti, non costituisce intercettazione, bensì documento, la registrazione fonografica occultamente eseguita da uno degli interlocutori quando questa non è stata predisposta dalla polizia giudiziaria, difettando il requisito della terzietà e clandestinità.

Bisogna, inoltre, aggiungere che l'intercettazione di conversazioni o comunicazioni assolve a diverse funzioni: oltre alla tradizionale funzione di ricerca della prova (artt. 266-271 c.p.p.), l'art. 295 c.p.p.[201] riconosce a questo strumento anche la funzione di ricerca del latitante, mentre dall'art. 226 disp. att. c.p.p.[202] si desume la funzione preventiva.

Quanto al parametro convenzionale, l'art. 8 CEDU sancisce il diritto di ogni persona al rispetto della vita privata familiare, del suo domicilio e della sua corrispondenza: l'autorità pubblica non può, pertanto, ingerirsi nell'esercizio di questo diritto, salvi i casi in cui l'ingerenza sia prevista dalla legge e si tratti di misura che, in una società democratica, si rende necessaria per la sicurezza nazionale, per la pubblica sicurezza, 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 o per la protezione dei diritti e delle libertà altrui. In base alla giurisprudenza della Corte di Strasburgo, questa norma costituisce il principale parametro di

[200] Sul punto, v. *infra*, capitolo III.

[201] Il c. 3 dell'art. 295 c.p.p. stabilisce che «al fine di agevolare le ricerche del latitante, il giudice o il pubblico ministero, nei limiti e con le modalità previste dagli articoli 266 e 267, può disporre l'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione (*omissis*)», mentre, ai sensi del c. 3-bis, «(*omissis*) il giudice o il pubblico ministero può disporre l'intercettazione di comunicazioni tra presenti quando si tratta di agevolare le ricerche di un latitante in relazione a uno dei delitti previsti dall'articolo 51, comma 3-bis nonché dell'articolo 407, comma 2, lettera a), n. 4».

[202] Secondo l'art. 226 dispp. att. c.p.p., «il Ministro dell'interno o, su sua delega, i responsabili dei Servizi centrali (*omissis*), nonché il questore o il comandante provinciale dei Carabinieri e della Guardia di finanza, richiedono al procuratore della Repubblica presso il tribunale del capoluogo del distretto in cui si trova il soggetto da sottoporre a controllo ovvero, nel caso non sia determinabile, del distretto in cui sono emerse le esigenze di prevenzione, l'autorizzazione all'intercettazione di comunicazioni o conversazioni, anche per via telematica, nonché all'intercettazione di comunicazioni o conversazioni tra presenti anche se queste avvengono nei luoghi indicati dall'art. 614 del codice penale quando sia necessario per l'acquisizione di notizie concernenti la prevenzione di delitti di cui all'art. 407, comma 2, lettera a), n. 4 e 51, comma 3-bis, del codice, nonché quelli di cui all'art. 51, comma 3-quater, del codice, commessi mediante l'impiego di tecnologie informatiche o telematiche (*omissis*)».

riferimento in materia di intercettazioni. Di conseguenza, in tanto esse saranno legittime, in quanto risultino giustificate sulla base dei parametri indicati dal § 2 dell'art. 8 CEDU, quali la legalità, la legittimità dell'obiettivo perseguito, la necessità e la proporzionalità[203]. Bisogna precisare che la tutela offerta dalla norma in discorso opera non soltanto nei confronti delle vittime dirette dell'intrusione, ma anche nei confronti di quelle potenziali, cioè di tutti quei soggetti che possono divenire il bersaglio di una misura restrittiva della libertà di comunicazione. In proposito, è principio consolidato quello per il quale l'intercettazione di conversazioni, *e-mail* e comunicazioni via *internet*, l'acquisizione dei dati esterni alle comunicazioni, la sorveglianza strategica e la sorveglianza via GPS costituiscono ingerenze nel diritto al rispetto della vita privata e della corrispondenza[204].

Anche la Carta europea dei diritti fondamentali (c.d. Carta di Nizza) pone dei limiti allo svolgimento delle attività lesive del diritto alla riservatezza. In particolare, statuisce all'art. 7 che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni e, in conseguenza di ciò, garantisce al successivo art. 8 il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano. Tali dati dovranno essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad altro fondamento legittimo previsto dalla legge. Ogni persona avrà, inoltre, il diritto di accedere ai dati raccolti che riguardino e di ottenerne la rettifica.

6. *I presupposti per intercettare*

Dato che la materia delle intercettazioni si pone al crocevia di diversi interessi tra loro in conflitto, occorre, prima di prendere in considerazione la disciplina in chiave dinamica, esaminarne, in chiave statica, i presupposti. Di fronte all'irreparabile pregiudizio che viene a subire la riservatezza per effetto dell'impiego di questo insidioso strumento captativo[205],

[203] Corte e.d.u., 10 febbraio 2009, *Iordachi c. Moldavia*; 9 gennaio 2001, *Natoli c. Italia*; 23 settembre 1998, *McLeod c. Regno Unito*.

[204] Corte e.d.u., 25 marzo 1998, *Kopp c. Svizzera*.

[205] Si pensi, a titolo di esempio, a tutte quelle persone, non indagate, che si trovino a riferire vicende personali nel corso della comunicazione intercettata o alla stessa persona sottoposta ad indagini che narri fatti privati non attinenti a quelli oggetto delle stesse.

appare infatti quant'altri mai opportuna una puntuale predeterminazione dei requisiti in presenza dei quali è consentito il ricorso ad esso. In proposito, bisogna segnalare come, malgrado i ripetuti interventi normativi che si sono susseguiti, questi ultimi abbiano resistito nel tempo, rimanendo sostanzialmente inalterati.

Anzitutto, è necessario che si proceda per uno dei reati indicati all'art. 266 c.p.p. Attraverso l'impiego di criteri quantitativi e qualitativi, il legislatore realizza un bilanciamento in astratto, contemplando, accanto a fattispecie di particolare gravità – come i delitti dolosi o preterintenzionali puniti con una pena superiore nel massimo a cinque anni –, reati meno gravi ancorché odiosi o rispetto ai quali l'intercettazione costituisce uno strumento di indagine assai penetrante – come la minaccia, l'usura, l'abusiva attività finanziaria o la molestia. Il catalogo è stato arricchito nel 2020[206]con l'indicazione dei delitti commessi avvalendosi delle condizioni tipiche dell'associazione mafiosa o al fine di agevolare l'attività di siffatte associazioni, mentre, ai sensi dell'art. 266-bis c.p.p., l'intercettazione del «flusso di comunicazioni relativo a sistemi informatici o telematici» è consentita nei procedimenti concernenti sia i reati di cui all'art. 266 c.p.p. sia i reati «commessi mediante l'impiego di tecnologie informatiche o telematiche», in quanto si tratta di reati compiuti con strumenti particolarmente insidiosi.

In secondo luogo, l'art. 267 c.p.p. individua il requisito probatorio dei "gravi indizi di reato". Occorre precisare che, in questa sede, il termine "indizi" non è inteso nel senso di "prova indiziaria", ma di ragionevole probabilità di sussistenza di un fatto di reato. Inoltre, gli "indizi" debbono attenere alla sussistenza del reato e non alla colpevolezza di un determinato individuo, ben potendo così essere sottoposta ad intercettazione anche l'utenza di un soggetto diverso dalla persona sottoposta alle indagini, purché vi sia comunque un collegamento tra il c.d. bersaglio ed il reato. In definitiva, a differenza di quanto è previsto per le misure cautelari, ove si fa riferimento al requisito dei «gravi indizi di colpevolezza», non è richiesta, per intercettare, la prova dell'attribuibilità del reato ad una determinata persona.

Da ultimo, lo stesso art. 267 c.p.p. stabilisce l'ulteriore presupposto dell'assoluta indispensabilità per la prosecuzione delle indagini, necessità investigativa che ha luogo nei casi in cui non sia possibile acquisire la prova con mezzi diversi dall'intercettazione.

---

[206] L. 28 febbraio 2020, n. 7.

Il c. 2 dell'art. 266 c.p.p. stabilisce poi che, negli stessi casi di cui al c. 1, è consentita l'intercettazione di comunicazioni tra presenti, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile: si tratta del primo riconoscimento legislativo di questo strumento assai incisivo sdoganato dalla giurisprudenza[207]. Su un piano generale, quindi, il legislatore ha scelto di rendere teoricamente applicabile il captatore informatico per tutti i reati intercettabili in via ordinaria. Nel caso in cui le intercettazioni ambientali vengano effettuate in abitazioni o altri luoghi di privata dimora (art. 614 c.p.) la norma prevede un quarto requisito, ovvero il fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa.

È infine opportuno segnalare i termini di durata dell'intercettazione, che non può superare i quindici giorni, ma può essere prorogata dal giudice con decreto motivato su richiesta del pubblico ministero per periodi successivi di quindici giorni, qualora permangano i presupposti indicati (art. 267, c. 3 c.p.p.).

Se quanto illustrato vale in relazione ai procedimenti per reati "comuni", una disciplina derogatoria è prevista per i reati di criminalità organizzata o equiparati: è il caso della minaccia col mezzo del telefono (art. 13 d.l. 1991 n. 152), del terrorismo anche internazionale (art. 407, c. 2 lett. a) n. 4 c.p.p.; art. 3 d.l. 2001 n. 374; artt. 270-ter e 280-bis c.p.), dei delitti contro la libertà individuale (art. 9, legge 2003 n. 228; artt. 600-604 c.p.), nonché, a seguito della l. n. 3 del 2019, dei delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni. Rispetto a questi reati più tenui sono i requisiti probatori, in quanto l'intercettazione è ammessa quando vi sono "sufficienti" indizi di reato (e non "gravi" indizi di reato) e quando l'intercettazione è "necessaria" (e non "indispensabile") per lo svolgimento delle indagini. Anche i termini di durata sono superiori, non potendo l'intercettazione superare i quaranta giorni, termine prorogabile dal giudice per periodi successivi di venti giorni. Un'ultima diversità attiene alle c.d. intercettazioni ambientali: infatti, nei procedimenti per i reati di criminalità organizzata o ad essi equiparati, le intercettazioni tra presenti, che avvengono nel domicilio privato, sono consentite sempre, a prescindere che vi sia motivo di ritenere che ivi si stia svolgendo l'attività criminosa (art. 13 d.l. 1991, n. 152). Come si vede, pertanto, introducendo questi requisiti speciali di ammissibilità per le intercettazioni relative ai

[207] Cass., sez. un., 28 aprile 2016, n. 26889, Scurato.

procedimenti per determinati gravi delitti, i *conditores* hanno dato vita ad un vero e proprio "binario privilegiato" di utilizzo dell'intercettazione.

7. *La normativa previgente sulle intercettazioni*

Come ebbe a dire Franco Cordero, quella delle intercettazioni costituisce una «materia incandescente»[208]: ciò trova conferma negli innumerevoli disegni di legge governativi, volti a novellare questo tormentato mezzo di ricerca della prova, che si sono susseguiti dalla metà degli anni Novanta in ogni legislatura[209], tutti conclusi in un nulla di fatto. Questa circostanza testimonia la profonda inadeguatezza della disciplina dettata dal legislatore del 1988 in materia e rafforza il convincimento che «quello dei mezzi di ricerca della prova tecnologici sia il terreno sul quale i riformatori hanno dimostrato in maniera lampante di non essere riusciti a porre le basi per affrontare le sfide che si sarebbero poste a cavallo del nuovo millennio»[210]. Non è un mistero, del resto, che gli architetti del codice Vassalli abbiano trascurato che una fitta schiera di "idrovore tecnologiche"[211] sempre più sofisticate avrebbe, in breve tempo, scalzato la testimonianza dal ruolo di prova regina, così come che essi abbiano completamente tralasciato di dare ai nuovi mezzi di ricerca della prova atipici una disciplina. Lo scenario appare anche più desolante se si considera la stasi dei dieci anni successivi, quando la crescente importanza della prova tecnologica era divenuta questione non più opinabile. Così, «senza cogliere la straordinaria opportunità di dettare le regole fondamentali e le garanzie di un gioco che sempre più spesso di giocava su un campo diverso, con strumenti ben più insidiosi e capaci di incidere nel nucleo più intimo dei soggetti partecipanti»[212], il legislatore costituzionale del 1999 si è limitato scolpire alcuni principi

[208] F. CORDERO, *Privacy viziosa*, in ID, *L'opera italiana da due soldi*, Torino, 2012, p. 44.

[209] In ordine cronologico, il d.d.l. C. n. 2773, presentato dal Ministro della giustizia Flick alla Camera dei Deputati il 27 novembre 1996; il d.d.l. C. n. 3612, presentato dal Ministro della giustizia Castelli alla Camera dei Deputati il 29 settembre 2005; il d.d.l. C. n. 1638, presentato dal Ministro della giustizia Mastella alla Camera dei Deputati il 14 settembre 2006; il d.d.l. C. n. 1415, presentato dal Ministro della giustizia Alfano alla Camera dei Deputati il 30 giugno 2008.

[210] M. GIALUZ, *Premessa,* cit., p. 1.

[211] A paragonare le intercettazioni a "idrovore foniche", che tutto indiscriminatamente captano, è G. GIOSTRA, *I mali della libertà di stampa si curano solo con più libertà*, in AA. VV., *Ddl Alfano: se lo conosci lo eviti*, Roma, 2009, p. 102.

[212] M. GIALUZ, *Premessa,* cit., p. 1.

sedimentati nel processo passato e ormai inidonei ad intercettare le sfide poste dal progresso tecnologico.

Tanto premesso, prima di entrare nel merito dell'evoluzione normativa che ha interessato lo strumento delle intercettazioni, è forse opportuno tracciare, per sommi capi, lo "scheletro" della sua disciplina, ripercorrendo le tappe essenziali del procedimento che permette di disporre ed eseguire le intercettazioni. È questo «un vero e proprio sotto-procedimento che viene gestito parallelamente alle investigazioni c.d. tradizionali operate mediante gli strumenti classici delle perquisizioni, ispezioni e sequestri»[213]. Si distinguono, in particolare, il procedimento esecutivo ordinario, normato all'art. 267, c. 1 c.p.p., e il procedimento esecutivo d'urgenza, contemplato invece dal c. 2 della medesima disposizione. Come si è detto, il pubblico ministero deve chiedere al g.i.p. l'autorizzazione a disporre le intercettazioni, trasmettendogli gli atti dai quali si ricava l'esistenza dei presupposti per le stesse; l'autorizzazione viene concessa dal giudice con decreto motivato quando ricorrono i gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini. Segue l'emanazione del c.d. decreto esecutivo del pubblico ministero, con il quale fissa le modalità e la durata delle operazioni (art. 267, c 3 c.p.p.): a tal proposito, sono intercettabili sia le utenze riferibili agli indagati, sia quelle riferibili ai testimoni, sia, infine, le utenze riferibili a persone estranee ai fatti, quando queste ultime possono essere destinatarie di comunicazioni provenienti da indagati o da testimoni[214].

Il procedimento d'urgenza è regolato dall'art. 267, c. 2 c.p.p., a norma del quale, in caso di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini[215], l'intercettazione è disposta dal pubblico ministero, che deve comunicare il relativo decreto motivato al giudice non oltre ventiquattro ore decorrenti dal proprio provvedimento. Il giudice, entro le quarantotto ore successive, decide sulla convalida con decreto motivato, in difetto della quale l'intercettazione non può essere proseguita ed i risultati non possono essere utilizzati.

Venendo alla fase di esecuzione, le operazioni di intercettazione risultano così distribuite:

---

[213] P. TONINI, *op. cit.*, p. 391-392.

[214] È il caso, ad esempio, delle indagini sui sequestri di persona a scopo di estorsione, in cui possono essere messi sotto controllo anche i telefoni dei familiari o dei conoscenti della persona sequestrata, totalmente estranei ai fatti per i quali si procede.

[215] L'esempio è nuovamente quello del sequestro di persona a scopo di estorsione.

a) la captazione è compiuta presso l'operatore telefonico;
b) la registrazione è svolta presso la procura della Repubblica
c) l'ascolto è effettuato presso gli uffici di polizia giudiziaria con redazione di verbali sommari contenenti le comunicazioni (c.d. brogliacci d'ascolto)

Secondo il c. 4 dell'art. 267 c.p.p., il pubblico ministero procede alle operazioni personalmente ovvero avvalendosi di un ufficiale di polizia giudiziaria. L'art. 268, c. 3 c.p.p. chiarisce poi che queste possono essere compiute esclusivamente per mezzo degli impianti installati nella procura della Repubblica, salvo che risultino insufficienti o inidonei e sussistano eccezionali ragioni d'urgenza, circostanza nella quale il pubblico ministero, con provvedimento motivato, può disporne il compimento mediante impianti di pubblico servizio o presso la polizia giudiziaria. La *ratio* di questa previsione risiede nella necessità di assicurare un controllo immediato e diretto del pubblico ministero sull'esecuzione delle operazioni, onde prevenire eventuali abusi degli operatori di polizia giudiziaria, anche se, nella prassi, non sono infrequenti le eccezioni, avallate dal tenore letterale dello stesso comma 3. Quanto alla documentazione, l'art. 268, c. 2 c.p.p. prevede che nel verbale sia trascritto, anche sommariamente, il contenuto delle comunicazioni intercettate: tali trascrizioni prendono tradizionalmente il nome di brogliacci d'ascolto, connotati da una funzione provvisoria e riassuntiva del contenuto delle comunicazioni stesse.

L'ultima fase è quella di selezione e trascrizione del captato: si tratta della fase maggiormente incisa dalle riforme che hanno interessato la disciplina delle intercettazioni, ragione per la quale verrà compiutamente affrontata in occasione dell'esame di queste ultime. A tal proposito, si può sin d'ora rilevare come il susseguirsi delle iniziative riformistiche abbia determinato, dal punto di vista del diritto intertemporale, la convivenza di due distinti regimi normativi, dei quali il primo, che continua a seguire la disciplina originaria del codice del 1988, si applica ai procedimenti iscritti fino al 31 agosto 2020, mentre il secondo interesserà quelli iscritti dopo tale data.

Nel delineare i punti salienti dalla "vecchia" normativa[216], qualche considerazione di ordine storico si impone. Apparse per la prima volta nel codice del 1913 e riproposte in veste

[216] Si vedano, in particolare, E. APRILE-F. SPIEZIA, *Le intercettazioni telefoniche e ambientali: innovazioni tecnologiche e nuove questioni giuridiche*, Milano, 2004; A. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996; L. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997; V. GREVI, *La nuova disciplina delle intercettazioni telefoniche*, Milano, 1982; G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Milano, 1983; O. MAZZA (a cura di), *Le nuove intercettazioni*, Torino, 2018; C. PARODI, *Le intercettazioni: profili operativi e giurisprudenziali*, Torino, 2002.

pressoché immutata nel codice del 1930, le intercettazioni erano originariamente contemplate da norme lacunose e sprovviste di garanzie, che attribuivano alla polizia giudiziaria una competenza praticamente illimitata. Il quadro muta sensibilmente con l'avvento della Carta fondamentale, che «costruisce la segretezza delle comunicazioni come uno dei diritti più forti dell'intero ordinamento»[217], e ciò «non perché la *privacy* occupi, in un'ipotetica scala di valori, un gradino superiore rispetto alla libertà personale o domiciliare, ma perché sono molto diverse le tecniche di compressione di questi diritti»[218]. Si deve, tuttavia, attendere il 1955 perché venga imposto l'obbligo di un decreto motivato dell'autorità giudiziaria per disporre l'intercettazione[219]. Poco dopo, la Corte costituzionale interviene con una celebre sentenza[220] con la quale, oltre a chiarire i parametri che debbono guidare l'autorità giudiziaria nella decisione sul provvedimento autorizzativo, opera una delicata ricostruzione dell'intero istituto, indicandone le doverose cautele. Nel 1974[221] i moniti del Giudice delle leggi vengono recepiti dal legislatore, il quale, però, si ritrova molto presto costretto ad una brusca sterzata a seguito dei dilaganti fenomeni eversivi. In questo contesto si insinua la novella del 1978[222]: fra gli aspetti più significativi dell'intervento si segnalano la possibilità di prorogare per un numero imprecisato di volte i quindici giorni originariamente previsti come limite temporale alla durata delle operazioni, l'introduzione dell'autorizzazione in forma orale, l'utilizzabilità dei risultati delle intercettazioni anche in procedimenti diversi da quelli per i quali le notizie sono state raccolte e la previsione dell'intercettazione c.d. preventiva. Dopo la svolta in senso autoritario degli anni di piombo, le nuove questioni, poste negli ultimi decenni dalle intercettazioni, hanno interessato essenzialmente il loro rapporto con l'organo inquirente, atteso che «da modo per sviluppare e confermare ipotesi formulate sulla base di altri accertamenti, la captazione segreta di colloqui riservati sta diventando, sempre più spesso, un punto di partenza delle indagini»[223].

[217] A. CAMON, *Le intercettazioni nel processo penale*, cit., p. 2.

[218] *Ibidem*, p. 3.

[219] Cfr. l'art. 7 della l. 18 giugno 1955, n. 517.

[220] Corte cost., 6 aprile 1973, n. 34.

[221] L. 8 aprile 1974, n. 98.

[222] Il riferimento è al d.l. 21 marzo 1978, n. 59 (conv. in l. 18 maggio 1978, n. 191), emanato, com'è noto, cinque giorni dopo il sequestro dell'on. Moro.

[223] A. CAMON, *Le intercettazioni nel processo penale*, cit., p. 6 e 7.

Si può osservare *ictu oculi* come il codice del 1988 abbia innovato rispetto al sistema previgente, introducendo il contraddittorio sugli esiti delle intercettazioni e riconoscendo così il potere al difensore dell'indagato, che può esaminare le registrazioni e gli atti autorizzativi, di chiedere al giudice l'acquisizione di quelle considerate rilevanti per la causa, al pari del pubblico ministero. Secondo la formulazione originaria dell'art. 268, c. 4 c.p.p., la registrazione delle intercettazioni ed i "verbali sommari" sono trasmessi al pubblico ministero per un controllo preliminare sulla loro ostensibilità. Solo nel caso in cui possa derivare un grave pregiudizio per le indagini, il pubblico ministero chiede al giudice per le indagini preliminari l'autorizzazione al differimento del deposito, che non può comunque avere luogo oltre la chiusura delle indagini, fattispecie che si verifica sovente nella prassi, ove il deposito viene effettuato al momento dell'avviso di conclusione delle indagini[224]. A questo punto, i difensori hanno la possibilità di operare un controllo sulla rilevanza ed utilizzabilità delle intercettazioni: il c. 6 dell'art. 268 c.p.p. prevede, infatti, che, in caso di deposito, è dato immediato avviso ai difensori delle parti private, che hanno facoltà di esaminare gli atti e ascoltare le registrazioni – ma senza poterne fare copia – entro il termine fissato dal pubblico ministero.

Coerentemente con il modello accusatorio, il pubblico ministero e le parti private hanno l'onere di chiedere al giudice per le indagini preliminari l'acquisizione delle intercettazioni: il giudice fissa, quindi, la data dell'udienza – denominata nella prassi "di stralcio" – di cui fa dare avviso alle parti almeno ventiquattro ore prima. È questa un'udienza in contraddittorio, alla quale non si applicano le regole della camera di consiglio: il giudice, che ha un limitato potere di filtro, deve stralciare le registrazioni di cui sia vietata l'utilizzazione e, dall'altro lato, disporre l'acquisizione di quelle indicate dalle parti che «non appaiano manifestamente irrilevanti». In realtà, si registra nel "diritto vivente" una certa desuetudine dell'udienza di stralcio, in quanto questa si tiene soltanto se le parti chiedono l'ammissione della singola intercettazione; ne consegue che, ove le parti non si attivino, lo stralcio non avviene e si dovrà quindi attendere il dibattimento, momento in cui potranno essere richiesti sia lo stralcio sia l'ammissione e la trascrizione delle singole intercettazioni. Ai sensi dell'art. 268, c. 7 c.p.p., il giudice dispone la trascrizione integrale delle registrazioni che ha ammesso, osservando le forme, i modi e le garanzie previste per l'espletamento delle

[224] La giurisprudenza ammette che il deposito dei verbali e delle registrazioni avvenga unitamente a tutti gli altri atti di indagine; si veda Cass., sez. V, 11 aprile 2003, Gualtieri, in *Cass. pen.*, 2004, 2921: «ove sia stato autorizzato il ritardo sino alla conclusione delle indagini preliminari», il termine di cui all'art. 268, c. 5 «coincide con quello di cui all'art. 415-bis stesso codice, sicché si fa luogo ad un unico deposito».

perizie. A tal fine, i difensori sono avvisati delle operazioni, alle quali possono prendere parte mediante consulenti di parte, e successivamente potranno estrarre copia delle trascrizioni effettuate dall'esperto e fare eseguire la trasposizione della registrazione su nastro magnetico[225]. Le trascrizioni debbono essere inserite nel fascicolo per il dibattimento.

Di regola, i verbali e le registrazioni di tutte le intercettazioni, acquisite o non acquisite al procedimento, sono conservati integralmente preso il pubblico ministero che ha disposto l'intercettazione fino al passaggio in giudicato della sentenza. È, tuttavia, possibile ottenerne la distruzione anticipata, qualora si tratti di elementi non necessari ai fini del procedimento: ai sensi dell'art. 269, c. 2 c.p.p., ogni persona interessata può quindi chiedere al giudice, che ha autorizzato o convalidato l'operazione di intercettazione, la distruzione della registrazione che la riguarda, a tutela della propria riservatezza. La decisione viene assunta nel contesto di un'udienza camerale e le successive operazioni di distruzione, di cui è redatto verbale, vengono eseguite sotto il controllo del giudice.

Occorre tenere presente che la disciplina di conservazione e distruzione appena esposta si applica alle intercettazioni legittimamente acquisite, mentre, per quelle acquisite in violazione di divieti probatori – dunque inutilizzabili a prescindere dalla loro efficacia dimostrativa – vale quanto previsto dall'art. 271 c.p.p. La norma, nella sua formulazione originaria, contempla i seguenti casi di inutilizzabilità procedurali:

a) quando le intercettazioni sono state eseguite «fuori dei casi consentiti dalla legge»[226], cioè nelle ipotesi non previste dagli artt. 266, 266-bis, 295, c. 3;
b) quando non sono state osservate le disposizioni dell'art. 267, cioè le intercettazioni sono state compiute in spregio dei presupposti e delle forme del provvedimento di autorizzazione e di esecuzione;
c) quando non sono stati osservati i commi 1 e 3 dell'art. 268, cioè le intercettazioni sono state compiute senza registrare la comunicazione e senza redigere il verbale sommario delle operazioni; oppure sono state compiute al di fuori degli impianti installati nella procura della Repubblica in difetto di motivate ragioni di urgenza.

[225] Ovviamente la disposizione del codice del 1988 è eseguita tenendo presente che ormai tutte le registrazioni sono incorporate con modalità digitali.

[226] Per quanto la lettera dell'art. 271 c.p.p. sanzioni con l'inutilizzabilità le intercettazioni che «siano state eseguite fuori dei casi consentiti dalla legge», la Cassazione ritiene che, qualora le intercettazioni siano state originariamente disposte per uno dei reati previsti dall'art. 266 c.p.p., esse restino legittime anche quando l'addebito venga successivamente derubricato in un reato che non avrebbe legittimato il ricorso a tale mezzo di ricerca della prova. Cfr., in proposito, Cass., sez. VI, 20 ottobre – 31 dicembre 2009, in *Arch. n. proc. pen*., 2013, 3, 317.

Nei casi *sub-c)*, come anche rilevato dalla Corte costituzionale[227], si tratta di comunicazioni non sottoposte a divieto assoluto di captazione e che avrebbero potuto essere legittimamente intercettate nel rispetto della corretta procedura prevista dal codice: in ragione di ciò, pur nel silenzio dell'art. 271 c.p.p. in ordine alle modalità procedurali da seguire per la distruzione, l'orientamento prevalente in giurisprudenza è nel senso della necessarietà di un'udienza camerale, da svolgersi nel contradditorio fra le parti.

Per quanto riguarda l'utilizzo di intercettazioni in procedimenti diversi da quelli nei quali sono state disposte, la versione originaria dell'art. 270, c. 1 c.p.p. si esprime in termini negativi, salvo che risultino indispensabili per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza[228]. Rispetto a questi reati, i verbali e le registrazioni delle intercettazioni eseguite altrove sono depositati presso l'autorità competente per il diverso procedimento e trovano applicazione le norme in tema di udienza di stralcio e trascrizione di cui al richiamato art. 268, c. 6, 7 e 8. Infine, il pubblico ministero e i difensori hanno facoltà di esaminare i verbali e le registrazioni depositate nel procedimento in cui le intercettazioni furono autorizzate.

8. *La l. n. 103/2017 (c.d. riforma Orlando)*

Dopo decenni di estenuanti dibattiti, nel 2017 i tempi sembravano maturi per mettere mano ad una riforma organica sulle intercettazioni. Sulla scorta delle direttive di delega contenute nella l. 23 giugno 2017, n. 103[229], veniva, quindi, adottato il d.lgs. 29 dicembre 2017, n. 216[230], il quale, oltre a riformare l'istituto, disciplinava, per la prima volta,

[227] Corte cost. n. 1 del 2013.

[228] Il c. 1 è stato modificato dal d.l. 30 dicembre 2019, n. 161, convertito con modifiche dalla l. 28 febbraio 2020, n. 7. Per un esame più approfondito, v. *infra*, Capitolo IV.

[229] In proposito, cfr. R. APRATI, *La delega della riforma Orlando in tema di intercettazioni*, in *Il libro dell'anno del diritto 2018*, all'indirizzo <http://www.treccani.it/enciclopedia/la-delega-della-riforma-orlando-in-tema-di-intercettazioni_%28Il-Libro-dell%27anno-del-Diritto%29/>; T. BENE, *La legge delega per la riforma delle intercettazioni*, in A. SCALFATI (a cura di), *La riforma della giustizia penale*, Torino, 2017, p. 289 ss.; C. CONTI, *La riservatezza delle intercettazioni nella "delega Orlando"*, in *Dir. pen. cont. – Riv.Trim.*, 2017, p. 78 ss.; A. CISTERNA, *Intercettazioni: i rischi di una delega troppo generica*, in *Guida dir.*, 2017, 32, p. 65.

[230] Sul quale si vedano, fra gli altri, T. BENE (a cura di), *L'intercettazione di comunicazioni*, Bari, 2018; G. GIOSTRA-R. ORLANDI, *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018; S. BUZZELLI, *Le nuove intercettazioni tra selettività arbitraria*

l'insidioso mezzo del captatore informatico, in precedenza regolato soltanto in via giurisprudenziale. Scopo dichiarato della legge delega era quello di «tutelare l'efficienza delle indagini e la riservatezza sia delle persone intercettate occasionalmente, sia dei destinatari delle intercettazioni quando fossero state captate conversazioni relative a fatti privati non rilevanti per le indagini»[231]. La c.d. riforma Orlando andava così a imporre alla polizia giudiziaria, diretta dal pubblico ministero, una selezione immediata delle dichiarazioni non rilevanti; si prevedeva, quindi, di ritardare l'acquisizione delle intercettazioni al momento in cui il giudice, in contraddittorio, avesse definitivamente valutato i dialoghi captati come rilevanti per le indagini o, comunque, non manifestamente irrilevanti, mentre tutte le intercettazioni sarebbero state custodite, nel frattempo, in un archivio riservato, posto sotto la responsabilità del procuratore della Repubblica, e coperte da segreto. Per l'effetto, era escluso che i verbali sommari potessero essere pubblicati, anche solo a titolo di notizia generica, fino a quanto il giudice non li avesse valutati come rilevanti per l'accertamento del reato.

Fin da subito, il nuovo sistema si risultò alquanto farraginoso e cadde, per questo, sotto le pressanti critiche di magistratura, avvocatura e dottrina[232]. Quanto alla tutela della riservatezza, la riforma veniva tacciata di impedire al pubblico ministero un controllo pieno sulle scelte probatorie, che finivano per essere rimesse integralmente alla polizia giudiziaria; per altro verso, si poneva il rischio di pregiudicare il diritto alla prova spettante all'indagato proprio a cagione dell'effettiva difficoltà di operare un vaglio in tempi brevi su un materiale pressoché sterminato. Né può essere trascurata l'accusa, avanzata dal Ministro della giustizia alla riforma Orlando, di aver messo «un bavaglio all'informazione»: il ritardo dovuto all'attesa di una valutazione definitiva di rilevanza da parte del giudice andava infatti a colpire la possibilità per i giornali e le televisioni di pubblicare immediatamente tutte le

e ridimensionamento delle garanzie difensive, in *La rivista di diritto dei media*, 2018, p. 214 ss.; A. CAMON, *Primi appunti sul nuovo procedimento d'acquisizione dei risultati delle intercettazioni*, in *Arch. pen.*, 2018, p. 449 ss.; C. CONTI, *Le nuove norme sulla riservatezza delle intercettazioni: anatomia di una riforma discussa*, *Giur. it.*, 2018, p. 1754 ss.; L. FILIPPI, *Attuazione della delega sulle intercettazioni. Un'altra occasione mancata*, in *il Penalista*, 2018; F. GIUNCHEDI, *Appunti su alcune criticità della nuova disciplina delle intercettazioni*, in *Arch. pen.*, 2018, 513 ss.; O. MAZZA, *Amorfismo legale e adiaforia costituzionale nella nuova disciplina delle intercettazioni*, in *Proc. pen. giust.*, 2018, p. 683 ss.

[231] P. TONINI, *op. cit.*, p. 403.

[232] Sulle critiche avanzate alla c.d. riforma Orlando si vedano, in particolare, L. FILIPPI, *Intercettazioni: una riforma complicata e inutile*, in *Dir. pen. proc.*, 2018, p. 305; G. GIOSTRA, *Su intercettazioni e segreto una disciplina impraticabile*, in *Il Sole 24 Ore*, 20 dicembre 2017, p. 33, nonché, più ampiamente, ID., *Il segreto estende i suoi confini e la sua durata*, in G. GIOSTRA-R. ORLANDI, *Nuove norme in tema di intercettazioni*, cit., p. 115 ss.

conversazioni captate, impedendo *scoop* economicamente e politicamente scottanti. A ciò si aggiungevano le censure avanzate alla disciplina concernente l'utilizzo del captatore informatico, alla quale si imputava di non aver regolamentato i plurimi e controversi impieghi di questo strumento di *law enforcement*[233]. Differita così l'entrata in vigore della riforma Orlando – fissata per il 26 luglio 2018 – al 31 marzo 2019[234], poi al 31 luglio 2019[235], quindi al 31 dicembre 2019[236], questa non ha mai formalmente visto la luce, essendosi il Governo risolto ad intervenire, non senza accese polemiche[237], con il d.l. 30 dicembre 2019, n. 161, intitolato «Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni».

Operando una ricognizione dei contenuti della legge delega del 2017, il provvedimento normativo articola i criteri e le direttive in cinque punti[238]: riservatezza, sanzioni penali, tutela della libertà di stampa e diritto di informazione, reati contro la p.a., captatori informatici.

In via principale, la delega "investe" sul pubblico ministero, al quale spetta di assicurare la riservatezza dei dati inutilizzabili o, comunque, irrilevanti rispetto ai fatti in corso di accertamento[239]: tali informazioni, da conservarsi in apposito archivio riservato e accessibile ai soli difensori (ma con sola facoltà di esame e di ascolto e non già di copia)[240], non potranno essere allegate, in ragione della loro presunta inutilità, alla richiesta di applicazione delle misure cautelari. Allo stesso pubblico ministero compete altresì l'obbligo di avviare la procedura di selezione del materiale, all'esito della quale soltanto cadrà il divieto di cui all'art. 114 c.p.p., con conseguente possibilità di ottenere la copia degli atti e richiedere la trascrizione delle intercettazioni qualificate come rilevanti dal g.i.p. o di quelle il cui rilascio

[233] A riguardo, v. L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, in G. GIOSTRA-R. ORLANDI, *Nuove norme in tema di intercettazioni*, cit., p. 290.

[234] Art. 2 d.l. 25 luglio 2018, n. 91.

[235] Art. 1, c. 1139, lett. *a*, l. 30 dicembre 2018, n. 145.

[236] Art. 9, c. 2, d.l. 14 giugno 2019, n. 53.

[237] In senso critico rispetto all'uso dello strumento del decreto-legge, W. NOCERINO, *Prime riflessioni a margine del nuovo decreto legge in materia di intercettazioni*, in *Sist. pen.* 2020/1, p. 64; A. SCALFATI, *Intercettazioni: spirito autoritario, propaganda e norme inutili*, in *Arch. pen.* web, 2020, p. 1.

[238] Art. 1, co. 84, lett. *a*, *b*, *c*, *d*, *e*.

[239] C. 84, lett. *a*), n. 1.

[240] C. 84, lett. *a)*, n. 2.

sia stato autorizzato dal giudice dopo la conclusione delle indagini[241]. Qualora si determini per la richiesta di rinvio a giudizio, il pubblico ministero dovrà quindi disporre la procedura, chiedendo lo stralcio delle comunicazioni inutilizzabili[242]. La polizia giudiziaria non potrà invece procedere, qualora emergano nella compilazione dei verbali d'ascolto informazioni inutilizzabili o sensibili e non pertinenti o irrilevanti, alla loro sommaria trascrizione, essendo fatto obbligo in capo ad essa di indicare soltanto data, ora e apparato da cui proviene la registrazione; di tale circostanza dovrà, nondimeno, informare il pubblico ministero, il quale potrà con decreto motivato autorizzare le trascrizioni dei dati che qualifichi come rilevanti[243].

Il c. 84, lett. *b)* prevede, invece, la formulazione di un nuovo delitto, consistente nella «diffusione, al solo di fine di recare danno alla reputazione o all'immagine altrui, di riprese visive o di registrazioni di conversazioni, anche telefoniche, svolte in sua presenza ed effettuate fraudolentemente», in relazione al quale la punibilità viene esclusa laddove la registrazione o le riprese siano utilizzate nell'ambito di un procedimento amministrativo o giudiziario ovvero per l'esercizio del diritto di difesa o del diritto di cronaca.

Infine, dopo alcuni generici richiami alla CEDU e alla relativa giurisprudenza[244], il c. 84, lett. *e*) passa a regolare, con indicazioni puntuali, l'utilizzo del captatore informatico. In proposito, si richiede che la registrazione sia attivata da apposito pulsante e non avvenga, pertanto, in maniera automatica con l'installazione del *virus*; al fine di poter controllare e gestire le registrazioni a distanza, il verbale delle operazioni dovrà riportare la data e l'ora di inizio e di conclusione delle registrazioni stesse. Quanto ai presupposti, il captatore potrà sempre essere utilizzato per i reati di cui all'art. 51, c. 3-bis e 3-quater c.p.p., mentre, per quelli dell'art. 266, c. 1 c.p.p., le intercettazioni di comunicazioni fra presenti in luoghi domiciliari dovranno presupporre che l'attività criminale sia in corso di svolgimento. Il decreto di autorizzazione indicherà, in ogni caso, il motivo per cui si rende necessario l'impiego di tale strumento. Accanto ad alcune indicazioni di carattere tecnico[245], la legge

[241] C. 84, lett. *a*), n. 3.

[242] C. 84, lett. *a*), n. 4.

[243] C. 84, lett. *a*), n. 5.

[244] Il c. 84, lett. *c)* e *d)* della delega invita a tenere conto della Convenzione e della relativa giurisprudenza a tutela della libertà di stampa e del diritto all'informazione, nonché a semplificare l'impiego delle intercettazioni per i più gravi reati contro la p.a. dei pubblici ufficiali.

[245] Si prevede, in particolare, che il trasferimento delle registrazioni debba essere predisposto automaticamente ed esclusivamente verso il *server* della Procura e che, al termine delle operazioni, il

delega estende poi alle intercettazioni raccolte con il captatore informatico alcune regole processuali concepite per le intercettazioni "classiche", seppur non senza qualche peculiarità. In caso di atti urgenti, l'utilizzo del captatore informatico può essere autorizzato dal pubblico ministero solo per i reati di cui all'art. 51, c. 3-bis e 3-quater c.p.p.: in tal caso, dovrà indicare, nel decreto di autorizzazione, sia le ragioni dell'urgenza sia la necessità di impiegare il captatore. In relazione all'impiego delle intercettazioni in altri procedimenti, invece, viene estesa la disciplina vigente, cosicché le intercettazioni con captatore informatico saranno utilizzabili in procedimenti diversi solo per i delitti di cui è consentito l'arresto in flagranza, mentre, laddove siano coinvolti soggetti estranei, le registrazioni non saranno divulgabili o pubblicabili in alcun modo.

Non vi è dubbio che filo conduttore della riforma in relazione alle intercettazioni telefoniche sia la tutela della *privacy*[246]. Ciò presuppone una responsabilizzazione di tutti i soggetti processuali: dalla polizia giudiziaria, che non potrà documentare le conversazioni riservate nei brogliacci, al pubblico ministero, che dovrà disporne da solo lo stralcio nel caso in cui chieda una misura cautelare; dai difensori, che non potranno estrarne copia, al giudice, che dovrà ammettere solo le intercettazioni rilevanti e non potrà escludere solo quelle manifestamente irrilevanti. Inoltre, nell'ottica di assicurare una sorta di tutela preventiva, la selezione del materiale andrà fatta, al più tardi, prima dell'invio dell'avviso di conclusione delle indagini preliminari o prima del decreto di giudizio immediato, mentre il rilascio delle copie potrà essere accordato solo rispetto alle intercettazioni rilevanti già selezionate dal giudice nella procedura di stralcio. In definitiva, l'obiettivo è quello che, nel momento in cui scatta il diritto alla copia delle registrazioni, le intercettazioni siano già state oggetto di selezione: solo così potrà essere impedito che circoli materiale suscettibile di nuocere alla *privacy* delle persone.

Circa l'efficace ed effettivo perseguimento della tutela della riservatezza sono state avanzate alcune riserve[247]. In particolare, ci si è interrogati se si sia correttamente bilanciato

dispositivo venga disattivato definitivamente, al fine di garantire la genuinità del materiale captato; i *virus* da installare dovranno inoltre essere conformi a determinati requisiti tecnici, da indicare con decreto ministeriale.

[246] Sul tema, v. L. FILIPPI, *La legge delega sulle intercettazioni*, in G. M. BACCARI-C. BONZANO-K. LA REGINA- E. MANCUSO (a cura di), *Le recenti riforme in materia penale: dai decreti di depenalizzazione (d. lgs. n. 7 e n. 8/2016) alla «legge Orlando» (l. n. 103/2017) e relativi decreti attuativi (3 ottobre 2017)*, Padova, 2017; L. GIORDANO, *La delega per la riforma delle intercettazioni*, in A. MARANDOLA-T. BENE (a cura di), *La riforma della giustizia penale*, Milano, 2017; A. ZAMPAGLIONE, *Delega in materia di intercettazioni: un costante bilanciamento di interessi*, in G. SPANGHER (a cura di), *La riforma Orlando*, Pisa, 2017.

[247] V., in particolare, R. APRATI, *La delega della riforma Orlando.* cit.

il diritto alla riservatezza con il diritto di difesa e, per altro verso, se lo stesso sia avvenuto con riguardo al rapporto tra riservatezza e necessità dell'accertamento penale. In merito alla prima questione, il problema sorge dalla difficoltà per la difesa di poter analizzare a pieno il contenuto delle conversazioni. La scelta di anticipare la selezione del materiale all'avviso di conclusione delle indagini e, al contempo, vietare la copia del materiale intercettato sembra addirittura destare dubbi di legittimità costituzionale in punto di compatibilità con il diritto di difesa, il diritto a tempi ragionevoli per la difesa ed il diritto alla parità fra le parti. Allo stesso tempo, questa soluzione normativa si porrebbe in maniera stridente anche con il *dictum* della Corte costituzionale[248], ad avviso della quale «il diritto all'accesso implica, come naturale conseguenza, quello di ottenere la trasposizione su nastro»: se infatti la lesione del diritto di difesa si potrebbe perfezionare senz'altro nei procedimenti nei quali non si sia fatto ricorso alla cautela, non è da escludere che ciò avvenga pure per i procedimenti in cui sono intervenuti dei provvedimenti cautelari, ben potendo il materiale di cui si è ottenuta copia essere sensibilmente irrisorio rispetto a quello depositato in vista della selezione e dell'acquisizione definitiva[249]. Anche rispetto al secondo quesito non sono mancate le perplessità. A questo riguardo, si segnala il dubbio che il legislatore delegante abbia imposto un adempimento processuale oltremodo gravoso durante le indagini preliminari, suscettibile di generare costi procedimentali troppo alti, oltre che di porre l'indagato nella posizione di lucrare più facilmente la prescrizione[250].

Ben più numerosi sarebbero i profili problematici connessi all'impiego del captatore informatico, che darebbe luogo ad un vero e proprio «pedinamento delle comunicazioni»[251]. Le perplessità[252] riguarderebbero anzitutto la natura di questo strumento intrusivo e polifunzionale. A non convincere è, in effetti, la logica della delega, che, concependolo come

[248] C. cost., 15 ottobre 2008, n. 336.

[249] Cfr. A: GAITO, *I nuovi orizzonti*, in ID. (a cura di), *Riservatezza e intercettazioni tra norma e prassi*, Roma, 2011, p. 213 ss.; C. SANTORIELLO, *Il diritto alla traccia fonica*, *ivi*, p. 225 ss.

[250] R. APRATI, *La delega della riforma Orlando*. cit.

[251] *Ibidem*.

[252] V., sul tema, D. CURTOTTI-W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, in G. M. BACCARI-C. BONZANO-K. LA REGINA- E. MANCUSO (a cura di), *Le recenti riforme in materia penale*, cit.; GIORDANO, *La delega per la riforma del captatore informatico*, in A. MARANDOLA-T. BENE (a cura di), *La riforma della giustizia*, cit.; L. FILIPPI, *La delega in materia di uso del captatore informatico*, in G. SPANGHER (a cura di), *La riforma Orlando*, cit., p. 151 ss.

una mera alternativa alle intercettazioni ambientali effettuate con la classica microspia[253], ne trascura le concrete implicazioni. Invero, la polifunzionalità del captatore informatico può essere apprezzata con riguardo alla tipologia di comunicazioni captate (telefoniche, fra presenti, telematiche), agli apparecchi intercettati (non solo quello infettato, ma anche tutti quelli che si trovano intorno ad esso), ai luoghi (ove inserito in un dispositivo informatico mobile, il captatore segue il suo detentore e registra conversazioni che avvengono in luoghi pubblici, aperti al pubblico, semi-privati, domiciliari), alle persone che registra (il proprietario dell'apparecchio o chiunque altro a cui venga consegnato). Si tratta, in altri termini, di un'intercettazione "itinerante", nell'ambito della quale può rimanere coinvolto chiunque, anche solo accidentalmente, venga a trovarsi nel raggio d'azione dell'apparecchio. Questa attitudine pone in risalto la straordinaria invasività del captatore informatico dal punto di vista della *privacy*: come si è detto[254], «siamo dunque di fronte ad uno strumento che serve per intercettare chi non frequenta luoghi fissi, chi non è abitudinario, chi è accorto e dunque non parla in luoghi consueti, chi non si sa se parlerà a distanza con un apparecchio o di persona». Senonché, appurato che la finalità dello strumento in discorso è quella di rendere possibili le intercettazioni laddove non sia determinabile un "luogo bersaglio" o un "apparecchio bersaglio", non si vede per quale ragione la delega continui a distinguere, per i reati diversi da quelli dell'art. 51, c. 3-bis e 3-quater c.p.p., i presupposti di autorizzazione in base ai luoghi. Questo rappresenta invero il *punctum dolens* della questione. Per contro, «se si parte dal presupposto che il *trojan* è sicuramente un mezzo che ha una potenzialità in più rispetto alle normali intercettazioni, esso dovrebbe allora essere consentito solo nei casi estremi in cui vi è la necessità di realizzare un monitoraggio a 360 gradi e non ci sono le condizioni per prevedere i luoghi o i mezzi in cui e con cui avverranno le comunicazioni»[255]. Pertanto, l'indicazione obbligatoria del motivo per cui si rende necessario il ricorso al captatore – e non l'indicazione dei luoghi – costituisce il fulcro attorno al quale gravita la legge delega: in tanto questo potrà considerarsi l'*extrema ratio* rispetto alle intercettazioni classiche, in quanto venga spiegato il motivo per il quale gli altri strumenti intercettativi risultano inidonei nel caso di specie.

[253] A conferma di ciò, la disciplina ripropone il sistema di un doppio binario, che distingue i reati più gravi, indicati all'art. 51, c. 3-bis e 3-quater c.p.p., dagli altri reati, rispetto ai quali è ammesso l'impiego di tale strumento.

[254] R. APRATI, *La delega della riforma Orlando.* cit.

[255] *Ibidem.*

A questo punto, si tratta di prendere in esame i contenuti del d.lgs. 29 dicembre 2017, n. 216, al fine di vedere come, in concreto, il Governo abbia esercitato la delega conferitagli[256]. Anzitutto, sul piano della tutela della riservatezza, il legislatore delegato è intervenuto con una normativa articolata in cinque punti principali: introduzione del divieto di trascrizione – anche sommaria – di intercettazioni irrilevanti, relative a dati sensibili o intercorse tra indagato e difensore; nuova disciplina in tema di deposito dei verbali e delle registrazioni; introduzione del meccanismo di acquisizione al fascicolo delle indagini; istituzione dell'archivio riservato delle intercettazioni; limiti alla riproduzione delle intercettazioni negli atti cautelari.

Dopo l'art. 268, c. 2 c.p.p., che prevede la trascrizione, anche sommaria, del contenuto delle comunicazioni intercettate, la riforma, attraverso l'introduzione di due ulteriori commi, fa esplicito divieto – pur senza prevedere alcuna specifica sanzione processuale in caso di relativa elusione – di trascrizione, anche sommaria, di tre categorie di comunicazioni o conversazioni: quelle irrilevanti ai fini delle indagini, quelle che riguardino dati personali sensibili[257] e quelle relative alle conversazioni, anche indirette, con i difensori. In questo modo, ogni volta che venga captato un dialogo del quale è fatto divieto di trascrizione anche sommaria, ai sensi del nuovo c. 2-bis dell'art. 268 c.p.p., nel verbale redatto dalla polizia giudiziaria verranno riportati soltanto la data, l'ora ed il dispositivo sul quale l'intercettazione è intervenuta. Tale annotazione, funzionale a lasciare traccia della conversazione in vista della sua futura distruzione ma senza riprodurne il contenuto, consentirà di portare a conoscenza del pubblico ministero la sussistenza di contenuti per i quali vige il divieto di trascrizione anche sommaria. In questo senso depone l'art. 267, c. 4 c.p.p., che, novellato con l'inserimento di un ulteriore periodo, precisa che l'ufficiale di polizia giudiziaria provvede informando preventivamente il pubblico ministero con annotazione sui contenuti delle comunicazioni e conversazioni. Come si intuisce, è al solo pubblico ministero – e non alla polizia giudiziaria – che spetta la facoltà di valutare la rilevanza dell'intercettazione: la disposizione viene così a rendere operativo il disposto di cui al nuovo art. 268, c. 2-ter c.p.p., che rimette al vaglio del *dominus* delle indagini la decisione circa la trascrizione o meno della conversazione. Depositata, quindi, al pubblico ministero l'annotazione di cui all'art. 267, c. 4, ultimo periodo, c.p.p., questi può, con decreto

[256] Si veda, su tutti, D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, in *Dir. pen. cont.*, 2018/1, p. 189 ss..

[257] Definiti tali dall'art. 4, comma 1, lett. d), decreto legislativo 30 giugno 2003, n. 196.

motivato, disporre che le comunicazioni e conversazioni di cui al c. 2-bis vengano trascritte nel verbale, qualora ne valuti la rilevanza per i fatti oggetto di prova. Consentendo al pubblico ministero di recuperare *ex post* le conversazioni che la polizia giudiziaria sospetta di possibile irrilevanza, si istituisce una sorta di doppio binario a seconda che le conversazioni siano giudicate di certa irrilevanza da parte di quest'ultima ovvero di dubbia rilevanza: nella seconda ipotesi, la polizia giudiziaria provvederà a depositare apposita annotazione sui contenuti, alla quale farà seguito il decreto motivato del pubblico ministero che disporrà la trascrizione o l'omessa trascrizione del brano, secondo un giudizio di rilevanza[258].

Una volta scaduto il termine per lo svolgimento delle operazioni[259], la polizia giudiziaria trasmette al pubblico ministero i verbali e le registrazioni per la loro conservazione nell'archivio riservato ai sensi del nuovo art. 268, c. 4 c.p.p. Al pubblico ministero compete, quindi, la scelta tra il deposito degli atti entro il termine di cinque giorni o, come più spesso accade nella prassi, la richiesta di autorizzazione al g.i.p. di ritardare il deposito non oltre la chiusura delle indagini, qualora dal deposito stesso possa derivare un grave pregiudizio per le investigazioni. La vera novità concerne l'oggetto del deposito: in base al nuovo art. 268-bis c.p.p., infatti, unitamente ai verbali e alle registrazioni debbono essere depositate anche le annotazioni disciplinate dall'art. 267, c. 4 c.p.p. ovvero quelle che la polizia giudiziaria trasmette per demandare al pubblico ministero la valutazione di rilevanza di singole intercettazioni ai fini della successiva trascrizione; inoltre, il pubblico ministero è tenuto, in tale sede, a formare l'elenco delle intercettazioni rilevanti ai fini di prova, funzionale alla successiva richiesta al g.i.p. di acquisizione al fascicolo delle indagini. Si abbandona così il sistema previgente, caratterizzato dall'automatica trasmigrazione di tutto il materiale inerente all'intercettazione negli atti d'indagine, in favore di un nuovo sistema, in cui vi rientra solo ciò che è rilevante ai fini del procedimento. Già nella fase del deposito degli atti di intercettazione, pertanto, la difesa potrà conoscere quali siano i progressivi che il pubblico ministero ritenga utili ai fini di prova.

[258] O di necessità, qualora si tratti di dati sensibili.

[259] Nel caso in cui, tuttavia, la prosecuzione delle operazioni renda necessario, in ragione della complessità delle indagini, che l'ufficiale di polizia giudiziaria delegato all'ascolto consulti le risultanze già acquisite, il pubblico ministero può disporre con decreto il differimento della trasmissione dei verbali e delle registrazioni, fissando contestualmente le prescrizioni per assicurare la tutela del segreto sul materiale non trasmesso.

Altra novità della riforma è l'eliminazione della c.d. udienza stralcio[260] e la sua sostituzione con il meccanismo di acquisizione delle intercettazioni al fascicolo delle indagini di cui agli artt. 268-ter e 268-quater c.p.p. Fuori dal caso in cui sia stata adottata una misura cautelare, la riforma prevede che, entro cinque giorni dal deposito, il pubblico ministero presenti al giudice la richiesta di acquisizione delle comunicazioni o conversazioni e dei flussi di comunicazioni informatiche o telematiche contenuti nell'elenco dei progressivi[261] e ne dia contestuale comunicazione ai difensori. Oltre che ad assicurare il pieno esercizio del diritto di difesa, il deposito degli atti relativi alle operazioni di intercettazione e l'elenco dei progressivi, di cui si intenda richiedere l'acquisizione, consente ai difensori di prendere contezza delle circostanze che la pubblica accusa intenda provare e fornisce un valido strumento per impostare la difesa. Si apre così la fase di fase di selezione del materiale intercettivo destinato a confluire nel fascicolo delle indagini e le parti avranno facoltà di interloquire in ordine ai progressivi che intendono acquisire, secondo lo schema del contraddittorio cartolare. Il giudice dispone con ordinanza, emessa in camera di consiglio senza l'intervento del pubblico ministero e dei difensori, l'acquisizione delle conversazioni e comunicazioni indicate dalle parti, salvo che siano manifestamente irrilevanti, e ordina, anche d'ufficio, lo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione. Di regola, quindi, il giudice provvede *de plano,* senza fissare apposita udienza e sulla base del mero contraddittorio cartolare. Ove invece risulti necessario[262], l'ordinanza è emessa all'esito di udienza, alla quale prendono parte il pubblico ministero e i difensori, mentre restano escluse le persone sottoposte alle indagini e le persone offese dal reato. Gli atti ed i verbali oggetto di acquisizione confluiscono nel fascicolo del pubblico ministero, mentre quelli non acquisiti sono immediatamente restituiti, ai sensi dell'art. 268-quater, c. 5, c.p.p., al pubblico ministero per la conservazione nell'archivio riservato. È appena il caso di precisare che i brani acquisiti risultano, nella maggior parte dei casi, già trascritti, anche solo sommariamente, dalla polizia giudiziaria nei relativi verbali; qualora tuttavia vengano acquisite comunicazioni o conversazioni su richiesta dei difensori che non siano state trascritte, il giudice dovrà ordinarne la trascrizione sommaria a cura del pubblico ministero.

[260] Sullo stralcio delle intercettazioni, v. M. F. FEBBRARO, *La procedura di "stralcio" nell'ambito delle intercettazioni di conversazioni e comunicazioni*, in *La giustizia penale differenziata. Gli accertamenti complementari*, coord. da M. MONTAGNA, Torino, 2011.

[261] Mentre annotazioni, verbali e registrazioni restano custodite nell'archivio riservato.

[262] Si può ritenere che la necessità dell'udienza insorga alla luce del tenore e della complessità delle richieste avanzate dalle difese ai sensi dell'art. 268-ter, 3 c.p.p.

Uno dei punti cardine della riforma è indubbiamente l'istituzione dell'archivio riservato delle intercettazioni[263]. Nell'ottica di assicurare la tutela della riservatezza delle informazioni e delle persone estranee al procedimento, tale istituto combina la necessità di segretezza con quella di conservazione dell'intero materiale, quantomeno sino alla pronuncia della sentenza irrevocabile. L'archivio riservato, disciplinato dall'art. 89-bis disp. att. c.p.p., è istituito presso l'ufficio del pubblico ministero, sotto la direzione e la sorveglianza del procuratore della Repubblica, con modalità tali da assicurare la segretezza della documentazione custodita. L'art. 7, c. 3 del decreto legislativo di riforma prevede, in proposito, che con decreto del Ministro della giustizia, da emanare entro tre mesi dall'entrata in vigore del decreto di riforma, sentito il Garante per la protezione dei dati personali, siano fissati i criteri a cui il procuratore della Repubblica si attiene per regolare le modalità di accesso all'archivio riservato, a tutela della riservatezza degli atti ivi custoditi. All'archivio potranno accedere il giudice che procede e i suoi ausiliari, il pubblico ministero e i suoi ausiliari – ivi compresi gli ufficiali di polizia giudiziaria delegati all'ascolto –, e i difensori delle parti, ai quali va assicurata la facoltà di ascoltare tutte le registrazioni, anche quelle non rilevanti per il procedimento in corso. Gli atti conservati nell'archivio (annotazioni, verbali, atti e registrazioni delle intercettazioni) sono coperti da segreto[264], funzionale sia alla tutela delle indagini sia alla riservatezza delle comunicazioni e conversazioni oggetto di captazione.

Un seguito assai modesto ha invece avuto la direttiva di delega in tema di riproduzione delle intercettazioni negli atti cautelari. Mosso dalla finalità di evitare la propalazione ai *mass media* delle trascrizioni anche di brani irrilevanti, il legislatore delegante aveva avanzato la proposta di vietare *ab origine* la riproducibilità delle trascrizioni integrali delle intercettazioni nel corpo delle ordinanze cautelari. Sull'onda della preoccupazione di libere ed arbitrarie interpretazioni di conversazioni «delle quali fosse possibile apprezzare esclusivamente il sunto del contenuto»[265], si è invece imboccata la strada della "responsabilizzazione" di pubblico ministero e polizia giudiziaria in ordine alla scelta dei brani da trascrivere: i novellati artt. 291 e 292 c.p.p., in tema di riproducibilità delle

[263] Si tratta di un vero e proprio archivio in cui si conservano non solo gli atti cartacei (o digitali) dei provvedimenti attinenti alle intercettazioni, ma anche i supporti, necessariamente digitali, sui quali sono registrate le intercettazioni stesse.

[264] La violazione dell'obbligo del segreto integra, a seconda dei casi, i delitti di rivelazione di segreto d'ufficio di cui all'art. 326 c.p., di rivelazione di segreti inerenti ad un procedimento penale *ex* art. 379-bis c.p. e, eventualmente, anche di favoreggiamento personale di cui all'art. 378 c.p.

[265] D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit.

trascrizioni delle intercettazioni negli atti cautelari, introducono così un doppio giudizio di pertinenza, con la conseguenza che la riproducibilità potrà avvenire soltanto allorché risulti necessaria e sarà in ogni caso limitata ai soli brani essenziali.

Contestualmente alla modifica delle disposizioni del codice di rito, sempre nell'ottica di un rafforzamento della tutela della sfera della riservatezza, la riforma introduce un nuovo reato nel titolo relativo ai delitti contro la persona: si tratta dell'art. 617-septies c.p., rubricato "diffusione di riprese e registrazioni fraudolente". Al fine di sanzionare le violazioni dei doveri di riservatezza che possono presidiare lo svolgimento di incontri e conversazioni private, la norma punisce, a querela della persona offesa, con la pena della reclusione fino a quattro anni, chiunque, al fine di recare danno all'altrui reputazione o immagine, diffonde con qualsiasi mezzo riprese audio o video, compiute fraudolentemente, di incontri privati o registrazioni, pur esse fraudolente, di conversazioni, anche telefoniche o telematiche, svolte in sua presenza o con la sua partecipazione.

Infine, la nuova disciplina sul captatore informatico. Superando l'orientamento venutosi a creare a seguito di un intervento delle sezioni unite[266], che aveva apparentemente escluso la possibilità di ricorrere alle intercettazioni mediante captatore informatico per i delitti diversi da quelli di criminalità organizzata, la novella, intervenendo direttamente sulla formulazione dell'art. 266, comma 2, c.p.p., esplicita la facoltà di ricorrere alle intercettazioni tra presenti anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Concepita come una peculiare forma di intercettazione tra presenti, la stessa soggiace alla relativa disciplina: in altri termini, è sempre consentita nei luoghi diversi da quelli di privata dimora, mentre, in tali luoghi, è autorizzabile dal giudice soltanto qualora sussista fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa; diverso regime viene invece previsto per il caso in cui si proceda per i delitti di criminalità organizzata di cui all'art. 51, c. 3-bis e 3-quater c.p.p., rispetto ai quali è sempre consentita, anche nei luoghi domiciliari[267]. Inoltre, quanto ai presupposti ed alle forme del provvedimento, l'art. 267 c.p.p., così come novellato, radica in capo al giudice un onere motivazionale più stringente: oltre la sussistenza di gravi indizi di reato e l'indispensabilità

[266] Cass., sez. un., 28 aprile 2016, n. 26889.

[267] La precisazione, attuata mediante l'inserimento del comma 2-bis all'art. 266 c.p.p., potrebbe apparire superflua, posto che la circostanza appare desumibile direttamente dalla disciplina di cui all'art. 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, ma determina, in realtà, un evidente restringimento dell'ambito operativo del *trojan*.

del ricorso al mezzo intercettivo, si richiede infatti l'indicazione delle ragioni che rendano necessaria tale modalità per lo svolgimento delle indagini. Ancora, salvo che si proceda per delitti di criminalità organizzata di tipo mafioso o di terrorismo, di cui all'art. 51, c. 3-bis e 3-quater, c.p.p., il decreto autorizzativo, come già anticipato, dovrà altresì indicare i luoghi e il tempo – anche indirettamente indeterminati – in relazione ai quali è consentita l'attivazione del microfono, nella prospettiva di evitare il rischio di un'attivazione indiscriminata e ininterrotta degli ascolti, che si protragga senza soluzione di continuità.

Tracciate le linee essenziali delle direttive di delega e del relativo decreto attuativo, il tempo è maturo per un bilancio della c.d. riforma Orlando. Su di essa si è espresso con toni critici Filippi, ad avviso del quale[268] il legislatore, «che aveva dichiarato di voler rendere più equilibrata la salvaguardia di interessi parimenti meritevoli di tutela a livello costituzionale, volendo tutelare la *privacy*», avrebbe finito, come per una sorta di eterogenesi dei fini, per rafforzare le esigenze connesse all'indagine, dimenticandosi di attuare «la presunzione di innocenza dell'imputato, il quale dalle cronache giudiziarie è sempre descritto come il colpevole» e, dall'altro lato, «i diritti processuali della persona offesa dal reato, esclusa dalla procedura di selezione delle intercettazioni». In definitiva, la riforma si sarebbe rivelata «un complicato sistema di "trascrizioni sommarie" e "annotazioni" da parte della polizia giudiziaria (*omissis*), ma con successiva verifica ed eventuale decreto di "trascrizione coatta" del p.m., ed un ulteriore macchinoso procedimento per l'acquisizione al fascicolo delle indagini, soltanto al fine di evitare che vi entri ciò che è irrilevante per le indagini; mentre l'accertamento del contenuto mediante la trascrizione peritale diventa un'eventualità e comunque sempre in dibattimento». Di "perdurante amorfismo legale delle intercettazioni" ha parlato Mazza[269], per il quale «le intercettazioni rimangono una prova largamente atipica, destinata a essere ancor più governata dalla giurisprudenza e, addirittura, dalle prassi, senza effettive garanzie per gli interessi costituzionalmente rilevanti che ne risultano coinvolti e con un significativo arretramento della tutela del diritto di difesa». Secondo Vergine[270], nonostante le buone intenzioni, la nuova disciplina delle intercettazioni «sembra stridere sia con la Carta costituzionale che con i *dicta* della CEDU, giacché non si comprende la

[268] L. FILIPPI, *Attuazione della delega sulle intercettazioni*, cit.

[269] A. MAZZA, *Amorfismo legale e adiaforia costituzionale nella nuova disciplina delle intercettazioni*, cit.

[270] F. VERGINE, *La riforma della disciplina delle intercettazioni: un valzer con un'orchestra scordata*, in *Proc. pen. giust.*, 2018, p. 787 ss.

limitazione delle facoltà di estrarre copia da parte del difensore allorché sia già avvenuta una ampia *discovery* delle intercettazioni». Per riprendere le parole di quest'ultimo, allora, può osservarsi «come difficilmente si sia assistito, nel corso degli anni, ad una valutazione negativa così unanime di un testo di legge»: per quanto le critiche avanzate siano di diversa natura, «la sensazione che se ne trae è che lo sforzo legislativo non abbia né soddisfatto le aspettative della giurisprudenza, né abbia sopito le critiche forensi, né, infine, abbia tamponato la falle evidenziate dalla dottrina». Questi rilievi, sebbene in alcun modo esaustivi, possono forse aiutare a comprendere le plurime criticità della mai entrata in vigore riforma Orlando.

9. *Il d.l. n. 161/2019 e la l. n. 3/2019 (c.d. riforma Bonafede)*

Come si è detto, il susseguirsi di rinvii dell'entrata in vigore della c.d. riforma Orlando culmina, con il cambio di maggioranza dell'estate 2019, nel d.l. 30 dicembre 2019, n. 161[271], intitolato «Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni». Se vi è un aspetto che caratterizza la c.d. (contro)riforma Bonafede, quello è senz'altro il criticabile *vulnus* alle prerogative parlamentari che il suo processo di adozione ha realizzato. Infatti, come già il decreto n. 161 era stato formulato negli ambienti del Ministero della giustizia senza la convocazione né l'audizione delle associazioni dei docenti universitari, dei magistrati e degli avvocati, anche la sua conversione in legge ha avuto luogo secondo un percorso parlamentare che non ha consentito quel dibattito di ampio respiro di cui le novità, introdotte alla fine dell'anno, suggerivano l'opportunità. Anzi, al momento della conversione nella legge n. 7 del 2020, il maxiemendamento sottoposto alla fiducia è

[271] Su cui, oltre ai vari commenti di G. AMATO, pubblicati in *Guida dir.*, 2020, 6, p. 64 ss., cfr., fra i tanti, M. GIALUZ (a cura di), *Le nuove intercettazioni*, cit.; C. GITTARDI, *La riforma delle intercettazioni, dopo due anni, alla stretta finale con molte novità*, in *Giustizia Insieme*, 2020; C. LARINNI, *La (contro)riforma delle intercettazioni*, in *Discrimen*, 2020; W. NOCERINO, *Prime riflessioni a margine del nuovo decreto legge in materia di intercettazioni*, in *Sist. pen.*, 2020/1, p. 63 ss; C. PARODI, *Il nuovo decreto intercettazioni: le indicazioni sulla riservatezza*, in *il Penalista*; G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, 2020/2, p. 109 ss., in *Sistema Penale*, 2020; D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni,* 2020/2, p. 71 ss., in *Sistema Penale*, 2020; G. SANTALUCIA, *Il diritto alla riservatezza nella nuova disciplina delle intercettazioni, ivi,* 2020/1, p. 47 ss.; G. SPANGHER, *Cosa prevede il dl intercettazioni*, trojan *ovunque* e articolo 15 della Costituzione calpestato, in *il Riformista*, 2020.

stato elaborato per lo più nei medesimi ambienti del Ministero, circostanza che ha condotto ad una riforma approvata «con un metodo e una tempistica palesemente inadeguati alla delicatezza dei beni giuridici in gioco»[272]. A seguito dello scoppio della pandemia da Covid19, l'entrata in vigore delle nuove norme è stata da ultimo differita al 1 settembre 2020[273]: per effetto di ciò, la manovra ha determinato la ricordata distinzione tra i "vecchi" procedimenti iscritti fino al 31 agosto e i "nuovi" procedimenti iscritti dopo tale data.

Prima di entrare nel merito di questo intervento normativo, è possibile fornire tre chiavi di lettura della riforma[274].

In primo luogo, si assiste al tentativo di rimediare alla scarsa attenzione prestata dal legislatore del 1988 rispetto alla tutela della riservatezza attraverso:

a) abbandono del vaglio preventivo affidato, nella prospettiva della riforma del 2017, alla polizia giudiziaria in fase di documentazione e promozione del ruolo di direzione e vigilanza del pubblico ministero a protezione della *privacy*;
b) riabilitazione del meccanismo della selezione/acquisizione con la previsione di un "doppio binario", rappresentato dal procedimento acquisitivo in contraddittorio (art. 268, c. 5 e 6 c.p.p.) e dal procedimento acquisitivo consensuale (artt. 415-bis, c. 2-bis e 454, c. 2-bis c.p.p.);
c) istituzione di un archivio delle intercettazioni, che conserva i tratti della segretezza e acquista natura digitale;
d) previsione di un divieto di pubblicazione speciale.

La seconda linea di intervento è rappresentata dall'introduzione di una disciplina del captatore informatico che, con qualche modifica del tutto trascurabile, conferma l'impostazione di fondo della riforma Orlando. Ribadito l'ambito applicativo estremamente ampio dello strumento in parola, il legislatore mostra di non aver saputo fare tesoro delle critiche connesse ad una disciplina che continua a concepire il *trojan* alla stregua di una modalità esecutiva delle intercettazioni ambientali, lasciando invece prive di base giuridica le perquisizioni *online*. Su questo versante, pertanto, l'intervento si rivela assai deludente.

A destare i maggiori profili di allarme è, tuttavia, la terza linea di intervento, con la quale viene sensibilmente esteso l'ambito di applicazione del mezzo, anche per quanto concerne

[272] M. GIALUZ, *Premessa,* cit., p. 4.

[273] Ad opera del decreto-legge 30 aprile 2020, n. 28, conv. nella legge n. 70 del 2020.

[274] Cfr. M. GIALUZ, *Premessa,* cit., 4 ss.

l'uso obliquo: è quello che emerge, oltre che dal nuovo comma 1, *f-quinquies* dell'art. 266 c.p.p.[275], dall'art. 270 c.p.p., che, valorizzando lo strumento captativo come vera e propria rete a strascico, renderà necessari intensi sforzi esegetici da parte della giurisprudenza.

Per tracciare una "mappa" dei principali ambiti di intervento della novella, si può seguire il seguente schema[276]:

1) la redazione dei c.d. brogliacci di ascolto;
2) l'archivio delle intercettazioni;
3) l'acquisizione delle intercettazioni con procedura di controllo giudiziale;
4) l'acquisizione delle intercettazioni su iniziativa del pubblico ministero;
5) segreto a tutela della riservatezza e divieto speciale di pubblicazione delle intercettazioni;
6) la nuova disciplina della circolazione del captato;
7) le intercettazioni con captatore informatico.

Nel ridisegnare la disciplina avente ad oggetto la selezione e l'acquisizione delle intercettazioni concepita dal d.lgs. 29 dicembre 2017, n. 216, il d.l. 30 dicembre 2019, n. 161, convertito con modifiche dalla l. 28 febbraio 2020, n. 7, riscrive l'art. 268, c. 2-bis c.p.p., relativo alla redazione dei verbali e alle eventuali omissioni nella trascrizione, nella prospettiva di ristabilire gli equilibri tra pubblico ministero e polizia giudiziaria. Nella sua nuova versione, il c.2-bis dell'art. 268 c.p.p. stabilisce che il pubblico ministero dia indicazioni e vigili affinché nei verbali non siano riportate espressioni lesive della reputazione delle persone o quelle che riguardano dati personali definiti sensibili dalla legge, salvo che risultino rilevanti ai fini delle indagini. La novella abroga quindi la seconda parte del c. 4 dell'art. 267 c.p.p. e il c. 2-ter dell'art. 268 c.p.p.[277], mentre resta fermo il divieto di trascrizione anche sommaria[278], introdotto dal d.lgs. n. 216 del 2017 al c. 7 dell'art. 103 c.p.p., relativo alle intercettazioni concernenti conversazioni o comunicazioni dei difensori, degli investigatori e dei consulenti tecnici.

[275] La norma stende l'elenco dei reati per i quali è ammessa l'intercettazione, ricomprendendo i "delitti commessi avvalendosi delle condizioni previste dall'art. 416-bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo".

[276] Cfr. M. GIALUZ (a cura di), *Le nuove intercettazioni*, cit.

[277] Così rinunciando al meccanismo di interlocuzione necessaria fra polizia giudiziaria e pubblico ministero.

[278] Con relativa indicazione soltanto della data, dell'ora e del dispositivo sul quale la registrazione è intervenuta.

Appare evidente come diretto destinatario della nuova prescrizione sia il pubblico ministero, in capo al quale grava l'onere di impedire che nei brogliacci vengano riportate alcune espressioni virtualmente lesive della riservatezza. In chiave di "snellimento procedurale"[279], pertanto, si assiste all'espunzione del meccanismo formalizzato di interlocuzione tra polizia giudiziaria e pubblico ministero, divenendo quest'ultimo il vero protagonista della tutela della riservatezza. In realtà, da una lettura sistematica del nuovo complesso normativo sorge il dubbio di trovarsi di fronte ad una disposizione "ipocrita"[280]: infatti, il novellato c. 2-bis, in combinato disposto con il c. 4 dell'art. 268[281], sembra imporre alla polizia giudiziaria di redigere i verbali, se non contestualmente alla registrazione, almeno in modo frazionato e non a conclusione di tutte le operazioni, ragione per la quale pare potersi concordare con chi ha scritto che la riforma Bonafede ha riportato «la disciplina a quella più naturale interlocuzione informale tra pubblico ministero e polizia giudiziaria»[282].

Assente nel codice del 1930 e in quello del 1988, il c.d. archivio riservato delle intercettazioni viene forgiato, con l'art. 89-bis disp. att. c.p.p., dal d.lgs. n. 216 del 2017, il quale, modificando contestualmente gli artt. 268 e 269 c.p.p., prevede che i verbali e le registrazioni siano trasmessi al pubblico ministero immediatamente dopo la scadenza del termine indicato per lo svolgimento delle operazioni, per poi confluire, insieme ad ogni altro atto ad esse relativo, nell'archivio in discorso, funzionale ad assicurarne la segretezza sino a quando non ne sia disposta l'acquisizione al fascicolo di cui all'art. 373, c. 5 c.p.p. «Fiore all'occhiello»[283] della novella del 2017, l'archivio delle intercettazioni rinasce dalle proprie ceneri nel 2020, arricchendosi di un *quid pluris* sul piano della digitalizzazione[284]. Con l'approvazione della l. n. 7 del. 2020, in particolare, l'art. 89-bis disp. att. c.p.p. viene

[279] In questi termini la Relazione tecnica di accompagnamento al d.d.l. S n. 1659, 9.

[280] Parla di «ipocrisia del nuovo art. 268, c. 2-bis c.p.p.» A. SCALFATI, *Intercettazioni: spirito autoritario, propaganda e norme inutili*, in *Arch. pen.* web, 2020, 1, p. 2.

[281] Ai sensi del quale, «i verbali e le registrazioni sono immediatamente trasmessi al pubblico ministero per la conservazione nell'archivio di cui all'art. 269, c. 1».

[282] D. PRETTI, *La metamorfosi delle intercettazioni,* cit., p. 76.

[283] A. CAMON, *Forme, destinazione e regime della documentazione*, in G. GIOSTRA-R. ORLANDI (a cura di), *Nuove norme in tema di intercettazioni*, cit., p. 79.

[284] L. FILIPPI, *D.L. intercettazioni: abrogata la riforma Orlando, si torna all'antico*, in *Quotidiano giuridico*, 10 gennaio 2020, p. 8.

integralmente soppiantato e l'archivio, mutato nome e natura, si ritrova con un nuovo referente normativo.

Quanto al primo aspetto, si segnala la soppressione dell'aggettivo "riservato", giustificata dalla configurazione del procedimento acquisitivo come partecipato: a tal proposito, giova comunque precisare che, nel 2017, «non era il *nomen iuris* a fare, dell'archivio *ex* art. 89-bis disp. att. c.p.p., un archivio "riservato"», in quanto «il *quid proprium* s'identificava nel regime restrittivo che governava i varchi di accesso al *caveau* e, soprattutto, il divieto di estrarre copia di quanto ivi custodito»[285]. A ben vedere, il legislatore del 2020 non ha sovvertito la disciplina, ma, circoscrivendo la possibilità di «ottenere copia» alle sole registrazioni e ai soli atti «acquisiti a norma degli articoli 268, 415-bis e 454 del codice», ha tralasciato sia le intercettazioni in possesso del pubblico ministero non ancora depositate ai sensi dell'art. 268, c. 4 e 5 c.p.p., sia quelle che il giudice ha ritenuto irrilevanti o, comunque, ha stralciato ai sensi dell'art. 268, c. 6 c.p.p.

Per altro verso, l'archivio delle intercettazioni diventa *expressis verbis* "digitale", ragione per la quale non dovrà più intendersi come uno spazio fisico. L'archivio, tenuto sotto la direzione e la sorveglianza del procuratore della Repubblica dell'ufficio che ha richiesto ed eseguito le intercettazioni ai sensi del c. 1 dell'art. 89-bis disp. att. c.p.p., è gestito con modalità tali da garantire la segretezza della documentazione relativa alle intercettazioni non necessarie per il procedimento, ed a quelle irrilevanti o di cui è vietata l'utilizzazione o riguardanti categorie particolari di dati personali come definiti dalla legge o dal regolamento in materia. La spinta verso la digitalizzazione in questa materia è stata salutata con favore dalla dottrina[286], la quale non ha però celato le preoccupazioni legate alle clausole d'invarianza finanziaria che hanno accompagnato la manovra.

Il d.l. n. 161 del 2019 – confermato da questo punto di vista in sede di conversione – ha, quindi, sdoppiato i canali attraverso i quali il materiale captato confluisce nei fascicoli: mentre in alcuni casi la scelta avviene in contraddittorio davanti al giudice, in altri si realizza un'acquisizione consensuale fuori udienza con chiamata in causa dell'organo giudicante solo in via occasionale. In proposito, si può osservare come questa parte della novella, animata dalla preoccupazione di prendere le distanze dalla riforma Orlando, abbia, per un verso,

[285] S. CIAMPI, *L'archivio delle intercettazioni tra presidio della riservatezza, tutela del diritto di difesa e svolta digitale*, in M. GIALUZ (a cura di), *Le nuove intercettazioni*, cit., p. 27.

[286] *Ibidem*, p. 29.

comportato la reintroduzione di diversi frammenti della disciplina originaria e, per altro verso, riconfermato alcune scelte operate nel 2017, mossa da una fretta inappropriata alla tecnicità della materia.

Per quanto concerne l'acquisizione delle intercettazioni con procedura di controllo giudiziale, si è già ricordato come i codificatori del 1988 si fossero preoccupati di predisporre un filtro di cui, tuttavia, la prassi aveva disvelato i molteplici difetti. In effetti, mentre il "dover essere" normativo imponeva al giudice, dopo il deposito dei verbali e delle registrazioni[287], di disporre l'acquisizione delle comunicazioni indicate dalle parti durante la c.d. udienza di stralcio, nella realtà accadeva il più delle volte che il deposito *de quo* venisse procrastinato e non si procedesse quasi mai allo stralcio, con la conseguenza che le registrazioni e i brogliacci confluivano direttamente nel fascicolo delle indagini e le parti si limitavano in seguito a domandare al giudice del dibattimento l'acquisizione di ciò a cui erano interessate. Caduto nel nulla il primo tentativo di riforma della materia, la novella del 2020 ripropone, con alcune novità, il tradizionale modello elaborato nel 1988. Le parti, conclusa la fase del deposito, hanno l'onere di indicare le «conversazioni» e i «flussi di comunicazioni informatiche o telematiche», che vogliono veder acquisiti; il giudice, dall'altro lato, asseconda le richieste relative ai materiali «che non appaiano irrilevanti», ben potendo, in ogni caso, stralciare, anche d'ufficio, le registrazioni e i verbali «di cui è vietata l'utilizzazione» e «quelli che riguardano categorie particolari di dati personali, sempre che non ne sia dimostrata la rilevanza». In altri termini, si introduce, quale criterio generale di selezione giudiziale, quello della "non irrilevanza" delle conversazioni indicate dalle parti, mentre, per quanto concerne «le categorie particolari di dati personali»[288], al contrario di quanto avviene in base alla regola generale, grava sulle parti l'onere di dimostrare le "rilevanza" del dato personale di cui desiderano ottenere l'acquisizione[289].

In merito ai profili procedurali, l'art. 268, c. 6 c.p.p. tratteggia, in maniera estremamente sintetica, una sorta di udienza in camera di consiglio *ex* art. 127 c.p.p., prevedendo una facoltà partecipativa delle parti, previo avviso di almeno ventiquattro ore[290]; tuttavia,

[287] Da effettuarsi al termine delle operazioni di intercettazione o, eccezionalmente, alla chiusura delle indagini.

[288] Qui il legislatore sembra rinviare all'art. 10 della direttiva UE 2016/680.

[289] V., su tutti, F. CAPRIOLI, *La procedura di filtro delle comunicazioni rilevanti nella legge di riforma della disciplina delle intercettazioni*, in *Cass. pen.*, 2020, p. 1405-1406.

[290] In proposito, cfr. L. FILIPPI, *Intercettazioni:* habemus legem!, in *Dir. pen. proc.*, 2020, p. 457, secondo il quale la facoltatività in parola «sembra consentire anche una semplice indicazione cartolare delle parti sulle registrazioni utilizzabili e rilevanti».

essendo tale diritto di partecipazione limitato all'attività di "stralcio", risulta immaginabile che, nel caso in cui il giudice non intenda scartare delle captazioni indicate dalle parti, decida *de plano*, senza fissazione dell'udienza. Le parti restano libere di non indicare alcuna intercettazione – fattispecie che escluderà l'intervento del giudice –, mentre è ben possibile che le indicazioni pervengano dalla sola difesa.

In alternativa all'udienza di stralcio, la riforma Bonafede prevede due nuove modalità di selezione delle intercettazioni, che contemplano un coinvolgimento del giudice solo in via eventuale. Tale meccanismo, configurato come eccezione, pare destinato a diventare la regola, ragione per la quale è stato autorevolmente definito come il «nucleo della riforma»[291]. Nel caso in cui la procedura di stralcio non venga esperita, in particolare, il pubblico ministero provvede, di propria iniziativa, alla selezione delle intercettazioni rilevanti: ciò può avvenire contestualmente all'avviso di cui all'art. 415-bis c.p.p. oppure, qualora ricorrano i presupposti per il giudizio immediato, con il deposito della richiesta, ai sensi del nuovo art. 454, c. 2-bis c.p.p. I difensori, che sono avvisati in entrambi i casi della facoltà di prendere visione di tutto il materiale intercettativo, hanno facoltà di estrarre copia solamente di quanto indicato come rilevante dal pubblico ministero, mentre, entro il termine di venti giorni dalla notifica dell'avviso o di quindici dalla notifica del decreto immediato, le parti possono indicare le ulteriori registrazioni ritenute rilevanti dal magistrato inquirente, che provvede con decreto motivato: solo in caso di rigetto, il difensore è abilitato a chiedere al giudice di dare luogo all'udienza di stralcio non attivata *ex ante*. È lecito presumere che, non avendo il legislatore del 2019 previsto forma alcuna di incentivo affinché venga attivata la procedura di stralcio *ex* art. 268, c. 6 c.p.p., il ricorso a questa modalità avrà luogo, come già avveniva in passato, «in modo mirato e non massivo»[292]; nessuna forma di sanzione è stata espressamente prevista, peraltro, nel caso in cui, oltre a non essersi proceduto nelle forme di cui all'art. 268 c.p.p., il pubblico ministero ometta l'attivazione della procedura di acquisizione anche alla conclusione delle indagini preliminari ovvero con il deposito della richiesta di giudizio immediato.

---

[291] Così, G. SPANGHER, *La riforma sconta due mesi di proroga, in vigore dal 1 maggio,* in *Guida dir.*, 2020, 13, 34, in riferimento alle ipotesi di cui ai novellati artt. 268, 415-bis 454 c.p.p.

[292] Così, testualmente, la delibera Consiglio Superiore della Magistratura del 29 luglio 2016, *Ricognizione di buone prassi in materia di intercettazione di conversazioni*, all'indirizzo <https://www.csm.it/documents/21768/87316/Delibera+29+luglio+2016/e02375fb-aa0f-c706-315b-a3067725a9ef>, 12.

Sia l'art. 415-bis, c. 2-bis c.p.p. sia l'art. 454, c. 2-bis c.p.p. riconoscono ai difensori la facoltà di indicare alla pubblica accusa l'elenco delle registrazioni ritenute rilevanti di cui chiedono copia: in caso di rigetto dell'istanza o di contestazioni sulle indicazioni ritenute rilevanti, le parti possono rivolgersi al giudice affinché provveda nelle forme dell'art. 268, c. 6 c.p.p. A questo riguardo, è apparsa opinabile la scelta del legislatore di prevedere una forma di interlocuzione diretta tra le parti, finalizzata ad includere, e di non contemplare analoga modalità *ad excludendum,* legittimando al pubblico ministero a tornare sui suoi passi[293].

La disciplina risulta, in definitiva, tutt'altro che nitida: non essendo indicate le tempistiche alle quali debbono attenersi il pubblico ministero per le richieste acquisitive e le parti per rivolgersi al giudice, è ben possibile che i tempi della procedura selettiva superino i termini di cui all'art. 415-bis, c. 3 e 458, c. 1 c.p.p. A fronte del silenzio del legislatore, che ha così dato vita ad una normativa di dubbia legittimità costituzionale, spetterà all'interprete l'arduo compito di ricercare una interpretazione rispettosa del diritto di difesa.

Venendo alla tutela della riservatezza, si può dire che sia proprio questa la parte meglio riuscita della novella, in quanto realizza un più avanzato bilanciamento tra i diritti fondamentali rispetto a quello istituito dalla riforma Orlando[294]. Ad essere precisi, il legislatore rafforza la protezione della riservatezza in senso lato nelle fasi di selezione, conservazione ed eventuale pubblicazione delle captazioni, mentre, rispetto all'attività di documentazione, viene approntato uno strumento di tutela della sola riservatezza in senso stretto. A quest'ultimo riguardo, si è già detto che il novellato art. 268, c. 2-bis c.p.p. affida al pubblico ministero il compito di dare indicazioni affinché nei brogliacci «non siano riportate espressioni lesive della reputazione delle persone o quelle che riguardano dati personali definiti sensibili dalla legge, salvo che si tratti di intercettazioni rilevanti ai fini delle indagini». Al posto di un divieto, quindi, si prevede solo una sorta di raccomandazione rafforzata, mentre, quanto all'oggetto della selezione, non si fa più riferimento all'eliminazione delle conversazioni «irrilevanti ai fini delle indagini», ma soltanto di quelle concernenti dati sensibili ovvero delle espressioni lesive della reputazione, sempre che non siano rilevanti ai fini delle indagini. Si è così giustamente osservato che «il legislatore ha fatto una scelta chiara di orientare il filtro documentativo affidato al pubblico ministero (a

[293] In tal senso, F. CAPRIOLI, *La procedura di filtro*, cit., p. 1402.

[294] Di questo avviso, M. GIALUZ, *Segreto a tutela della riservatezza e divieto speciale di pubblicazione delle intercettazioni*, in ID. (a cura di), *Le nuove intercettazioni*, cit., p. 61.

livello di indirizzo e vigilanza) e alla polizia giudiziaria (a livello operativo) alla sola tutela della riservatezza in senso stretto e dell'onore della persona coinvolta nella captazione»[295].

Quanto alla tutela della riservatezza in senso lato, essendo già state illustrate le principali novità che riguardano la fase della selezione[296] e della conservazione del materiale captato[297], è piuttosto al nuovo c. 2-bis dell'art. 114 c.p.p. che occorre rivolgere l'attenzione. La riforma, nel prevedere che «è sempre vietata la pubblicazione, anche parziale, del contenuto delle intercettazioni non acquisite ai sensi degli artt. 268, 415-bis o 454 c.p.p.», ha dato adito a prese di posizione di segno opposto: a chi si è espresso nei termini di una norma inutile e contraddittoria[298], infatti, si sono contrapposte le voci di coloro che hanno negato l'introduzione di un segreto sugli atti contenuti nell'archivio. A ben vedere, volendo attribuire alla statuizione un preciso contenuto normativo, si può ritenere che la novella abbia realizzato un inedito bilanciamento tra diritto-dovere di informare e l'interesse a non divulgare conversazioni irrilevanti per l'accertamento penale[299]. Secondo questa interpretazione, il c. 2-bis dell'art. 114 c.p.p. andrebbe a stabilire un duplice divieto di pubblicazione dei colloqui intercettati, dei quali il primo riguarda «tutto il materiale intercettato prima che sia intervenuto lo *screening* acquisitivo contemplato dagli artt. 268, 415-bis e 454 c.p.p.»[300], mentre il secondo farebbe riferimento «ai verbali e alle registrazioni che non sono state acquisite (*omissis*) perché ritenute inutilizzabili o irrilevanti»[301]. Quanto al nodo nascente dal tenore letterale della disposizione, che allude alla sola pubblicazione del «contenuto», potrebbe agevolmente rispondersi che, ove interpretata in senso restrittivo,

[295] Così, M. GIALUZ, *Segreto a tutela della riservatezza e divieto speciale di pubblicazione delle intercettazioni*, in ID. (a cura di), *Le nuove intercettazioni*, cit., p. 64.

[296] La fase della selezione del materiale captato risulta affidata ai due "congegni" del procedimento acquisitivo in contraddittorio di cui all'art. 268, c. 5 e 6 c.p.p. e del procedimento acquisitivo consensuale di cui agli artt. 415-bis, c. 2-bis e 454, c. 2-bis c.p.p.

[297] Il riferimento è qui al nuovo archivio digitale delle intercettazioni di cui agli artt. 269 c.p.p. e 89-bis disp. att. c.p.p.

[298] V., su tutti, G. SANTALUCIA, *Il diritto alla riservatezza della nuova disciplina delle intercettazioni*, in *Sist. pen.*, 2020/1, p. 57. Secondo i fautori di questa tesi, la norma sarebbe istitutiva di un vero e proprio segreto a tutela della riservatezza sulle intercettazioni prima dello stralcio e poi su quelle stralciate.

[299] In questi termini, M. GIALUZ, *Segreto a tutela della riservatezza e divieto speciale di pubblicazione delle intercettazioni*, in ID. (a cura di), *Le nuove intercettazioni*, cit., p. 70.

[300] *Ibidem*.

[301] *Ibidem*.

la norma finirebbe per risultare irragionevole e paradossale[302]. Qualora, invece, si valorizzasse il richiamo al solo «contenuto» da parte del c. 2-bis, si dovrebbe ritenere che la norma speciale vada riferita «ai soli casi nei quali viene in rilievo la facoltà di divulgare il contenuto e non il testo di un atto contenente il riferimento alle intercettazioni»[303]. In questo modo, la norma troverebbe applicazione rispetto alle intercettazioni utilizzate nelle indagini preliminari per fondare gli atti di indagine, mentre resterebbe "lettera morta" rispetto all'ordinanza cautelare, atto sicuramente pubblicabile anche nel testo.

Una delle previsioni più controverse della riforma Bonafede in tema di intercettazioni è, senza dubbio, quella concernente il novellato art. 270 c.p.p. Nella sua nuova veste, la norma prevede, al c. 1, che «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'art. 266, c. 1 c.p.p.». Duplice l'operazione del legislatore: da un lato, viene affiancato il requisito della "rilevanza" a quello della "indispensabilità"; dall'altro, si inserisce un riferimento ai reati di cui all'art. 266, c. 1 c.p.p. tra quelli per i quali non opera la regola di esclusione. Tra i complessi nodi interpretativi che sollevano questi due interventi, si possono menzionare, in prima battuta, i dubbi circa l'effettiva portata precettiva del requisito della "rilevanza", atteso che lo stesso sembrerebbe risolversi nel già previsto presupposto della "indispensabilità"[304]. Per altro verso, tutt'altro che agevole è l'esegesi del nuovo art. 270, c. 1 c.p.p., «nella parte in cui si consente l'utilizzazione dei risultati delle intercettazioni in procedimenti diversi solo se funzionali (*omissis*) all'accertamento "di delitti per i quali è obbligatorio l'arresto in flagranza e dei reati di cui all'art. 266, comma 1" c.p.p.»[305]. Il *punctum dolens* della questione risiede nel fatto che, laddove si andasse ad attribuire valore aggiuntivo alla congiunzione "e", così consentendo la circolazione delle captazioni, oltre che per le fattispecie per le quali la legge prevede l'arresto obbligatorio in flagranza, anche per tutte quelle di cui all'art. 266, c. c.p.p.[306], si finirebbe per «alimentare

[302] *Ibidem*.

[303] *Ibidem*, p. 71.

[304] Cfr., a questo riguardo, K. NATALI, *Sezioni unite e "legge Bonafede": nuove regole per l'uso trasversale delle intercettazioni*, in *Cass. pen.*, 2020, p. 18 del dattiloscritto, ad avviso del quale non si comprende come degli elementi probatori possano risultare "indispensabili" per l'accertamento di un reato, «pur non essendo rilevanti agli stessi fini».

[305] *Ibidem*.

[306] Questa tesi è sostenuta, per esempio, da D. PRETTI, *La metamorfosi delle intercettazioni*, cit.

il ricorso a pratiche investigative pericolose e difficilmente sorvegliabili di pesca "a strascico"»[307]. Una simile interpretazione, peraltro, sembra porsi in rotta di collisione anche con la Costituzione, così come interpretata dai giudici del Palazzo della Consulta[308], ad avviso dei quali una norma che consentisse il trasferimento delle intercettazioni in procedimenti diversi per tutti i reati di cui all'art. 266, c. 1 c.p.p. sarebbe «apertamente contrastante con le garanzie poste dall'art. 15 Cost. (*omissis*) a tutela della libertà e della segretezza delle comunicazioni, dal momento che trasformerebbe l'intervento del giudice (*omissis*) in "un'inammissibile autorizzazione in bianco" a disporre le intercettazioni»[309].

Quanto al c. 2 dell'art. 270 c.p.p., si è polemicamente parlato di un «ritorno al passato»[310]. Se, infatti, il d.lgs. n. 216 del 2017 aveva opportunamente inserito, nel secondo periodo, un richiamo all'art. 268-bis c.p.p., fissando testualmente l'obbligo di deposito dei «decreti che hanno disposto, autorizzato, convalidato o prorogato l'intercettazione», il riformatore del 2020 ha omesso ogni riferimento espresso alla tematica del deposito dei decreti autorizzativi delle intercettazioni. In conseguenza di questa scelta – compiuta forse senza neppure averne piena contezza –, si è determinato un significativo passo indietro, in quanto, allo stato dell'arte, resta previsto un obbligo di deposito presso l'autorità competente per il procedimento *ad quem* dei soli verbali e registrazioni delle intercettazioni. In altri termini, il legislatore ha "scrollato le spalle" rispetto alle indicazioni provenienti dalla miglior dottrina[311], così perdendo l'ennesima occasione di risolvere in maniera tombale uno dei più rilevanti nodi critici dell'art. 270 c.p.p., per il quale, in oggi, sembra non esserci pace.

Uno snodo decisivo della riforma Bonafede è, infine, rappresentato dalla l. 9 gennaio 2019, n. 3 (c.d. legge "spazza-corrotti" o "anticorruzione")[312], che, entrata in vigore il 31 gennaio 2019, si è preoccupata di «affrontare in modo efficace il fenomeno corruttivo e, in

---

[307] K. NATALI, *Sezioni unite e "legge Bonafede"*, cit., p. 20 del dattiloscritto.

[308] In questo senso, L. FILIPPI, *Intercettazioni,* cit., p. 462.

[309] Così Corte cost. n. 63 del 1994.

[310] J. DELLA TORRE, *La nuova disciplina della circolazione del captato: un nodo arduo da sciogliere*, in M. GIALUZ (a cura di), *Le nuove intercettazioni*, cit., p. 103.

[311] Si veda, in proposito, A. CAMON, sub *art. 270 c.p.p.*, in G. CONSO-G. ILLUMINATI (cur.), *Commentario breve al codice di procedura penale*, II ed., Padova, 2015, p. 1052 ss.

[312] Cfr. l. 9 gennaio 2019 n. 3, recante «Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici», in G.U., 16 gennaio 2019, n. 13.

generale, (*omissis*) assicurare una maggiore incisività all'azione di contrasto dei reati contro la pubblica amministrazione»[313]. Fra gli ambiti interessati da tale provvedimento legislativo spicca quello concernente la disciplina processuale in materia di intercettazioni di comunicazioni o conversazioni tra presenti mediante installazione del captatore informatico su dispositivo elettronico portatile, già oggetto del precedente d.lgs. n. 216 del 2017. Abbandonato il tentativo di rintracciare un punto di equilibrio tra l'esigenza di repressione dei reati e il rispetto dei diritti costituzionalmente tutelati, la l. n. 3 del 2019 interviene sugli artt. 266, c. 2-bis e 267, c. 1 c.p.p., estendendo l'ambito applicativo della disciplina "speciale" sulle intercettazioni eseguite mediante inserimento del captatore informatico, in precedenza contemplata per i soli delitti di cui all'art. 51, c. 3-bis e 3-quater c.p.p., anche ai reati dei pubblici ufficiali contro la pubblica amministrazione[314], puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'art. 4 c.p.p.[315] Più in particolare, il nuovo c. 2-bis dell'art. 266 prevede che, nei procedimenti per i delitti di cui all'art. 51, c. 3-bis e 3-quater c.p.p., le intrusioni realizzate con impiego del c.d. *trojan* sono sempre consentite nei luoghi di privata dimora: in questo modo, si prescinde dall'accertamento del requisito costituito dal fondato motivo di ritenere che nei predetti luoghi si stia svolgendo l'attività criminosa, indispensabile per l'autorizzazione delle intercettazioni nei luoghi domiciliari, ove si proceda per i reati diversi da quelli di criminalità organizzata. Quanto alla motivazione del decreto autorizzativo *ex* art. 267 c.p.p., nei casi in cui si proceda per reati "comuni", il giudice per le indagini preliminari deve indicare, oltre alle ragioni che hanno determinato il ricorso al captatore informatico, anche «i luoghi e il tempo» di attivazione del microfono-spia, al fine di assicurare un controllo giurisdizionale più incisivo sui movimenti del dispositivo bersaglio; diviene invece irrilevante la predeterminazione delle coordinate spazio-temporali nel caso in cui si proceda per delitti di criminalità organizzata o con finalità terroristiche. La duplice disciplina trova una eco anche nell'ambito dell'attivazione d'urgenza da parte dell'organo dell'accusa: il nuovo c. 2-bis dell'art. 267 c.p.p. stabilisce infatti che, nei casi di urgenza, il pubblico ministero può

[313] Si veda la Relazione di accompagnamento al Disegno di legge n. 1189, presentato alla Camera il 24 settembre 2018 dal Ministro della Giustizia Bonafede, reperibile sul sito www.camera.it

[314] Restano, pertanto, esclusi i reati commessi da incaricati di pubblico servizio o da esercenti servizi di pubblica necessità, nonché quelli commessi da privati nei confronti della pubblica amministrazione.

[315] Ai sensi dell'art. 4 c.p.p., si ha riguardo alla pena stabilita dalla legge per ciascun reato consumato o tentato, senza tenere conto della continuazione, della recidiva e delle circostanze del reato, fatta eccezione delle circostanze aggravanti per le quali la legge stabilisce una pena di specie diversa da quella ordinaria del reato e di quelle ad effetto speciale.

disporre l'intercettazione tra presenti mediante captatore informatico soltanto nei procedimenti per i delitti di cui all'art. 51, c. 3-bis e 3-quater c.p.p.

Si può affermare, in linea di estrema sintesi, che il filo rosso dell'intervento normativo, attuato con la l. n. 3 del 2019 in tema di intercettazioni ambientali mediante captatore informatico, sia rappresentato dall'ambizione a realizzare un'equivalenza piena tra le fattispecie di cui all'art. 51, c. 3-bis e 3-quater c.p.p. e i delitti gravi dei pubblici ufficiali contro la pubblica amministrazione. A fronte di questa uniformazione sul piano del trattamento procedimentale della corruzione alla criminalità organizzata, voci critiche si sono levate da più parti[316]: il rischio principale appare senz'altro quello di un uso distorto del *trojan virus*, anche considerato che non si vede per quale ragione «il captatore informatico possa essere più agevolmente utilizzato nelle indagini concernenti i delitti contro la pubblica amministrazione rispetto a quelle relative ai reati di criminalità organizzata non ricompresi nell'elenco di cui all'art. 51, commi 3-bis e 3-quater c.p.p.»[317].

Nel complesso, la riforma Bonafede sulle intercettazioni si segnala per alcuni punti di luce e diverse zone d'ombra. In positivo, si può dire che essa abbia assicurato una maggiore tutela della riservatezza dei terzi coinvolti: è quanto desumibile dai commi 2-bis e 6 dell'art. 268 c.p.p., oltre che dall'istituzione dell'archivio digitale delle intercettazioni di cui all'att. 269, c. 1 c.p.p. e dalla previsione del divieto di pubblicazione delle intercettazioni non acquisite ai sensi dell'art. 114, c. 2-bis c.p.p. Per contro, desta forti perplessità la reintroduzione di un'udienza di stralcio, che, come ricordato, aveva già mostrato i suoi limiti nella prassi[318], nonché la previsione di un nuovo momento di selezione a seguito del deposito dell'avviso di conclusione delle indagini *ex* art. 415-bis, c. 2-bis c.p.p. ovvero della richiesta di giudizio immediato.

[316] Sulla riforma del *trojan virus* ad opera della l. n. 3 del 2019, si vedano, tra gli altri, L. CAMALDO, *Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico*, in *Dir. pen. cont.*, 24 settembre 2019, p. 1 ss.; M. TORRE, *Il captatore informatico dopo la legge c.d. "spazza-corrotti"*, in *Dir. pen. proc.*, 2019, p. 648 ss.

[317] L. AGOSTINO -M. PERALDO (a cura di), *Le intercettazioni con captatore informatico: ambito di applicazione e garanzie procedurali*, in M. GIALUZ (a cura di), *Le nuove intercettazioni*, cit., p. 79.

[318] Il grande assente sembra piuttosto il contraddittorio con il reale controinteressato alla trascrizione delle comunicazioni, cioè il soggetto estraneo al procedimento penale la cui voce è stata occasionalmente captata.

10. Le intercettazioni nei confronti dei parlamentari e del Presidente della Repubblica

Le intercettazioni che riguardano i membri del Parlamento[319] sono disciplinate dalla c.d. legge Boato (l. 20 giugno 2003, n. 140), sulla quale si è pronunciata in più occasioni la Corte costituzionale. L'intervento normativo in parola arriva a seguito della modifica dell'art. 68 della Costituzione, realizzata ad opera della legge costituzionale 29 ottobre 1993 n. 3, che, nella prospettiva di rimuovere ciò che veniva percepito, agli occhi dell'opinione pubblica, come un "ingiustificato privilegio", aveva espunto dalla Carta fondamentale l'istituto dell'autorizzazione a procedere. In base ai commi 2 e 3 dell'art. 68 Cost., pertanto, viene concessa dalla Camera di appartenenza del parlamentare, divenuto oggetto dell'interesse dell'autorità giudiziaria, una c.d. autorizzazione *ad acta*, per l'esecuzione di controlli a sorpresa incidenti sulla sfera personale o domiciliare, per l'esecuzione di forme di limitazione della libertà personale, per la sottoposizione del predetto soggetto ad intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni, nonché per il sequestro di corrispondenza. La l. n. 140 del 2003 viene così a dare concreta applicazione alle previsioni della disciplina costituzionale illustrate, operando una distinzione tra i casi in cui il parlamentare sia il destinatario dell'intercettazione e quelli, diversi, in cui questi sia stato accidentalmente sottoposto ad intercettazione.

Le intercettazioni riguardanti parlamentari si dividono tradizionalmente in tre categorie[320]: intercettazioni dirette, indirette e casuali.

a) Le intercettazioni "dirette" ricorrono quando sottoposti ad intercettazione sono utenze o luoghi appartenenti al parlamentare o nella sua disponibilità.
b) Siamo in presenza di intercettazioni "indirette" quando l'attività di captazione riguarda utenze intestate a soggetti differenti, che, tuttavia, sono interlocutori abituali del parlamentare, ovvero concerne luoghi a lui non appartenenti, ma che si presumono dal medesimo frequentati[321].

[319] V., per approfondimenti sul tema, M. GIALUZ, *Intercettazioni di colloqui riservati e libertà funzionali del parlamentare: qualche riflessione sulla portata della prerogativa dell'art. 68, comma 3, Cost.*, in *Cass. pen.*, 2004, p. 3682 ss.; V. GREVI, *Anomali e paradossi in tema di intercettazioni «indirette» relative a membri del parlamento*, in *Cass. Pen.*, 2007, p. 3159 ss.

[320] Si veda, in proposito, P. TONINI, *Manuale di procedura penale*, cit., p. 415-416.

[321] Corte cost., n. 114 del 2010.

Per disporre un'intercettazione diretta o indiretta nei confronti di un parlamentare, occorre, ai sensi dell'art. 4 della l. n. 140, una preventiva autorizzazione a procedere della Camera di appartenenza dello stesso, a pena di inutilizzabilità assoluta dell'atto.

c) Si definisce "casuale" l'intercettazione allorché non sia disposta su utenze riferibili al parlamentare e il suo ingresso nell'area di ascolto sia del tutto accidentale. Ai sensi dell'art. 6 della l. n. 140, il giudice per le indagini preliminari, qualora ritenga irrilevanti i verbali e le registrazioni delle conversazioni intercettate nel corso di procedimenti a carico di terzi, alle quali abbia accidentalmente partecipato un parlamentare, ne decide, sentire le parti, la distruzione in camera di consiglio, in base all'art. 269, c. 2 e 3 c.p.p. Qualora, invece, il giudice consideri rilevanti le intercettazioni in questione, deve chiedere un'autorizzazione alla Camera cui il parlamentare appartiene ovvero apparteneva al momento della captazione. L'autorizzazione si rende necessaria nei soli casi in cui l'intercettazione debba essere utilizzata tanto nei confronti del parlamentare quanto nei confronti di terzi. Secondo quanto statuito dalla Corte costituzionale[322], nel caso in cui l'autorizzazione non venga concessa, le intercettazioni saranno inutilizzabili nei confronti del parlamentare coinvolto, mentre potranno essere utilizzate nei confronti di terzi, circostanza che impedisce la distruzione dei relativi verbali e registrazioni. Infine, non occorre alcuna autorizzazione per il caso in cui l'autorità giudiziaria intenda impiegare i risultati delle intercettazioni nei soli confronti di persone diverse dal parlamentare. È appena il caso di precisare che l'art. 6 della l. n. 140 è applicabile esclusivamente nell'ipotesi in cui l'intercettazione del parlamentare sia casuale, in quanto ciò esclude *ab origine* il pericolo di un uso abnorme del potere di intercettare, non potendo l'autorità procedente munirsi di una preventiva autorizzazione della Camera di appartenenza proprio per il carattere inaspettato del coinvolgimento dell'esponente politico.

Diverso discorso deve farsi per il caso in cui prenda parte alla conversazione intercettata un soggetto per il quale vige un divieto di intercettazione, in considerazione della sua qualità ovvero del segreto al quale è vincolato, quale il Presidente della Repubblica. Sul punto, è intervenuta la Corte costituzionale in una nota pronuncia del 2013[323], con la quale ha chiarito

[322] Corte cost., n. 390 del 2007.

[323] Corte cost., n. 1 del 2013.

che vi sono «ragioni di ordine sostanziale, espressive di un'esigenza di tutela "rafforzata" di determinati colloqui in funzione di salvaguardia di valori e diritti di rilievo costituzionale che si affiancano al generale interesse alla segretezza delle comunicazioni (quali la libertà di religione, il diritto di difesa, la tutela della riservatezza su dati sensibili ed altro)».

La vicenda, che offre il destro alla Consulta per una ricostruzione del ruolo di garante dell'equilibrio costituzionale rivestito dal Capo dello Stato[324], prende le mosse dalle intercettazioni telefoniche, disposte dal Procuratore della Repubblica presso il Tribunale ordinario di Palermo nell'ambito della nota "trattativa" tra Stato e mafia, nei confronti del senatore Mancino. Fra le conversazioni casualmente intercettate figurano anche quelle dell'allora Presidente della Repubblica Napolitano, che, in forza del principio di riservatezza delle conversazioni e comunicazioni del Capo dello Stato, solleva un conflitto di attribuzione tra poteri dello Stato, per violazione degli artt. 90 e 3 Cost. e delle disposizioni di legge ordinaria che ne costituiscono attuazione, innanzi alla Corte costituzionale. Accertata la sussistenza degli elementi soggettivi e oggettivi[325], il giudice delle leggi, entrando nel merito del giudizio, si sofferma sull'aspettativa di riservatezza delle comunicazioni intrattenute dal Presidente della Repubblica, che discende dallo svolgimento di un'attività "informale" sotteso al suo ruolo istituzionale. A questo riguardo, la Corte ha buon gioco nel rilevare come «il Presidente deve tessere costantemente una rete di raccordi allo scopo di armonizzare eventuali posizioni in conflitto ed asprezze polemiche, indicare ai vari titolari di organi costituzionali i principi in base ai quali possono e devono essere ricercate soluzioni il più possibile condivise dei diversi problemi che via via si pongono»: per l'effetto, risulta indispensabile che «affianchi continuamente ai propri poteri formali (*omissis*) un uso discreto di quello che è stato definito il "potere di persuasione", essenzialmente composto di attività informali». Ciononostante, mentre limitazioni specifiche all'esercizio di poteri di indagine mediante atti invasivi, quali le intercettazioni telefoniche, sono previste da norme di rango costituzionale per i membri delle Camere[326] e per i componenti del Governo[327],

[324] Emblematica, a questo riguardo, la presenza di due autorevoli giudici relatori, quali il costituzionalista Silvestri e il penalista Frigo.

[325] Quali la natura di "potere" dello Stato e la sussistenza di attribuzioni costituzionalmente tutelate.

[326] Art. 68, c. 3 Cost.

[327] Art. 10 della legge cost. 16 gennaio 1989, n. 1, recante «Modifiche degli articoli 96, 134 e 135 della Costituzione e della legge costituzionale 11 marzo 1953, n. 1, e norme in materia di procedimenti per i reati di cui all'articolo 96 della Costituzione».

altrettanto non può dirsi con riguardo al Capo dello Stato. A venire in rilievo è, allora, una norma dal "tono costituzionale", quale l'art. 7, c. 2 e 3 della l. n. 219 del 1989, che attribuisce al Comitato parlamentare[328] il potere di deliberare i provvedimenti che dispongono intercettazioni telefoniche nei confronti del Presidente della Repubblica, dopo che la Corte costituzionale lo abbia sospeso dalla carica.

Trattandosi, nel caso di specie, di intercettazioni casuali, la soluzione alla quale perviene la Corte è nel senso di un obbligo per l'autorità giudiziaria procedente di distruggere, nel più breve tempo possibile, le registrazioni *de quibus*: in effetti, in situazioni nelle quali le intercettazioni risultano inutilizzabili «per ragioni sostanziali, derivanti dalla violazione di una protezione "assoluta" del colloquio per la qualità degli interlocutori o per la pertinenza del suo oggetto», il contraddittorio consistente nel deposito e nell'udienza di stralcio «risulterebbe antitetic(o) rispetto alla *ratio* della tutela. L'accesso delle altre parti del giudizio, con rischio concreto di divulgazione dei contenuti del colloquio anche al di fuori del processo, vanificherebbe l'obiettivo perseguito, sacrificando i princìpi e i diritti di rilievo costituzionale che si intende salvaguardare». Per questi motivi, la Corte conclude che «non spettava alla Procura della Repubblica (*omissis*) di valutare la rilevanza delle intercettazioni di conversazioni telefoniche del Presidente della Repubblica» né «di omettere di chiedere al giudice l'immediata distruzione della documentazione relativa alle intercettazioni indicate (*omissis*) senza sottoposizione della stessa al contraddittorio tra le parti e con modalità idonee ad assicurare la segretezza del contenuto delle conversazioni intercettate».

11. *Le intercettazioni preventive*

Nell'ottica di prevenzione di reati di particolare gravità, il legislatore consente l'utilizzo di intercettazioni che sfuggono, per la loro funzione, alle finalità del processo penale. La loro regolamentazione è contenuta nelle disposizioni di attuazione del codice, che ne individua anzitutto i presupposti.

Ai sensi dell'art. 266, c. 1 disp. att. c.p.p., le intercettazioni preventiva sono disposte quando sia necessario acquisire «notizie concernenti la prevenzione dei delitti» di cui all'art. 407, c. 2, lett. *a*, n. 4 e all'art. 51, c. 3-bis c.p.p., nonché quelli di cui all'art. 51, c. 3-quater

[328] Di cui all'art. 12 della l. cost. 11 marzo 1953, n. 1.

c.p.p., commessi mediante l'impiego di tecnologie informatiche o telematiche[329]. Fra i presupposti generali rientrano, pertanto, i delitti di criminalità terroristica o mafiosa e assimilati. Legittimati a formulare la richiesta sono il ministro dell'interno o, su sua delega, i responsabili dei servizi centrali di polizia, carabinieri, guardia di finanza e DIA, mentre il soggetto che concede l'autorizzazione è il procuratore della repubblica presso il tribunale del capoluogo del distretto in cui si trova il "bersaglio" o, ove non determinabile, del distretto in cui sono emerse le esigenze di prevenzione. In ragione della caratteristica di indipendenza che l'assetto costituzionale riconosce al pubblico ministero, lo svolgimento delle intercettazioni preventive resta, come si vede, sotto il controllo di tale organo.

Accanto ai presupposti generali, l'art. 4 d.l. n. 144 del 2005, mod. dalla l. n. 133 del 2012, contempla alcuni presupposti speciali. In particolare, ai sensi di questa norma, le intercettazioni preventive sono disposte quando «siano ritenute indispensabili per la prevenzione di attività terroristiche o di eversione dell'ordinamento costituzionale», contrastate dai servizi segreti per la sicurezza dello Stato. Legittimati alla richiesta sono il presidente del consiglio dei ministri e i direttori dei servizi segreti (AISE e AISI), da lui delegati; soggetto che concede l'autorizzazione è il procuratore generale presso la corte d'appello di Roma.

Infine, una regolamentazione generale delle intercettazioni preventive è prevista dai commi 2-5 dell'art. 226 disp. att. c.p.p., ai sensi del quale la durata massima è di quaranta giorni, prorogabile per periodi successivi di venti giorni (c. 2). Delle operazioni svolte e dei contenuti intercettati viene redatto verbale sintetico, depositato presso il procuratore della Repubblica che ha autorizzato le attività entro cinque giorni dal termine delle stesse (c. 3). Il procuratore, verificata la conformità, dispone l'immediata distruzione dei supporti e dei verbali[330]; in ogni caso, gli elementi acquisiti non possono essere utilizzati nel procedimento penale, fatti salvi i fini investigativi (c. 5). Inoltre, le attività di intercettazione preventiva e le notizie acquisite non possono essere menzionate in atti di indagine né costituire oggetti di deposizione né essere altrimenti divulgate.

[329] V., per l'ultima modifica, d.l. n. 7 del 2015, conv. in l. n. 43 del 2015.

[330] In deroga a tale disciplina, procuratore può autorizzare, per un periodo non superiore a ventiquattro mesi, la conservazione dei dati acquisiti, anche relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, quando gli stessi siano indispensabili per la prosecuzione dell'attività finalizzata alla prevenzione dei delitti per i quali sono consentite le intercettazioni in oggetto (c. 3-bis, introdotto dal d.l. n. 7 del 2015, conv. in l. n. 43 del 2015).

La materia delle intercettazioni preventive è stata da ultimo attenzionata dal legislatore in occasione della complessa manovra finanziaria approvata per l'anno 2023[331]. A venire in rilievo sono, in particolare, le intercettazioni preventive effettuate dai Servizi di informazione per la sicurezza, cioè quelle dirette a «raccogliere informazioni utili per la prevenzione di gravi reati e non per l'acquisizione di elementi finalizzati all'accertamento della responsabilità per singoli fatti delittuosi»[332], ovvero espletabili «a prescindere dall'esistenza di una *notitia criminis* e dall'obiettivo di raccogliere prove utilizzabili in giudizio»[333]. Le c.d. intercettazioni preventive d'*intelligence*, introdotte nel nostro ordinamento ad opera dell'art. 4 del d.l. 27 luglio 2005, n. 144, convertito in l. 31 luglio 2005, n. 155, modificate dapprima nel 2007[334] e poi nel 2012[335], rappresentano una sorta di *tertium genus*, non essendo riconducibili né alle intercettazioni giudiziarie *ex* artt. 266 ss. c.p.p. né alle intercettazioni preventive di polizia *ex* artt. 226 disp. att. c.p.p. Di esse si è occupata la l. 29 dicembre 2022, n. 197, che, nel tentativo di approntare una «profonda revisione del sistema delle intercettazioni»[336], ha, in realtà, dato vita ad un impianto normativo che ben poche differenze presenta rispetto alla disciplina previgente. Si può invero individuare il *quid novi* della riforma nella definitiva emancipazione dell'istituto delle intercettazioni preventive d'*intelligence*, che finisce così per trovare integrale regolamentazione negli artt. 4 e 4-bis del d.l. 144 del 2005: se infatti la normativa previgente si limitava a richiamare le previsioni di cui all'art. 226, c. 1 disp. att. c.p.p., la novella stabilisce oggi in maniera analitica le singole *species* di captazioni esperibili: «l'intercettazione di comunicazioni o conversazioni, anche per via telematica, nonché l'intercettazione di comunicazioni o conversazioni tra presenti, anche se queste avvengono nei luoghi indicati dall'art. 614 c.p.».

Quanto ai presupposti legittimanti il decreto autorizzativo del procuratore generale presso la Corte d'appello di Roma, si prevede che le intercettazioni debbano risultare

[331] Cfr., in proposito, W. NOCERINO, *La riforma delle intercettazioni preventive d'intelligence*, in *Sistema Penale*, 2023.

[332] Così R. CANTONE - L. A. D'ANGELO, *Una nuova ipotesi di intercettazione preventiva*, in A. A. DALIA (a cura di), *Le nuove norme di contrasto al terrorismo*, 2006, p. 54.

[333] In tal senso G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, cit., p. 171 ss.

[334] L. 3 agosto 2007, n. 124.

[335] L. 7 agosto 2012, n. 133.

[336] In questi termini C. NORDIO, *Intervento al Senato*, 6 dicembre 2022, consultabile su *Sist. pen.*, 8 dicembre 2022.

"indispensabili" alle attività dei Servizi. L'aspetto maggiormente innovativo è, però, rappresentato dalla disciplina relativa alle modalità di svolgimento delle intercettazioni. Ai sensi del nuovo art. 4-bis, rientrano nel materiale oggetto di deposito presso il procuratore generale, oltre al verbale sintetico delle operazioni svolte e ai supporti utilizzati, anche i contenuti delle captazioni[337]; conseguentemente, anche i termini per procedere al deposito vengono rimodulati, estendendo la novella gli attuali 5 giorni a 30, decorrenti dalla conclusione delle operazioni, con possibilità di differire il termine per un periodo non superiore a 6 mesi[338]. Vengono quindi ampliati i doveri di distruzione di tutto il materiale consegnato, ivi compresi i contenuti intercettati e ogni eventuale copia, anche informatica, totale o parziale, degli stessi. A ciò si aggiunge l'obbligo per il procuratore di distruggere altresì la documentazione da lui stesso detenuta, decorsi 30 giorni dalla conclusione delle operazioni. I risultati delle attività che esulano dall'intercettazione *stricto sensu* intesa (c.d. controlli)[339] dovranno poi essere distrutti entro 6 mesi dall'acquisizione e i relativi verbali essere trasmessi al procuratore generale, ferma restando la possibilità per quest'ultimo di autorizzare la proroga del termine per la conservazione di tali dati per un periodo non superiore a 24 mesi. Novità di non poco rilievo è poi quella riguardante le eccezioni alle c.d. *exclusionary rules*: ai sensi del comma 5 dell'art. 4-bis, gli elementi acquisiti attraverso le attività preventive non possono essere utilizzati nel corso del procedimento penale né essere menzionati in atti di indagine, costituire oggetto di deposizione o essere altrimenti divulgati, ferma restando la possibilità di utilizzare quel materiale per «fini investigativi». Infine, viene previsto che le spese relative alle attività di intercettazione e tracciamento, attualmente a carico del Ministero della giustizia, siano imputate all'apposito programma di spesa iscritto nello stato di previsione della spesa del Ministero dell'economia e delle finanze, nell'ambito degli stanziamenti previsti a legislazione vigente[340]: per quanto la previsione *de qua* sia forse utile a chiarire la *ratio* dell'inserimento di tale riforma all'interno di una legge di bilancio, non si può comunque tacere come ciò contribuisca a rafforzare la riservatezza del comparto

[337] Art. 4-bis, c. 2, d.l. 144/2005.

[338] Previa autorizzazione del procuratore generale su richiesta motivata dei Direttori dei Servizi di informazione, comprovante particolari esigenze di natura tecnica e operativa.

[339] Si tratta del tracciamento delle comunicazioni telefoniche e telematiche, dell'acquisizione dei dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e dell'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni.

[340] Art. 1, c. 684, l. 197/2022.

dei Servizi d'*intelligence*, irrobustendo le garanzie di segretezza delle informazioni a disposizione di questi ultimi.

PARTE II

NODI CRITICI DELLA DISCIPLINA DELLE TECNOLOGIE DI CONTROLLO

CAPITOLO III

I NUOVI STRUMENTI DELLA TECNICA TRA VUOTO NORMATIVO E PROSPETTIVE *DE IURE CONDENDO*

SOMMARIO: 1. Libertà e sicurezza: i c.d. strumenti di osservazione occulta. – 2. Il captatore informatico (c.d. *trojan horse*): il problema della selezione dei dati. – 3. Gli altri mezzi atipici di ricerca della prova. – 3.1. Il pedinamento elettronico tramite *GPS*. – 3.2. Le perquisizioni *online* e l'acquisizione di dati conservati nel *cloud*. – 3.3. L'utilizzo dei droni a fini di *law enforcement*. – 3.4. Le videoriprese. – 3.5. Il riconoscimento facciale e l'impiego del *SARI*. – 3.6. Il cacciatore di *IMSI*. – 4. L'agente segreto attrezzato per il suono. – 5. I tabulati telefonici.

1. *Libertà e sicurezza: i c.d. strumenti di osservazione occulta*

Come osservava Damaska agli albori del nuovo millennio, «guardare al futuro del processo penale, oggi significa soprattutto parlare della progressiva adozione di modelli scientifici nell'indagine sui fatti (perché) un numero sempre più elevato di fatti rilevanti nel processo (può ormai essere dimostrato) soltanto con strumenti tecnici sofisticati»[341]. A questo proposito, si è già avuto modo di constare che l'evoluzione scientifica e tecnologica ha inciso profondamente anche sulle dinamiche dell'accertamento penale, cosicché si è assistito, nel corso dell'ultimo ventennio, al proliferare di penetranti strumenti investigativi, che hanno reso sempre più delicato il bilanciamento tra le opposte e contrapposte esigenze di libertà e sicurezza. Ora è, quindi, il momento di una rassegna dei principali ritrovati della tecnica che hanno innovato, nella prospettiva *de qua*, le investigazioni penali, focalizzando comunque l'attenzione sul problema di fondo della presente materia, ovvero l'imbarazzante *vulnus* normativo dal quale è affetta la disciplina dei nuovi mezzi di ricerca della prova. Il tema è tutt'altro che marginale, nella misura in cui coinvolge direttamente il rapporto tra individuo e autorità. In effetti, posto che il contributo tecnologico consente ormai di superare le "barriere fisiche", si rende quant'altri mai necessario ricorrere a "barriere giuridiche" che tutelino la nostra libertà. Ad onta di ciò, si registra uno iato tra il "dover essere" codicistico e l'"essere" della prassi, dovuto, per lo più, alla carenza di una base normativa. Questo dato appare ancora più allarmante, se si considera come sovente gli algoritmi, sottesi agli strumenti che assicurano una sicurezza totale, siano delle vere e proprie *black box*. Senza

[341] M. DAMASKA, *Il diritto delle prove alla deriva*, Bologna, 2003, p. 205.

contare il rischio che vengano annichiliti gli spazi riservati. Si contrappongono, quindi, un modello "assolutistico", caratterizzato dall'impiego massiccio dei ritrovati della tecnica, e i valori della democrazia; in breve, l'intelligenza artificiale e i diritti. Tuttavia, nell'ipersecuritaria realtà globalizzata, non si può certo liquidare come una romantica sensibilità novecentesca l'attenzione alla protezione dei dati, il trattamento dei quali incide proprio sulle libertà fondamentali.

Nell'attuale scenario della sorveglianza globale si collocano, pertanto, gli strumenti di osservazione occulta, i quali segnalano l'ormai irreversibile dipendenza del processo penale dall'intelligenza artificiale. Senonché, «mentre cittadini e giuristi sono (fortunatamente) sempre più consapevoli dei vantaggi e dei rischi causati da indagini scientificamente avanzate, il potenziale sviluppo delle tecnologie automatizzate per rafforzare i diritti di difesa resta ad oggi in gran parte inesplorato. Ciò, da una parte, tende a fornire una immagine incompleta e talvolta distorta dei sistemi di IA in ambito penale; dall'altra, a non stimolare l'espansione di questi strumenti su fronti applicativi diversi ed innovativi»[342]. A fronte di siffatta simmetria, il dilemma che si pone è se ci si debba difendere "dalla" intelligenza artificiale o "con" l'intelligenza artificiale[343]. In proposito, la strada indicata da taluno è stata quella del «diritto al rimedio effettivo»[344]. Per quanto diverse disposizioni sovranazionali riconoscano espressamente questo diritto, segnatamente gli artt. 13 CEDU e 47 CDFUE, non mancano i profili di vaghezza connessi alla nozione di tale "rimedio". All'interno dell'Unione[345], si è delineato un modello incentrato sul «rigetto di una delega totale all'automazione e sull'esercizio di un controllo *ex post* da parte di un essere umano sulle valutazioni emesse dai sistemi di IA»[346], ma si può forse dubitare, alla luce delle conoscenze tecniche oggi in possesso da parte dell'operatore giuridico medio, che, per garantire l'effettività dei diritti di difesa allorché siano in gioco sistemi di IA, quella della revisione umana sia la migliore opzione possibile.

---

[342] G. LASAGNI, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma*, in G. DI PAOLO-L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Trento, 2022, p. 64.

[343] *Ibidem*.

[344] *Ibidem*, p. 66.

[345] V., in particolare, l'art. 11 della Direttiva 2016/680.

[346] G. LASAGNI, *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale?*, cit., p. 70.

Certo è che l'intelligenza artificiale non appartiene più alla fantascienza ed è sempre più presente nella nostra quotidianità: dalle macchine a guida automatica all'uso del *machine learning* nei servizi di implementazione del sistema sanitario; dai dispositivi finalizzati a individuare le truffe *online* agli assistenti domotici come *Google Home* e *Alexa*; dalle *chatbot* ai dispositivi di *smart compose* di *gmail*. Nell'ambito del procedimento penale, che, com'è noto, è un meccanismo di ricostruzione della realtà[347], l'impiego di dispositivi basato sull'IA si sta diffondendo in diversi ambiti.

Anzitutto, nell'ambito della prevenzione, rilevano i *software* di *predictive policing*, come il *PredPol*[348] o, guardando all'esperienza italiana, il *Key crime*[349], adottato dalla Questura di Milano, oppure l'*X-Law*[350], un *software* elaborato dalla Questura di Napoli e completato dal Dipartimento di Pubblica Sicurezza del Ministero dell'Interno e utilizzato in diverse realtà del nostro Paese.

Quanto all'ambito "probatorio", occorre tenere distinte le *digital* o *automated evidence* di ultima generazione[351] – come i captatori o i *tool* di riconoscimento facciale – dalle c.d. *machine-evidence* o *e-evidence*. In merito alle prime, si riscontra, nella fase delle indagini preliminari, un impiego sempre più ampio di sistemi basati su prove algoritmiche in senso lato, destinato a crescere notevolmente con l'esplosione dell'*Internet of Things*[352]: in altri

[347] G. GIOSTRA, *Prima lezione sulla giustizia penale*, Bari, 2020, p. 6 utilizza, per descrivere il procedimento penale, l'efficace metafora del potente tibetano, che consente di transitare dalla *res iudicanda* alla *res iudicata*.

[348] Si tratta di un programma messo a punto da matematici e criminologi che identifica le zone della città dove si verificano i crimini con maggiore probabilità.

[349] È un *software* capace di predire le rapine in base a giorno, ora e luogo degli eventi già accaduti, correlando dettagli sui criminali coinvolti e sulle loro armi.

[350] Consiste in una forma di IA dotata di un algoritmo di tipo euristico che, sulla base dell'acquisizione di caratteristiche socio-ambientali del territorio in esame e dei delitti quotidiani consumati e scoperti dalle denunce di cittadini o da altre informazioni di Polizia o di attività di prossimità, ricerca e mostra modelli criminali che si configurano sul territorio in maniera ciclica e stanziale, prevedendone la singola e regolare distribuzione spazio temporale.

[351] Le definizioni alludono qui, la prima, a ogni forma di raccolta ed impiego procedimentali di «dati originariamente contenuti in supporti informatici o telematici, oppure ancora trasmessi in modalità digitale» (M. PITTIRUTI, Digital evidence *e procedimento penale*, Torino, 2017, p. 8); la seconda, all' «impiego processuale di dati conoscitivi che siano trattati e generati automaticamente, attraverso algoritmi», più o meno sofisticati (S. QUATTROCOLO, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Espanola de derecho procesal*, 2019, p. 3). Per una panoramica più completa, v. inoltre, M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. Pen. Cont.*, 2019.

[352] L'esempio paradigmatico è quello del frigorifero intelligente che offre informazioni sulla temperatura in una stanza.

termini, si assiste ad una diffusione degli elementi di prova nascenti da un'elaborazione automatizzata di un algoritmo che governa il *software*. Le seconde, invece, saranno prodotte dalla stessa automobile a guida automatizzata nell'ipotesi di incidenti generati da una cooperazione tra uomo e robot. Resta, in ogni caso, comune il quesito di fondo, ovvero se si debba giungere alla conclusione che la prova digitale è "impermeabile" al confronto dialettico. Per verificare l'attendibilità dei dati, bisognerebbe infatti risalire al codice sorgente, ma, per ragioni commerciali o di tutela della proprietà intellettuale, questo è sovente segreto. Il risultato di questa sostanziale impossibilità di verificare l'attendibilità della prova è quello che si definisce "asimmetria cognitiva" (*knowledge impairment*).

Infine, l'ambito decisorio risulta interessato dalla giustizia predittiva in senso lato: al suo interno è possibile distinguere la giustizia predittiva in senso proprio, consistente nell'analisi di un cospicuo numero di pronunce giudiziali effettuato tramite tecnologie di IA al fine di elaborare previsioni quanto più precise e attendibili in ordine al possibile di esito di alcune specifiche tipologie di controversia, dai c.d. *risk assessment tools*, vale a dire algoritmi, a loro volta spesso fondati sull'IA, in grado di calcolare il rischio che un prevenuto si sottragga al processo o commetta dei reati.

Se manifesti sono i benefici della tecnologica per la giustizia penale, soprattutto in termini di efficienza, non possono nondimeno tacersi i rischi derivanti da un loro impiego massivo. A ciò si deve aggiungere che l'esigenza di avvalersi in sede penale di prodotti di aziende private, come gli strumenti di captazione o di sorveglianza elettronica, «per la gestione dei quali è spesso necessario avvalersi dei servizi dei privati che producono la tecnologia acquistata e che soli dispongono del *know how* per garantirne il funzionamento e la supervisione»[353], sembra indirizzare il sistema penale verso «una progressiva privatizzazione di aree rilevanti dell'amministrazione giudiziaria»[354]. Vi è poi il tutt'altro che trascurabile problema della tendenza naturalmente espansiva degli strumenti tecnologicamente avanzati[355].

[353] C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, vol. 5, n. 3, 2019, p. 1174-1775.

[354] *Ibidem*, p. 1175.

[355] La questione si pone con particolare riguardo alla gestione dei dati personali che possono essere raccolti attraverso i mezzi di sorveglianza elettronica, come nel caso dei *virus* informatici o della sorveglianza mediante GPS.

Vero è che l'utilizzo delle tecnologie avanzate in ambito penale impatta pesantemente sulle tradizionali aree di libertà garantite ai singoli, «rispetto alle quali siamo avvezzi a una tipologia di aggressioni e limitazioni che poco ha oramai a che vedere con quella (spesso immateriale e quindi non avvertibile) collegata a mezzi tecnologicamente sofisticati»[356]. Un esempio calzante è dato dalla sorveglianza elettronica mediante geolocalizzazione, che ha fatto capolino in Italia sotto le vesti del pedinamento elettronico. Se l'uso della tecnologia nel procedimento penale entra quindi in tensione con i diritti fondamentali dei singoli, mettendo alla prova le garanzie che li circondano, la "civiltà delle macchine", per contro, implementa il sistema con nuovi concetti, «che si collocano lungo i confini semantici degli istituti "tradizionali" e ne forzano il senso, sfidando l'interprete a stabilire dove collocarli»[357]: è il caso dell'"identità digitale"[358], che pone il problema se siano coperte dallo *ius tacendi* anche le coordinate identificative riconducibili a tale nozione.

Ciò detto, non si può che denunciare, ancora una volta, il difetto di un *corpus* normativo dedicato alla disciplina dell'intelligenza artificiale. Se vi è infatti un indice utile a desumere l'irragionevole vetustà del nostro procedimento penale, quello è dato senz'altro dall'incapacità cronica di assimilare l'evoluzione tecnologica. All'indomani dell'esperienza pandemica, che ha segnato una prima e timida apertura al digitale, l'auspicio è, pertanto, quello che il legislatore si decida ad affrontare una volta per tutte la transizione digitale.

2. *Il captatore informatico (c.d.* trojan horse*): il problema della selezione dei dati*

Emblema dello "sfruttamento" tecnologico a fini di *law enforcement* e in fase di repressione, il captatore informatico è stato definito «un Giano bifronte»[359]: nell'intento di delineare lo stato dell'arte relativo a questo insidioso mezzo di ricerca della prova, di esso è stato posto in luce il duplice impiego, sia a fini repressivi che esplorativi. Si è già avuto modo

[356] C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale*, cit., p. 1178.

[357] *Ibidem*, p. 1180.

[358] Cioè il *nickname* o l'*avatar* di chi svolge attività in rete.

[359] W. NOCERINO, *Il captatore informatico: un Giano bifronte. Prassi operative vs risvolti giuridici*, in *Cass. pen.*, 2020, p. 824.

di tracciare, almeno in parte, quella che è stata l'«odissea»[360] del captatore informatico, disciplinato prima in via pretoria e solo successivamente in via legislativa. Da questo punto di vista, si può dire che la vicenda che lo riguarda valga a stigmatizzare il "puntuale ritardo" con il quale il legislatore si fa carico di codificare gli sviluppi della prassi, senza neppure offrire una disciplina sistematica e di ampio respiro in relazione agli specifici istituti che vengono di volta in volta in rilievo.

Strumenti "diabolici" e dalla capacità intrusiva sconfinata, «i "captatori" sono *virus* (riconducibili alla classe dei *trojan horses*) che "conquistano i diritti d'amministrazione" del sistema in cui vengono iniettati, assumendone il controllo»[361]. La loro potenzialità investigativa è a dir poco sorprendente: sono capaci di «leggere ciò che è archiviato nel dispositivo, dai documenti di testo alla rubrica degli indirizzi *e-mail*, dall'elenco dei contatti ai siti "preferiti" sino ad ogni singola comunicazione scambiata in *chat* con programmi di messaggistica come *Whatsapp*, *Telegram*, *Messenger*; può gestire i *software* che vi sono installati; controllare e scaricare le immagini e i filmati presenti nelle gallerie; collegarsi ad *Internet*; registrare i dati in partenza e quelli in arrivo (*omissis*); memorizzare i pulsanti premuti sulla tastiera dell'apparecchio (*omissis*); inserire dati nuovi o distruggere quelli esistenti, alterando irreversibilmente l'archivio; fotografare quel che viene visualizzato sullo schermo (*omissis*); se l'apparecchio è un portatile o uno *smartphone* dotato di *gps*, può "tracciarne" gli spostamenti; può accendere il microfono o la *cam*, trasformandoli in una "cimice informatica" che consente di svolgere un'intercettazione ambientale o una ripresa video»[362]. Questi *virus* possono essere inoculati fisicamente nell'apparecchio di cui ci si sia impadroniti ovvero essere mandati da lontano, ad esempio come allegato ad una *e-mail* o sotto le vesti di una comunicazione inviata da servizi di messaggistica o, ancora, come aggiornamento di un *software*.

Come ricordato, lo strumento in discorso viene attenzionato dapprima soltanto dalla giurisprudenza. La prima pronuncia della Cassazione sull'argomento[363] concerne l'utilizzo del captatore al fine di esaminare i *file* memorizzati sul *computer* di un dipendente pubblico, collocato all'interno del suo ufficio. In quella vicenda, la Corte, pur senza dedicare la dovuta

[360] F. CAJANI, *L'odissea del captatore informatico*, in *Cass. pen.*, 2016, p. 4140.

[361] A. CAMON, *Cavalli di Troia in Cassazione*, in *Arch. nuova proc. pen.*, 2017, p. 91.

[362] *Ibidem*.

[363] Cass. sez. V, 14 ottobre 2009, n. 16556, Virruso ed altri.

attenzione ai profili del diritto alla riservatezza e del domicilio informatico, esclude la possibilità di applicare la disciplina delle intercettazioni, non essendo l'oggetto del controllo una comunicazione, e conclude nel senso della legittimità della manovra in forza della norma in tema di prove atipiche (art. 189 c.p.p.).

Qualche tempo dopo, la Corte viene chiamata a confrontarsi con i captatori quali strumenti per azionare a distanza il microfono di un apparecchio ed eseguire così un'intercettazione ambientale[364]. In particolare, il quesito che viene posto alle Sezioni Unite è «se – anche nei luoghi di privata dimora *ex* art. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa – sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un "captatore informatico" in dispositivi elettronici portatili (*omissis*)». Come si intuisce, si tratta di una vicenda dai contorni più delicati rispetto a quella del 2009, in quanto l'introduzione del *malware* all'interno di un cellulare, anziché di un *computer* fisso, è in grado di rendere lo strumento d'indagine assai più invasivo. In questa occasione, la Corte, proprio in considerazione della natura itinerante dei dispositivi adoperati come microspie, afferma che il captatore è utilizzabile per realizzare intercettazioni "tra presenti" nei soli procedimenti per delitti di criminalità organizzata: in tali casi, infatti, trova applicazione la disciplina di cui all'art. 13 del d.l. n. 151 del 1991, convertito dalla l. n. 203 del 1991, che, derogando ai presupposti fissati dall'art. 266, c. 2 c.p.p., consente la captazione anche nei luoghi di privata dimora, senza che sia necessario che tali luoghi siano sedi di attività criminosa in atto. Al contrario, viene escluso l'utilizzo del mezzo di ricerca della prova per i reati comuni, in quanto, non essendo possibile formulare *ex ante* una previsione dei luoghi di privata dimora nei quali il dispositivo portatile potrebbe essere introdotto al momento dell'autorizzazione, si renderebbe impossibile verificare il rispetto della condizione di legittimità prevista dall'art. 266, c. 2 c.p.p., il quale presuppone, per la legittimità delle captazioni in luoghi domiciliari, che sia in atto l'attività criminosa.

La sentenza *de qua* ha suscitato un acceso dibattito, nell'ambito del quale si sono manifestate posizioni contrastanti[365]. In proposito, sono state avanzate tre riserve al *decisum*

[364] Cass., Sez. un. 28 aprile 2016, n. 26889, Scurato.

[365] Un orientamento ha espresso critiche decise, che sono state compendiate in una "*Denuncia dei rischi connessi all'installazione occulta di virus informatici su smartphone e tablet per finalità di indagine penale*", diffusa nel luglio 2016 da alcuni docenti universitari, con la quale, traendo spunto dalla preoccupazione ingenerata dal fatto che le Sezioni unite avevano affermato la legittimità, sia pure a determinate condizioni, dello strumento in esame per compiere intercettazioni, si è auspicato l'intervento del legislatore per regolare la materia, al fine di realizzare un adeguato bilanciamento dei principi costituzionali e convenzionali coinvolti.

delle Sezioni Unite[366]. In primo luogo, una prognosi ragionevole può portare ad escludere uno "spostamento" dell'intercettazione, come nel caso in cui il *virus* venga iniettato in un *computer* portatile che, di fatto, è abitualmente tenuto fermo[367].

In secondo luogo, un'intercettazione pressoché certa di dialoghi che si svolgono in un domicilio potrebbe avvenire solo laddove il *virus* tenesse costantemente attivo il microfono del dispositivo infettato, circostanza che si verifica di rado. In effetti, molti programmi consentono di accenderlo e spegnerlo a richiesta e, comunque, un'intercettazione continuativa causerebbe un consumo rilevante della batteria, così aumentando il rischio di essere scoperti. Alla luce di ciò, appare preferibile limitare a determinate fasce orarie l'attivazione del microfono piuttosto che affiancare l'intercettazione ad un pedinamento, tradizionale o elettronico, dell'imputato: in questo modo, sarà possibile avviare la registrazione solo allorché quest'ultimo si trovi all'aperto ovvero all'interno di quel domicilio nel quale si ha motivo di pensare che l'attività criminosa sia in corso»[368].

In terzo luogo, resta ferma la garanzia "postuma", rappresentata dallo stralcio delle conversazioni avvenute nei luoghi di cui all'art. 614 c.p., per il caso in cui le stesse rimangano effettivamente impigliate nelle maglie dell'intercettazione, in difetto di un preventivo accertamento dell'organo giurisdizionale circa la sussistenza del fondato motivo di ritenere che nel luogo di privata dimora si stia svolgendo l'attività criminosa.

Rebus sic stantibus, si può concludere che la soluzione offerta dalle Sezioni Unite non "discenda" direttamente dalle norme, essendo piuttosto il frutto di un compromesso: se da un lato si decide di dare spazio al captatore, dall'altro se ne tracciano in maniera rigorosa i

---

Una diversa opinione (R. ORLANDI, *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Arch. pen*. (*web*), 25 luglio 2016), invece, ha invitato a distinguere l'uso della moderna tecnologia informatica per effettuare intercettazioni tra presenti – che trova nelle disposizioni dapprima citate la fonte "base normativa" – dal suo impiego per svolgere altre attività di ricerca della prova, come perquisire a distanza gli archivi di *computer, tablet, smartphone*. Sotto quest'ultimo aspetto è stato affermato che l'impiego del nuovo strumento esulerebbe dal raggio d'azione degli artt. 14 e 15 Cost. e, dunque, non basterebbe l'introduzione di una specifica disciplina normativa, ma sarebbe necessario l'affermazione di un nuovo diritto fondamentale all'uso libero e riservato delle tecnologie informatiche, sul modello di quanto avvenuto in altri ordinamenti ed in particolare in Germania, a partire da una nota sentenza Bundesverfassungsgericht 27 febbraio 2008, in *Riv. trim. dir. pen. econ*., 3, 2009, 679 e ss., con nota di R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung*.

[366] Cfr., sul punto, A. CAMON, *Cavalli di Troia in Cassazione*, cit., p. 93 ss.

[367] L'esempio è di G. AMATO, *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un "captatore informatico"*, in *Guida dir.*, 2016, n. 34-35, p. 79.

[368] Cfr. A. CAMON, *Cavalli di Troia in Cassazione*, cit., p. 93.

confini, limitandone l'impiego ai soli reati di particolare gravità. In altri termini, «in considerazione della profonda invasività del mezzo tecnologico in esame e dei connessi rischi per la libertà di comunicare anche degli eventuali terzi che entrano in contatto con il detentore del dispositivo "infettato", le Sezioni unite non hanno voluto legittimare l'adozione di un'autorizzazione di intercettazioni "al buio", cioè concessa dal giudice senza poter valutare preventivamente lo svolgimento di attività criminosa nel luogo domiciliare in cui potrebbe essere introdotto il dispositivo, ritenuto non prevedibile»[369].

Al fine di cogliere gli ulteriori sviluppi che hanno interessato la disciplina del captatore informatico a seguito degli interventi legislativi, qualche precisazione merita la teoria della "intercettazione ambientale itinerante"[370], enucleata dalla Suprema Corte, nella prospettiva di escludere l'intercettazione di comunicazioni fra presenti con lo strumento in questione, anche in ambiente non domiciliare, nei procedimenti per reati comuni, e di ammetterla invece nei procedimenti per reati di criminalità organizzata. Da un punto di vista metodologico, infatti, questa teoria, focalizzando l'attenzione sulla struttura tecnica del captatore, funge da argomento utile a predicarne l'utilizzabilità nel solo settore dei reati di criminalità organizzata, ovvero quella classe di delitti in cui non opera il limite di ammissibilità delle intercettazioni domiciliari *ex* art. 266, c. 2 c.p.p., che, imponendo l'indicazione del luogo *ex ante*, risulterebbe incompatibile con la peculiare natura dello strumento probatorio. Da un punto di vista interpretativo, si argomenta, invece, che la nozione evocata ribalda l'opzione ermeneutica della necessaria predeterminazione dei luoghi dell'intercettazione ambientale, in quanto la legge processuale si limita a menzionare l'"ambiente" al solo fine di tutelare il domicilio, mentre da nessun'altra parte si desume l'obbligo di indicare i luoghi dell'intercettazione tra presenti.

Sul presupposto di questo orientamento giurisprudenziale, si innesta il ricordato d.lgs. n. 216/2017, che, superando l'asserita incompatibilità tra impiego del captatore e applicazione della disciplina codicistica, «ammette l'inserimento del captatore informatico nei dispositivi elettronici portatili, ai fini d'intercettazione delle comunicazioni fra presenti, anche nei procedimenti per reati comuni e non solo di criminalità organizzata (art. 266,

[369] L. GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sistema penale*, 4/2020, p. 112.

[370] V., in proposito, M. BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 2018, p. 5 ss.

comma 2, primo periodo, c.p.p, nuovo testo)»[371]. Per altro verso, tuttavia, il legislatore sembra far rientrare dalla finestra ciò che ha fatto uscire dalla porta: infatti, lo stesso decreto n. 216, nel consentire le intercettazioni domiciliari attraverso il captatore nei soli casi in cui ricorra una condizione analoga a quella prevista dall'art. 266, c. 2 c.p.p., ovvero il motivo di ritenere che nei luoghi domiciliari si stia svolgendo l'attività criminosa, mantiene la distinzione tra delitti comuni e delitti di criminalità organizzata, facendo salvi i reati di cui all'art. 51, c. 3-bis e 3-quater c.p.p., rispetto ai quali l'uso del captatore è sempre consentito ai sensi del nuovo c. 2-bis dell'art. 266 c.p.p.[372] Peraltro, è appena il caso di precisare che, fra le novità introdotte dalla c.d. riforma Orlando, figura la previsione per la quale, nell'ipotesi di intercettazioni domiciliari eseguite, nei procedimenti per reati comuni, tramite captatore, occorre indicare, nel provvedimento autorizzativo, il luogo di attivazione del microfono[373], mentre, in base al nuovo disposto di cui all'art. 267, c. 1 c.p.p., non pare potersi desumere che il luogo dell'intercettazione debba essere individuato e indicato *ex ante* anche per le intercettazioni extradomiciliari. In questo modo, viene superato «l'equivoco in cui era caduta la Suprema Corte quando, nella decisione a Sezioni Unite del 2016, aveva concluso per l'inapplicabilità dell'art. 266, comma 2 c.p.p. all'intercettazione mediante captatore, sul rilievo (*omissis*) dell'imprevedibilità (e incontrollabilità) dei luoghi in cui l'apparecchio "infettato" verrà introdotto»[374].

Com'è noto, il legislatore è nuovamente intervenuto in materia con la l. 9 gennaio 2019, n. 3, per poi completare il mosaico normativo con la l. n. 7 del 2020. Tra le novità più rilevanti si segnala l'ampliamento delle ipotesi in cui l'art. 266, c. 2-bis c.p.p. consente sempre l'utilizzo del captatore informatico, nell'ambito delle quali sono ricompresi, oltre ai reati dei pubblici ufficiali contro la pubblica amministrazione, anche quelli commessi dagli incaricati di pubblico servizio. Allo stato dell'arte, pertanto, anche in procedimenti relativi ai più gravi reati contro la pubblica amministrazione l'intercettazione tra presenti mediante *trojan* risulta sempre consentita e potrà ordinariamente avvenire all'interno del domicilio: in

[371] M. BONTEMPELLI, *Il captatore informatico*, cit., p. 7.

[372] Parla, al riguardo, di una presunzione legale assoluta di «continuità della condotta criminosa», R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv.it. dir. proc. pen.*, 2018, p. 554.

[373] Così da poter accertare la condizione di cui all'art. 266, c. 2 c.p.p.

[374] M. BONTEMPELLI, *Il captatore informatico*, cit., p. 8.

tal caso, l'autorizzazione dovrà essere sempre subordinata alla previa indicazione delle ragioni che consentono l'attivazione del *virus* anche nei luoghi indicati dall'art. 614 c.p.

Il d. l. 161 del 2019 ha altresì riformato la disciplina dell'art. 270 c.p.p., sulla quale già era intervenuto l'art. 4 del d.lgs. n. 216 del 2017, prevedendo una limitazione all'utilizzo dei risultati delle intercettazioni compiute a mezzo di captatore informatico in procedimenti diversi da quello nel quale erano state autorizzate. Sul punto, il nuovo c. 1-bis dell'art. 270 c.p.p. prevede oggi che «i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione qualora risultino indispensabili per l'accertamento dei delitti indicati dall'art. 266, comma 2-bis».

Merita, a questo punto, ricordare un risalente insegnamento della Corte costituzionale[375], che, nel qualificare il diritto alla libertà e alla segretezza della corrispondenza e di ogni altra forma di comunicazione come «parte necessaria di quello spazio vitale che circonda la persona e senza il quale non questa non può esistere e svilupparsi in armonia con i postulati della dignità umana», ha individuato un duplice fondamento della sua inviolabilità, facente capo agli artt. 2 e 15 Cost. Ad avviso del giudice delle leggi, infatti, «il diritto a una comunicazione libera e segreta è involabile, nel senso generale che il suo contenuto essenziale non può essere oggetto di revisione costituzionale, in quanto incorpora un valore della personalità avente un carattere fondante rispetto al sistema democratico voluto dal Costituente»; per altro verso, «lo stesso diritto è inviolabile nel senso che il suo contenuto di valore non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante, sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse e sia rispettata la duplice garanzia che la disciplina prevista risponda ai requisiti propri della riserva assoluta di legge e la misura limitativa sia disposta con atto motivato dell'autorità giudiziaria».

Pur alla luce di tali rilievi, la normativa oggi vigente per il captatore informatico risulta, per molti versi, insoddisfacente. Anzitutto, restano oscure le ragioni per le quali il legislatore abbia inserito, all'art. 266, c. 2 e 2-bis c.p.p., un riferimento al solo «dispositivo elettronico portatile». A destare le maggiori perplessità, tuttavia, è soprattutto la mancanza di una disciplina riferita a ciò che non costituisce intercettazione in senso stretto: si tratta di un

[375] Corte cost., sent. 11 luglio 1991, n. 366.

vulnus non indifferente, considerata la mole di dati che questo performante strumento intrusivo è in grado di raccogliere. In altri termini, l'utilizzo del *trojan* è stato affrontato solo dal punto di vista del suo utilizzo all'interno delle c.d. intercettazioni ambientali, lasciando privo di base giuridica lo spinoso problema delle perquisizioni da remoto degli archivi di *computer*, *tablet* e *smartphone*, nonché quello relativo alla possibilità di utilizzare programmi che effettuano *screenshot*. A questo proposito, non è superfluo rammentare come la garanzia costituzionale di cui all'art. 14 Cost. sia stata estesa anche al c.d. domicilio informatico, definito alla stregua di 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»[376]. Sulla scorta di ciò, una parte della dottrina[377] ha parlato di "perquisizioni *online*", ponendo l'accento sulla peculiarità di tale strumento d'indagine rispetto alle perquisizioni tradizionali, alle ispezioni, al pedinamento e alle stesse intercettazioni. Certo è che, ad oggi, il dibattito è aperto: tutte le operazioni che esulano dall'intercettazione tra presenti vengono lasciate alla delicata valutazione della giurisprudenza, chiamata, ancora una volta, a rimediare all'inerzia del legislatore.

3. *Gli altri mezzi atipici di ricerca della prova*

Dopo l'entrata in vigore del codice del 1988, grazie al progresso scientifico, è stata elaborata una serie di mezzi atipici di ricerca della prova, come le videoriprese e il pedinamento satellitare tramite GPS, di cui tuttavia il codice non fornisce una disciplina specifica. L'unica norma che si riferisce a questi strumenti è l'art. 189 c.p.p.[378], il quale pone

[376] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. bras. dir. proc. pen.*, vol. 3, 2/2017, p. 491.

[377] S. MARCOLINI, *Le cosiddette perquisizioni online (o perquisizioni elettroniche)*, in *Cass. pen.*, 2010, p. 2855 ss.

[378] In effetti, l'art. 189 c.p.p. dovrebbe estendersi non solo ai mezzi di prova (come le ricognizioni informali), ma anche ai mezzi di ricerca della prova e alle attività di indagine atipiche della polizia giudiziaria (riconoscimento fotografico, controllo satellitare tramite GPS, videoriprese di condotte o spostamenti di persone, *bloodstain pattern analysis*, accessi a sistemi informatici).

come suoi requisiti l'idoneità dell'accertamento, la mancanza di pregiudizio per la libertà morale della persona e il previo contraddittorio davanti al giudice chiamato a regolare le specifiche modalità di assunzione della prova. Il problema consiste nel fatto che la norma in questione, ancorché collocata fra i princìpi generali della prova, si pone in maniera stridente rispetto ai connotati dei mezzi di ricerca della prova, che, per loro natura, vengono compiuti in segreto durante le indagini e appaiono, perciò, difficilmente conciliabili con un previo contraddittorio davanti al giudice. Il nodo è stato sciolto dalla giurisprudenza costituzionale, che, nel riconoscere il rilievo costituzionale dell'esigenza di accertamento dei reati[379], ha legittimato un contraddittorio "postumo", cioè compiuto nel momento in cui i risultati dei mezzi atipici di ricerca della prova vengono ammessi dal giudice: in questo modo, viene rimandato *ex post* l'accertamento sulla sussistenza dei requisiti previsti dall'art. 189 c.p.p. Ciò detto, si può procedere ad una panoramica dei principali mezzi atipici di ricerca della prova, che, per quanto non esaustiva, contribuisce a offrire una quadro più completo dello stato dell'arte, caratterizzato da un ingiustificato vuoto normativo al quale la giurisprudenza tenta di dare risposta attraverso il suo ruolo suppletivo.

3.1 *Il pedinamento elettronico tramite* GPS

Uno dei più controversi mezzi atipici di ricerca della prova è indubbiamente il pedinamento elettronico effettuato tramite GPS. Se possiamo definire il pedinamento "tradizionale" come quell'attività mediante la quale si segue con circospezione una persona, al fine di spiarne i comportamenti e la cui utilità dipende dal fatto che la persona occultamente seguita non si accorga di esserlo, la prassi investigativa si è oggi arricchita di sistemi elettronici che consentono di localizzare una persona o una cosa a distanza rispetto all'inquirente. Invariata la funzione, a cambiare sono, come s'intuisce, le modalità di espletamento, in quanto gli spostamenti della persona da pedinare vengono esaminati da

[379] Si veda, in proposito, Corte cost. 27 giugno 1996, n. 238, che si è occupata del prelievo coattivo per l'esame del DNA.

remoto, attraverso strumenti tecnologici, che permettono di evitare lo spostamento fisico dell'operatore sul luogo d'interesse.

Si distinguono due sistemi per mezzo dei quali il pedinamento a distanza può realizzarsi. Il primo è quello di localizzazione cellulare, che sfrutta il sistema di "celle" di copertura della telefonia mobile, in cui il territorio terrestre viene suddiviso: in questo modo la potenza del segnale radio di ogni cella telefonica viene analizzata in relazione alle coordinate geografiche della rispettiva stazione radio base, collegata con il dispositivo mobile o terminale e la distanza da tale stazione viene determinata in base alla conoscenza dell'attenuazione dell'ambiente di radiopropagazione[380]. Dall'altro lato, il pedinamento a distanza può avvenire mediante sistemi di tipo satellitare. Il riferimento è qui alla tecnologica *Global Positioning System* (GPS), che permette di determinare con estrema precisione la posizione di un oggetto sulla superficie terrestre, in termini di latitudine, longitudine e altezza, nonché di seguirne il movimento e calcolarne la velocità, grazie ad una rete di 24 satelliti collocati a circa 20.000 Km d'altezza e suddivisi in 6 rotte orbitali[381]: in forza di ciò, i satelliti trasmettono un segnale radio e attraverso l'elaborazione dei segnali ricevuti da parte del ricevitore sulla Terra avviene la localizzazione. L'impiego di questa tecnologia nelle indagini avviene tipicamente attraverso l'installazione occulta della stazione che riceve il segnale satellitare sull'autovettura del soggetto, i cui spostamenti intende monitorare l'organo inquirente.

La portata dirompente di questi innovativi strumenti di monitoraggio rispetto alla tradizionale fisionomia del pedinamento si coglie *ictu oculi*, ma, come anche gli altri mezzi ad elevato tasso tecnologico, questi strumenti di indagine pongono non pochi dubbi dal punto di vista delle ricadute processuali. Per questa ragione, nel silenzio della legge, la giurisprudenza si è a lungo affaticata nel tentativo di chiarificare la natura giuridica della geolocalizzazione, pervenendo ad una soluzione non del tutto convincente. La posizione oggi dominante è, infatti, nel senso di ritenere il pedinamento elettronico tramite GPS niente più che una forma di "pedinamento" eseguita con strumenti tecnologici, non assimilabile in

[380] R. OLIVIERI, *I sistemi di geolocalizzazione e l'analisi forense degli smartphone*, in G. COSTABILE-A. ATTANASIO-M. IANULARDO (a cura di), *IISFA Memberbook 2014. Digital forensics. Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER*, Forlì, 2015, pp. 141 ss.

[381] M. TORRE, *Indagini informatiche e processo penale*, Firenze, 2016, p. 159.

alcun modo all'attività di intercettazione prevista dagli artt. 266 ss. c.p.p.[382]: per l'effetto, questa forma di attività investigativa non necessiterebbe di alcuna autorizzazione preventiva da parte del giudice per le indagini preliminari, poiché, costituendo un mezzo atipico di ricerca della prova, rientra nella libera competenza della polizia giudiziaria. In altri termini, ad avviso della Suprema Corte, la rilevazione della persona pedinata attraverso il sistema di monitoraggio GPS non implicherebbe la compressione di alcun diritto fondamentale.

A tale orientamento è possibile muovere ragionevoli critiche. Il bene giuridico leso attraverso questo tipo di attività investigativa pare infatti riconducibile al diritto alla riservatezza, tutelato dagli artt. 2, 17 e 8 della CEDU, come conferma la giurisprudenza della Corte di Strasburgo. In particolare, in una pronuncia del 2009[383], la Corte e.d.u. ha rilevato che il pedinamento elettronico interferisce con il diritto al rispetto della vita private e deve, per questo, essere supportato da adeguate garanzie e da una solida base legale, nonché risultare proporzionato rispetto al sussistente livello di gravità. Nel caso di specie, il "test" è stato positivamente superato dalla Germania, in quanto, pur non essendo contemplata una preventiva autorizzazione giudiziale, la disciplina tedesca prevede un meccanismo di controllo *ex post* volto a verificare la legittimità, l'opportunità e la necessità di prolungare nel tempo il ricorso al GPS; inoltre, nel caso posto all'attenzione dei giudici di Strasburgo, l'impiego della peculiare modalità investigativa in questione risultava del tutto giustificata dalla gravità dei fatti – nella specie, reati di stampo terroristico – per i quali si procedeva.

Ad una soluzione analoga è pervenuta la Corte e.d.u. nel 2018[384]. La vicenda aveva ad oggetto un'interferenza nel diritto al rispetto della vita privata, lamentata dal ricorrente per essere stato sottoposto ad una "*surveillance* totale", consistente in una forma di pedinamento elettronico tramite GPS, installato a sua insaputa sulla sua propria autovettura. La Corte europea ha, in quell'occasione, condannato la Francia, poiché l'allora vigente art. 81 codice di rito riconosceva al giudice istruttore un generico potere di procedere a tutti gli atti di indagine che avesse ritenuto utili al fine della ricerca della verità, non conferendo all'indagato alcuno strumento di controllo. Da qui, la violazione dell'art. 8 CEDU.

[382] T. BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2019, p. 443 ss. In questo senso, v. Cass., sez. II, 4 aprile 2019, n. 23172.

[383] Corte e.d.u., sent. 2 settembre 2009, *Uzun c. Germania*.

[384] Corte e.d.u., sent. 8 febbraio 2018, *Ben Faiza c. Francia*.

L'impiego del pedinamento elettronico tramite GPS porta a galla, ancora una volta, il difficile contemperamento tra le ragioni investigative e la tutela della *privacy*. Per quanto sia lampante la maggiore incisività, in termini euristici, di un pedinamento di questo genere rispetto ad uno "tradizionale", manca, ad oggi, una disciplina legislativa che regolamenti in maniera puntuale lo strumento in questione, prevedendo, come pare suggerire la giurisprudenza di Strasburgo, un controllo più penetrante da parte dell'autorità giudiziaria. Vero è che la repentina evoluzione tecnologica rende arduo intercettare tempestivamente i rischi posti in essere dagli strumenti che essa stessa mette a disposizione, ma, a fronte della risposta assolutamente insufficiente offerta dalla giurisprudenza in termini di tutela della *privacy*, un intervento del legislatore sul tema pare quant'altri mai necessario e auspicabile nel più breve tempo possibile.

3.2. *Le perquisizioni online e l'acquisizione di dati conservati nel* cloud

Come si è avuto modo di osservare in occasione dell'esame del captatore informatico, il codice di rito, limitandosi a regolarne l'utilizzo ai soli fini della realizzazione di un'intercettazione tra presenti, trascura le innumerevoli potenzialità di questo insidioso strumento investigativo. Resta così scoperta la delicata materia delle c.d. perquisizioni *online*, condotte appunto attraverso l'invio, normalmente a mezzo *e-mail*, di un *trojan* capace di creare un particolare collegamento tra il *computer* sul quale viene installato e un altro dispositivo remoto, tale per cui l'utente di quest'ultimo è in grado di assumere il pieno controllo del primo sistema informatico. Si suole distinguere, nell'ambito delle perquisizioni *online*, tra attività di *online search* e attività di *online surveillance*: mentre le prime consentono di acquisire copia della generalità degli elementi salvati nella memoria del dispositivo "bersaglio", le seconde sono tese ad un controllo immediato e continuativo del flusso informativo del sistema digitale[385]. Con la locuzione "perquisizioni *online*" si allude, pertanto, a quell'«insieme di operazioni volte ad esplorare e monitorare un sistema informatico, rese possibili dall'infiltrazione segreta nello stesso, che consentono sia di

[385] V., sul punto, A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 2015, p. 2274 e nt. 3; S. MARCOLINI, *Le cosiddette perquisizioni* on-line *(o perquisizioni elettroniche)*, in *Cass. pen.*, 07/08, 2010, p. 2855 ss.

acquisire dati salvati sul *computer*, e quindi precostituiti, sia di captare flussi di dati in tempo reale»[386]. Proprio in ragione della loro vocazione poliedrica, le perquisizioni *online* rappresentano un istituto di natura ibrida, oltre che di difficile inquadramento giuridico, che pone notevoli problematiche di ordine processuale in punto di tutela dei diritti fondamentali.

Dal punto di vista della qualificazione giuridica, le perquisizioni *online* si pongono "a cavallo" tra le intercettazioni e le perquisizioni. Se, per un verso, l'istituto in discorso differisce dalle perquisizioni "tradizionali" per il fatto di essere finalizzato all'acquisizione occulta di elementi utili a fini investigativi in un contesto spaziale e temporale indefinito[387], per altro verso l'evoluzione tecnologica degli strumenti di osservazione occulta sembra aver messo in crisi la stessa nozione di intercettazione, così come intesa dalle Sezioni Unite "Torcasio"[388]: in particolare, si è detto che «a vacillare sono soprattutto i criteri basati sulla necessaria concomitanza tra attività captative segreta e interlocuzione tra i soggetti coinvolti nella comunicazione/conversazione, nonché lo stesso inquadramento di quest'ultima»[389].

Fin da queste sommarie considerazioni è facile persuadersi del fatto che le perquisizioni *online* postulano una più incisiva compressione delle garanzie individuali rispetto alle intercettazioni, in ragione dell'ingente mole di risultati probatori, più complessi e articolati, potenzialmente suscettibile di vanificare le esigenze difensive presidiate dallo stralcio e dall'archivio digitale[390]. Per questa ragione, difettando il diritto positivo, si impone la necessità, indossate le lenti del comparatista, di rivolgere l'attenzione al di fuori del panorama nazionale. Nell'esperienza tedesca, per rimanere in Europa, prima ancora di arrivare alla formulazione di una norma *ad hoc* sul tema, dottrina e giurisprudenza si erano interrogate circa il delicato rapporto tra *Online Durchsuchung* e diritti costituzionalmente garantiti, con specifico riferimento all'impiego dello strumento in questione. In Germania e,

[386] F. IOVENE, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont.*, n. 3-4/2014, 2014, p. 330.

[387] Le perquisizioni "tradizionali", infatti, pur essendo un atto "a sorpresa", sono conoscibili dall'indagato per mezzo della consegna del decreto motivato e del successivo deposito degli atti nella segreteria del pubblico ministero.

[388] V., sul punto, Cass., sez. un., 28 maggio 2003, Torcasio, che qualifica l'intercettazione di comunicazioni o conversazioni come una «captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti».

[389] L. PARLATO, *Le perquisizioni on-line: un tema che resta un tabù*, in G. GIOSTRA-R. ORLANDI (a cura di), *Revisioni normative in Tema di Intercettazioni: Riservatezza, Garanzie Difensive e Nuove Tecnologie Informatiche*, Torino, 2021, p. 344.

[390] Cfr. L. PARLATO, *Le perquisizioni on-line*, cit., p. 338.

segnatamente, nel *Land Nord Rhein Westfalen* veniva così autorizzato, attraverso una modifica della Legge sulla protezione della Costituzione del *Land*, un organismo di *intelligence* a "protezione della costituzione" (*Verfassungsschutzbehörde*) ad effettuare due distinte tipologie di indagine, quali il monitoraggio e la ricognizione segreta di *Internet* e l'accesso segreto a sistemi informatici (§ 5 Abs. 2, n. 11). Nel 2008 interviene la Corte costituzionale tedesca[391], che, nel dichiarare la normativa in questione incostituzionale per contrasto con i principi di proporzionalità e determinatezza, non si spinge ad escludere *tout court* l'ammissibilità dello strumento d'indagine in questione. È in questa occasione che la Corte, preso atto dell'inadeguatezza delle garanzie offerte dalle norme costituzionali a tutela della segretezza delle telecomunicazioni e dell'inviolabilità del domicilio, nonché del diritto all'autodeterminazione informativa[392], predispone una tutela ulteriore e sussidiaria rispetto a quella già vigente, riconoscendo l'esistenza del nuovo diritto fondamentale, e di rango costituzionale, "alla garanzia della segretezza e integrità dei sistemi informatici" (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). In altri termini, «di fronte alle sfide lanciate dal progresso tecnologico (*omissis*), la semplice, quanto doverosa, interpretazione evolutiva del dettato costituzionale non basta», in quanto «le tradizionali garanzie della segretezza delle telecomunicazioni e dell'autodeterminazione informativa non sono sufficienti»[393].

A livello comunitario, l'importanza di uno strumento d'indagine quale le perquisizioni *online* si è apprezzata sia ai fini della cooperazione giudiziaria sia con riguardo alle nuove competenze penali, attribuite all'Unione Europea dal Trattato di Lisbona, fra le quali rientra, ai sensi dell'art. 83 TFUE, la criminalità informatica. In primo luogo, vengono in rilievo le conclusioni del Consiglio del 27 novembre 2008 relative ad una strategia di lavoro concertata e a misure pratiche di lotta alla criminalità informatica[394], contenenti un invito agli Stati membri ad agevolare le perquisizioni a distanza, ove previste dalla legislazione nazionale, consentendo queste ultime ai servizi investigativi, con l'accordo del Paese ospite, di accedere

[391] *BVerfG*, 27 febbraio 2008, *BVerfGE* 120, 274 ss. Per un commento alla sentenza si veda R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d.* Online Durchsuchung. *La prospettiva delle investigazioni ad alto contenuto tecnologico e il bilanciamento con i diritti inviolabili della persona. Aspetti di diritto penale sostanziale*, in *Riv. trim. dir. pen. ec.*, 2009, p. 697 ss.

[392] *Informationelles Selbstbestimmungsrecht*, messo a punto nel 1983 con la nota sentenza sul censimento (*Volkszählungsurteil*). *BVerfG*, 15 dicembre 1983, *BVerfGE* 65, 1 ss.

[393] F. IOVENE, *Le c.d. perquisizioni* online, cit., p. 331.

[394] G.U.U.E. 17 marzo 2009, C 62/16.

rapidamente alle informazioni. Si segnala poi la direttiva sulla lotta alla pedopornografia[395], che, al *considerandum* 27, auspica la messa a disposizione dell'autorità inquirente, da parte degli Stati membri, di efficaci strumenti investigativi, fra i quali figurano «controlli a distanza anche con uso di strumenti elettronici di sorveglianza, (*omissis*) tenuto conto del principio di proporzionalità e del carattere e della gravità dei reati oggetto di indagine». È evidente come, tanto nel primo quanto nel secondo caso, il riferimento pare essere proprio all'istituto delle perquisizioni *online* (*remote computer searches*). In definitiva, «l'Unione Europea si sta muovendo nel senso di stimolare il rinnovamento e l'armonizzazione dei sistemi processuali nazionali per quanto riguarda gli strumenti di indagine»[396], essendo progressivamente emersa una sensibilità da parte degli ordinamenti nazionali tesa a riconoscere la peculiarità dei nuovi strumenti investigativi e delle criticità alle quali essi possono porre capo.

Posto che l'accesso "segreto" ad un sistema informatico sia suscettibile di ledere la sfera privata degli individui a più livelli, si possono individuare diversi profili di garanzia che vengono coinvolti da un'operazione del genere: dalla libertà e segretezza delle comunicazioni (art. 15 Cost.) all'inviolabilità del domicilio (art. 14 Cost.); dalla tutela della riservatezza (artt. 2 Cost., 8 CEDU, 7 CDFUE) alla tutela dei dati personali (artt. 8 CDFUE e 16 16 TFUE). Invero, configurandosi il sistema informatico come «un sistema complesso, contenente una moltitudine diversificata di dati» e non essendo ancora possibile, *rebus sic stantibus*, «un accesso selettivo al dispositivo tecnologico», pare superata, nel contesto odierno, «la distinzione tra dati intimi e dati sociali, tra informazioni segrete e informazioni riservate»[397]. Ciò induce a parlare di un superamento della distinzione tra segretezza e riservatezza, atteso che «la promiscuità dei dati e il tipo di intromissione da parte dell'autorità pubblica fanno (*omissis*) sì che il pericolo per il diritto della personalità in generale sia qualitativamente e quantitativamente diverso da quello di una semplice raccolta di dati, a cui fa da baluardo il diritto all'autodeterminazione informativa, quale filiazione del diritto alla *privacy*»[398]. La sfida odierna pare, dunque, essere quella di individuare, preso atto

[395] Direttiva 2011/92/UE, che sostituisce la DQ 2004/68/GAI, G.U.U.E. 17 dicembre 2011, L 351/1.

[396] F. IOVENE, *Le c.d. perquisizioni* online, cit., p. 333.

[397] Il rilievo è di F. IOVENE, *Le c.d. perquisizioni* online, cit., p. 334.

[398] *Ibidem*.

dell'esistenza di un nuovo bene giuridico, rappresentato dalla "riservatezza informatica"[399], il fondamento costituzionale di tale diritto, onde stabilire i presupposti per una sua legittima compressione da parte della pubblica autorità.

Quanto all'ordinamento italiano, in cui, come si è detto, manca una disciplina legislativa che regolamenti le perquisizioni *online*, si possono richiamare due casi affrontati dalla giurisprudenza di legittimità, che hanno visto l'impiego di tecniche di indagine in senso lato assimilabili alla *Online Durchsuchung*. Il filo rosso che unisce questi due casi è dato dall'utilizzo, in entrambe le ipotesi, di strumenti tipici con i quali, però, si andava a realizzare un monitoraggio continuativo – ed occulto nel primo caso – del sistema informatico oggetto dell'indagine.

Il primo caso[400] verte sull'utilizzo di un captatore informatico (*gotsh*) capace di acquisire, da remoto, copia dei *files* esistenti sul dispositivo "bersaglio" e di registrare in tempo reale quelli in corso di elaborazione. Secondo il ricorrente, alla fattispecie in esame si sarebbe dovuta applicare la disciplina delle intercettazioni informatiche; inoltre, ledendo l'attività posta in essere gli artt. 14 e 15 Cost., la prova sarebbe stata incostituzionale e i relativi risultati inutilizzabili ai sensi dell'art. 191 c.p.p. Nel respingere le eccezioni sollevate dal ricorrente, la Cassazione ha buon gioco nell'escludere la riconducibilità dell'attività captativa in esame all'alveo delle intercettazioni[401]: non trattandosi di comunicazione, non scatta infatti la tutela dell'art. 15 Cost. né può ritenersi integrata una violazione dell'art. 14 Cost., trovandosi il *computer* monitorato in un luogo aperto al pubblico e non all'interno di un luogo di privata dimora. A ben vedere, se sull'esclusione della garanzia di cui all'art. 15 Cost. non sembra potersi obiettare alcunché, qualche perplessità[402] desta invece l'esclusione, in maniera *tranchant*, dell'operatività dell'art. 14 Cost., estendendosi quest'ultima

[399] La riservatezza informatica è definita quale «interesse al godimento e controllo esclusivo sia di determinati dati e informazioni, che dei relativi mezzi e procedimenti informatici e telematici di trattamento, che pur configurandosi sempre quale "diritto di escludere" i terzi non legittimati dal corrispondente accesso e utilizzo, prescinde in tutto o in parte dai tradizionali limiti e presupposti dei concetti civilistici di proprietà o possesso, ovvero dalle condizioni che fondano la rilevanza giuridica del segreto o della riservatezza personale in genere». Così, L. PICOTTI, (voce) *Reati informatici*, in *Enc. giur. Treccani*, agg. VIII, Roma, 2000, p. 20 ss.

[400] Cass., sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass*., n. 246954. Cfr. S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ss.

[401] Il decreto del pubblico ministero non aveva ad oggetto un flusso di comunicazioni, bensì «una relazione operativa tra microprocessore e video del sistema elettronico, ossia un flusso unidirezionale di dati confinato all'interno dei circuiti del *personal computer*».

[402] V., sul punto, F. IOVENE, *Le c.d. perquisizioni* online, cit., p. 339.

disposizione anche al "domicilio informatico", il quale prescinde dal luogo di ubicazione del *device* o della persona. A riserve di ordine costituzionale si somma poi l'opinabile riconduzione dell'attività captativa in questione all'acquisizione della prova documentale: infatti, pur essendo l'art. 234 c.p.p. una norma a struttura aperta e idonea ricomprendere anche i documenti informatici[403], «bisogna fare attenzione a non confondere il contenuto con il contenitore: i dati digitali non sono prove documentali e non seguono le regole di ammissione per questi dettate dagli artt. 495, co. 3 e 515 c.p.p.»[404]

Di segno opposto è la soluzione offerta nel notorio "caso Ryanair"[405], avente ad oggetto la perquisizione, ai sensi dell'art. 247 c.p.p., e il successivo sequestro delle credenziali di accesso al sistema *online* di prenotazione dei voli della compagnia aerea. La vicenda offre il destro alla Suprema Corte per fissare un limite invalicabile alla disciplina delle perquisizioni *online*: nell'avallare la decisione di annullamento, emessa dal Tribunale del riesame, del decreto di perquisizione e sequestro del pubblico ministero, gli Ermellini sanciscono infatti un divieto di perquisizioni *ad explorandum*. Nel caso di specie, l'attività investigativa era volta alla preventiva identificazione dei c.d. ovulatori, cioè i corrieri internazionali di sostanze stupefacenti o psicotrope, che si realizzava attraverso un'inversione dialettica dell'ordine delle fasi del procedimento penale, in quanto il monitoraggio preventivo del sistema delle prenotazioni *online*, oltre a impattare su dati personali di soggetti estranei alle indagini, veniva effettuato in difetto di una *notitia criminis*, la cui iscrizione fa scattare il decorso dei termini per la durata delle indagini preliminari. Secondo la Corte, pertanto, «è da escludere un preventivo ed indefinito monitoraggio del sistema predetto in attesa dell'eventuale e futura comparsa del dato da acquisire a base delle indagini: si verrebbe altrimenti ad integrare un nuovo ed anomalo strumento di ricerca della prova, con finalità nettamente esplorative, di mera investigazione (paragonabile alle intercettazioni), che nulla ha a che fare con la perquisizione».

Al fine di riconoscere uno spazio di legittimità alle eterogenee forme di ricerca della prova in rete, si guarda solitamente alla controversa categoria della prova atipica. In realtà, «il fatto che le perquisizioni *online* non siano riconducibili ad alcuno dei mezzi di ricerca

[403] In tal senso, F. CORDERO, sub *art. 234*, in *Codice di procedura penale commentato*, II ed., Torino, 1992.

[404] F. IOVENE, *Le c.d. perquisizioni* online, cit., p. 339.

[405] Cass., sez. IV, 17 aprile 2012, n. 19618, in *Cass. pen*., 2013, p. 1523 ss.

della prova specificamente disciplinati dal codice di rito non significa che si possa automaticamente concludere nel senso della loro ammissibilità alle condizioni stabilite dall'art. 189 c.p.p.»[406]. Per questa ragione, si discute se si tratti di una prova atipica o, piuttosto, di una prova incostituzionale. Anche a voler trascurare l'orientamento secondo cui residua «il più radicale dubbio che il principio di legalità processuale sia violato dalla stessa ammissibilità di una prova atipica, il ricorso alla quale, comunque, sarebbe addirittura superfluo qualora si riconoscesse che le innovazioni tecnico-scientifiche sarebbero agevolmente inquadrabili in ipotesi già presenti nel testo originario del codice di procedura penale»[407], occorre ragionare sulla compatibilità di un meccanismo concepito per la fase dibattimentale rispetto a quella investigativa, laddove manchi fisiologicamente in seno ad esso la possibilità di un confronto dialettico sulle modalità di acquisizione probatoria. In effetti, «la tesi che ammette l'estensione di questo modello alla fase investigativa suggerisce un'interpretazione "adeguatrice", *rectius* analogica, dell'art. 189 c.p.p., fino a collocare il contraddittorio sulla prova (e non per la prova) in dibattimento, nella fase delle richieste di prova»[408]: in questo modo, «il contraddittorio (*omissis*) dovrebbe essere posticipato al momento in cui si chiede ingresso al risultato di una prova alla quale le parti non hanno avuto modo di assistere, direttamente o tramite i propri difensori o esperti»[409] e «si realizzerebbe in un momento nel quale l'eventuale lesione del diritto alla riservatezza (*omissis*) sia già avvenuta e non sia più in alcun modo rimediabile, a prescindere dalla futura utilizzabilità del dato»[410]. Certo è che questa soluzione pare porsi in maniera stridente con la salvaguardia dei diritti fondamentali di nuova emersione, con rilevanti conseguenze, fra l'altro, sul piano dell'utilizzabilità dei relativi risultati di prova.

Il tema del domicilio informatico viene in rilievo, a maggior ragione, con riguardo all'acquisizione dei dati conservati nel *cloud*. Per *cloud computing* s'intende l'insieme delle tecnologie che consentono di memorizzare, archiviare ed elaborare dati grazie all'utilizzo di risorse distribuite e accessibili in rete[411]. Com'era inevitabile, il suo successo, dipendente

[406] F. IOVENE, *Le c.d. perquisizioni* online, cit., p. 340.

[407] G. UBERTIS, *Sistema di procedura penale, I, Principi generali*, Milano, 2017, p. 117.

[408] E. MANCUSO, *Le perquisizioni* on-line, in *Jus – Rivista di Scienze Giuridiche*, 2017.

[409] *Ibidem.*

[410] *Ibidem*.

[411] V., in particolare, S. ATERNO – M. MATTIUCCI, Cloud Forensics *e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen*., 2013, p. 865.

dalla generale flessibilità del servizio offerto, ha destato l'attenzione anche delle organizzazioni criminali, che, nell'ottica di ostacolare l'identificazione degli autori e la ricostruzione delle attività illecite, hanno intuito ben presto le potenzialità insite nella delocalizzazione garantita dal *cloud computing*. Il problema è ora stabilire se, rispetto a questo tipo di operazioni investigative, nel concetto di luogo di privata dimora possa essere automaticamente fatto rientrare il domicilio informatico: infatti, mentre il dubbio non si pone con riguardo ad apparati di uso personale (come cellulari, *tablet* o *p.c.*), più controversa è la questione nel caso di dati e informazioni "depositati" con le forme del *cloud computing*. Qualora infatti l'autorità giudiziaria si trovi a dover verificare se e quali *file* siano detenuti da un soggetto in assenza di una disponibilità fisica dei supporti, si tratta di appurare quali strumenti giuridici possano essere utilizzati, specialmente nel caso in cui il *server* sul quale i *file* si trovino sia all'estero.

Sul punto, si segnala una pronuncia della Cassazione[412], che si è trovata a dover stabilire se il sequestro dei dati di un *server* allocato fisicamente nel territorio di uno Stato estero integri una violazione della sovranità di quest'ultimo. Ad avviso della S.C., che definisce l'attività di *cloud computing* come una «tecnologia che permette di elaborare, archiviare e memorizzare dati grazie all'utilizzo di risorse *hardware* e *software* distribuite nella rete», il decreto di sequestro ex artt. 254 ss. c.p.p., avente ad oggetto le *e-mail* di un *account* straniero, non richiede, a pena di inutilizzabilità, il ricorso alla rogatoria, così come prescrive la Convenzione di Budapest del 2001, dal momento che «la detenzione consiste nell'avere la disponibilità di una cosa, ossia nell'avere la possibilità di utilizzarla tutte le volte che si desideri pur nella consapevolezza che essa appartiene ad altri». Risultando i dati contenuti in uno spazio virtuale di memoria, ancorché generato da un *server* allocato all'estero, detenuti dal titolare delle credenziali di accesso, il quale ha il potere di disporre di tali dati attraverso una *password* – e non dalla società che gestisce il *server* –, è possibile, secondo la Corte, evitare la procedura di sequestro a mezzo della rogatoria. Questa tesi risulta condivisibile nella misura in cui si consideri che lo stesso titolare dei *file*, in quanto depositati su di un supporto che non si trova nella sua disponibilità fisica, ne può fruire solo attraverso tale flusso, mentre la polizia giudiziaria, nell'eseguire l'ispezione, non forza alcuna misura

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

di protezione, limitandosi piuttosto a richiamare sul *client* le informazioni utili ai fini delle indagini, al fine di farne una copia[413].

3.3. *L'utilizzo dei droni a fini di* law enforcement

Mentre l'impiego dei droni non pone di per sé particolari problemi in termini di tutela della *privacy*, i performanti strumenti tecnici di cui sono dotati rendono invece imprescindibile una riflessione sulla compatibilità di un impiego generalizzato dei velivoli a pilotaggio remoto con il rispetto delle libertà e dei diritti fondamentali degli individui[414]. La questione assume un particolare rilievo dal punto di vista della protezione dei dati personali, posto che il sorvolo di un drone, ove equipaggiato con videocamere o altri sensori di captazione di informazioni confidenziali, è idoneo a ledere il diritto alla riservatezza, financo ad avere una rilevanza penale, ai sensi dell'art. 615-bis c.p. (in materia di interferenza illecita nella vita privata), laddove i dati personali siano stati indebitamente captati nei luoghi di privata dimora. Il quadro si complica ulteriormente in presenza di sistemi aeromobili a pilotaggio remoto guidati da tecnologie di intelligenza artificiale[415]: da un lato, infatti, queste tecnologie sono in grado di assorbire un'enorme mole di dati grazie a sistemi di *big data analytics* sempre più raffinati[416]; dall'altro, l'utilizzo di algoritmi può porre capo a situazioni

[413] Cfr. S. ATERNO-M. MATTIUCCI, *Cloud Forensics e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen.* web, 2013.

[414] In materia, tra gli altri, si veda D. BOCCHESE, *Il diritto alla privacy nell'era dei droni*, in *El transporte como motor del desarrollo socioeconomico*, di M. V. PETIT LAVALL, A. PUETZ (a cura di), *Instituto Universitario de Derecho del Transporte* (IDT), 2018, p. 395 s.; A. DAVOLA, *L'acquisizione di dati da parte dei privati nelle operazioni con SAPR*, in E. PALMERINI-M. A. BIASIOTTI-G. F. AIELLO (a cura di), *Diritto dei droni. Regole, questioni e prassi*, Milano, 2018, p. 137 ss.; N. TRIGGIANI, *Le videoriprese investigative e l'uso dei droni*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2019, p. 161 ss.

[415] Cfr. C. TUCKER, Privacy, *Algorithms and Artificial Intelligence*, in *The Economics of Artificial Intelligence: An Agenda*, University of Chicago, 2019, p. 423 s. Si vedano sul tema anche le interessanti considerazioni espresse da N. FABIANO, *Gdpr e privacy, consapevolezza e opportunità*, Firenze, 2020, p. 244 ss.

[416] Per una panoramica sull'argomento dei *big data analytics* si vedano A. TETI, *Big Data. La guida completa per il Data Scientist*, Milano, 2017; A. DE MAURO, *Big Data Analytics: Analizzare e interpretare dati con il machine learning*, Apogeo Ed., 2019.

non prevedibili di ricombinazione dei dati acquisiti che vengono successivamente incorporati nel processo decisionale iniziale.

Il tema è stato oggetto di attenzione da parte del Gruppo di lavoro indipendente, rubricato "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali", istituito sulla base dell'art. 29 della dir. CE 95/46, in seguito sostituito dall'*European Data Protection Board* (Comitato europeo per la protezione dei dati) con l'entrata in vigore, nel 2018, del reg. UE n. 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione dei dati, nonché alla libera circolazione degli stessi. Il c.d. "Art. 29 *Working Party*" ha, quindi, enucleato una serie di raccomandazioni destinate ai legislatori nazionali «con finalità di tutela del diritto alla riservatezza delle persone in relazione all'impiego di SAPR (sistemi aeromobili a pilotaggio remoto) in qualunque ambito operativo, mettendo allo stesso tempo in evidenza la particolare invasività del trattamento dei dati derivante dall'uso di tali mezzi rispetto ai tradizionali strumenti di videosorveglianza che sono caratterizzati da immobilità»[417].

Nel parere "*Privacy and Data Protection Issues Relating to the Utilisation of Drones*", emanato il 16 giugno 2015, sono stati trasfusi i risultati dello studio. In questo documento, i garanti europei hanno preso coscienza delle potenzialità insite nelle caratteristiche tecnico-operative delle apparecchiature che spesso equipaggiano i velivoli a pilotaggio remoto, avvertendo la necessità di apprestare idonee cautele al diritto alla riservatezza e alla protezione dei dati personali. Già in questo parere si fa riferimento ai concetti di *privacy by design* e di *privacy by default*, tra loro complementari e recepiti poi nel *General Data Protection Regulation* (GDPR)[418]. Mentre il primo «implica l'obbligo di adottare, sin dalla fase di progettazione, specifiche misure che permettano di garantire *ab origine* e per l'intero ciclo di vita del sistema, il rispetto delle disposizioni in materia di *privacy*»[419], il secondo «impone (*omissis*) al titolare del trattamento di adottare "le misure tecniche ed organizzative adeguate, per garantire che siano trattati, per impostazione predefinita, solo i dati personali

[417] M. LAMON-M. BONAZZI, *I droni a supporto della pubblica sicurezza*, in *Giureta – Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente*, 2021, p. 187.

[418] Regolamento (UE) 2016/679.

[419] M. LAMON-M. BONAZZI, *I droni a supporto della pubblica sicurezza*, cit., p. 188. In particolare, l'art. 25, par. 1, del GDPR impone al soggetto titolare del trattamento dei dati (c.d. *data controller*) di adottare le misure tecniche ed organizzative adeguate, quali la "pseudonimizzazione" e la "minimizzazione", al fine di soddisfare i requisiti imposti dal regolamento per tutelare i diritti degli interessati.

necessari per ogni specifica finalità di trattamento in conformità al principio di minimizzazione dei dati"»[420]. In ossequio alle prescrizioni promananti dalle fonti convenzionali e sovranazionali e, segnatamente, ai principi in materia di tutela del diritto alla riservatezza e alla protezione dei dati personali (art. 8 CEDU e artt. 7 e 8 CDFUE), il Gruppo di Lavoro "Articolo 29" ha poi precisato che eventuali deroghe alla riservatezza dei dati personali debbono, in ogni caso, risultare conformi alla legge, necessarie e rispondenti a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. In conseguenza di ciò, in tanto le autorità dovrebbero poter disporre dei droni, in quanto sussista un'adeguata base giuridica e il loro utilizzo risulti proporzionato e necessario alle finalità perseguite.

Un'esigenza di contemperamento fra i diversi interessi in gioco si pone, *a fortiori*, con riguardo all'eventuale impiego di mezzi aerei a pilotaggio remoto da parte della polizia a fini di *law enforcement*, il cui utilizzo è regolamentato, per quanto in maniera non del tutto esaustiva, dal decreto del Ministro dell'Interno del 29 aprile 2016[421]. Per quanto non sia dato rinvenire all'interno di questo provvedimento alcuna indicazione in punto di rispetto e tutela dei dati personali, non pare comunque potersi prescindere, nei casi in cui le forze di polizia si avvalgano di droni per finalità investigative e di prevenzione dei reati, dal d.lgs. 22 dicembre 2018, n. 151, che ha recepito nel nostro ordinamento la direttiva UE n. 680/2016, dedicata alla tutela delle persone fisiche rispetto al trattamento dei dati personali effettuato da parte delle autorità competenti per scopi di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali.

Nel d.p.r. 29 settembre 2000, n. 367[422], si rinviene poi un riferimento normativo, per quanto generale, alla possibilità di effettuare rilevamenti e riprese aeree sul territorio nazionale, da parte di pubbliche autorità o enti privati, per l'espletamento dei rispettivi compiti istituzionali, senza necessità di preventivi atti di assenso e anche ove il trattamento non sia contemplato da una fonte primaria o di regolamento. La previsione in questione

[420] *Ibidem*. V., in tal senso, art. 25, par. 2, del GDPR.

[421] Si tratta del decreto recante le modalità di utilizzo da parte delle Forze di polizia degli aeromobili a pilotaggio automatico.

[422] D.p.r. 29 settembre 2000, n. 367, Regolamento recante norme per la semplificazione dei procedimenti relativi a rilevamenti e riprese aeree sul territorio nazionale e sulle acque territoriali.

sembra porsi in contrasto con il regolamento ENAC[423] sui mezzi aerei a pilotaggio remoto; tuttavia, da un confronto tra la normativa ENAC e quella europea, nell'allegato al reg. di esecuzione UE 2019/947 viene ribadito, con riferimento alle operazioni della categoria *specific*, l'obbligo dell'operatore UAS di «predisporre procedure volte a garantire che tutte le operazioni rispettino il regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati».

Da ultimo, vi è il profilo concernente l'applicazione della normativa elaborata dal Garante della protezione dei dati personali in materia di sorveglianza e, più in particolare, del provvedimento n. 1712680 dell'8 aprile 2010[424]. Il punto è se tale provvedimento, in attesa di una più puntuale normativa di settore sul tema, sia da tenersi in considerazione per i trattamenti di dati effettuati dalle Forze di polizia con finalità di controllo del territorio, tutela dell'ordine e della pubblica sicurezza. In proposito, il d.p.r. 15 gennaio 2018, n. 15, prevede, agli artt. 22, 23 e 24, particolari modalità del trattamento dei dati attraverso sistemi di videosorveglianza e di ripresa fotografica, audio e video, in ordine all'adempimento delle finalità istituzionali delle Forze di polizia. L'auspicio pare quindi quello di un'armonizzazione tra le normative di riferimento in materia di tutela dei dati personali e di impiego dei droni, nonché di una tempestiva definizione delle "linee guida", in relazione ai velivoli a pilotaggio remoto in uso alle Forze di polizia, da parte del dipartimento di pubblica sicurezza. Alla luce del tracciato quadro normativo, si può pacificamente concludere per la doverosità di un più elevato livello di uniformità della disciplina relativa alla tutela della *privacy* e dei dati personali acquisiti durante operazioni di *law enforcement* e implicanti l'esercizio dei mezzi aerei a pilotaggio remoto.

[423] Ai sensi dell'art. 29 del regolamento, rubricato "Protezione dei dati e *privacy*", «laddove le operazioni svolte attraverso *Unmanned Aircraft Systems* (UAS) possano comportare un trattamento di dati personali, tale circostanza deve essere menzionata nella documentazione sottoposta ai fini del rilascio della pertinente autorizzazione».

[424] Pubblicato in G.U. del 29 aprile 2010, n. 99.

3.4. *Le videoriprese*

Il termine "videoriprese" designa un'eterogenea pluralità di fattispecie. Occorre anzitutto distinguere tra videoriprese effettuate al di fuori di un procedimento penale e videoriprese effettuate dalla polizia giudiziaria al fine di investigare su di una *notitia criminis*. Mentre le prime costituiscono, ai sensi dell'art. 234 c.p.p., un "documento", cioè una prova rappresentativa di un fatto, le seconde possono essere "documentative", ai sensi dell'art. 141-bis c.p.p., ovvero "investigative", ai sensi dell'art. 189 c.p.p. È invero con riferimento a queste ultime che si registra, nel nostro ordinamento, una lacuna normativa, non essendo stato capace il legislatore di disciplinare questo penetrante strumento investigativo, suscettibile di incidere sui diritti fondamentali delle persone.

A fronte del vuoto normativo, la giurisprudenza ha progressivamente fissato alcuni punti fermi in materia, svolgendo, anche in questo caso, un ruolo di "supplente". Un primo importante approdo risale al 2002, quando la Corte costituzionale[425], tracciando uno spartiacque fondato sull'oggetto delle videoriprese, opera una distinzione tra comportamenti comunicativi e comportamenti non comunicativi[426]. Mentre nel secondo caso, venendo registrata soltanto l'immagine, non è possibile ricondurre l'attività di videoripresa ad uno specifico paradigma normativo, nel primo caso ci si trova innanzi ad un'intercettazione di comunicazioni, regolamentata dalla prima o dalla seconda parte del c. 2 dell'art. 266 c.p.p., a seconda che la videoripresa sia effettuata rispettivamente in luoghi pubblici o riservati ovvero nel domicilio[427]. È appena il caso di precisare che «l'atipicità delle videoriprese di comportamenti non comunicativi presenta (*omissis*) risvolti problematici in quelle ipotesi in cui, venendo in gioco il bene della inviolabilità del domicilio di cui all'art. 14 Cost., sia necessario ossequiare il corredo di garanzie lì compendiato nella riserva di legge e di

[425] C. cost., sent. 11 aprile 2002, n. 135, in *Giur. cost*., 2002, p. 2185.

[426] Critico, in ordine alla suddivisione tra comportamenti comunicativi e non comunicativi, è A. CAMON, *Captazione di immagini*, in *dir. proc. pen.*, 2013, p. 142, il quale osserva come tale impostazione «fornisc(a) uno scopo formalmente legittimo a manovre che, nella realtà, puntano a tutt'altro. Nemmeno i più ingenui potrebbero veramente pensare che, nella pratica, s'installino videocamere nelle abitazioni altrui sperando che per avventura uno dei soggetti sotto controllo sia muto e comunichi a gesti, o che sia così impaurito dall'eventualità d'essere ascoltato da scambiare biglietti con gli astanti. L'obiettivo di catturare una comunicazione è remoto, improbabile, meramente teorico; eppure un effetto lo produce: rende legittima la lesione dell'intimità domiciliare. Lo squilibrio fra mezzi (dirompenti) e fini (talmente lontani da non essere raggiunti mai) è però insopportabile», sottolineando altresì come anche la valutazione *ex post* in ordine ai contenuti comunicativi si basi su confini tutt'altro che lineari, cosicché «l'utilizzabilità della prova viene ancorata a parametri evanescenti».

[427] In altri termini, i "dialoghi" sono destinati a confluire nel fascicolo per il dibattimento *ex* art. 268, c. 7 c.p.p.

giurisdizione»[428]: in effetti, la stessa Consulta riconosce che «l'ipotesi della videoregistrazione che non abbia carattere di intercettazione di comunicazioni potrebbe perciò essere disciplinata soltanto dal legislatore, nel rispetto delle garanzie costituzionali dell'art. 14 Cost.».

Rimasto lettera morta il monito volto alla predisposizione di una specifica base normativa disciplinante il ricorso alle videoriprese in ambienti riconducili alla nozione di domicilio, le Sezioni Unite "Prisco" del 2006[429] sono tornate a confrontarsi con la materia, tentando una più completa sistematizzazione della stessa. Anzitutto, in ordine all'ammissibilità e utilizzabilità delle videoriprese investigative, la Corte nega che il difetto di una normativa *ad hoc* valga ad escludere *tout court* l'ammissibilità degli strumenti investigativi in questione, operando anche nella fase delle indagini preliminari il principio sancito all'art. 189 c.p.p.[430]. Ciò premesso, viene ad affrontare il "cuore" del problema, ovvero la regolamentazione delle videoriprese investigative in ambito domiciliare e, mediante «un argomento che si atteggia come generale *actio finium regundorum* dell'operatività del principio di atipicità rispetto a strumenti probatori che incidano su beni costituzionalmente tutelati»[431], osserva come «l'art. 189 c.p.p. (*omissis*) presuppone la formazione lecita della prova e soltanto in questo caso la rende ammissibile», cosicché «non può considerarsi "non disciplinata dalla legge" la prova basata su un'attività che la legge vieta, come nel caso delle riprese visive di comportamenti non comunicativi avvenuti in ambito domiciliare». In questo modo, la Sezioni Unite riconoscono nella riserva di legge costituzionalmente imposta, quale quella in tema di inviolabilità del domicilio *ex* art. 14 Cost., un ostacolo all'operare dell'art. 189 c.p.p. come base normativa per l'ammissione di una prova atipica. In altri termini, «la mancanza di una previsione di legge funge al contempo da presupposto operativo dell'art. 189 c.p.p. e da motivo di esclusione della legittimità di ogni attività incidente sul bene di cui all'art. 14 Cost.»[432]. Quanto alle videoriprese effettuate

[428] V. BONINI, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Proc. pen. giust.*, 2019, p. 339.

[429] Cass., sez. un., 28 marzo 2006, n. 26795, Prisco.

[430] In particolare, secondo la Cassazione, «il contraddittorio previsto dall'art. 189 c.p.p. non riguarda la ricerca della prova ma la sua assunzione e interviene, dunque, (*omissis*) quando il giudice è chiamato a decidere sull'ammissione della prova».

[431] V. BONINI, *Videoriprese investigative*, cit., p. 340.

[432] *Ibidem*.

in luoghi pubblici, in cui cioè non vi è alcuna aspettative di riservatezza, ovvero in luoghi riservati, come una *toilette* o un *privé* di un *night club*, si è in presenza, secondo le Sezioni Unite, di un mezzo di ricerca della prova atipico: se nel primo caso i risultati potranno essere acquisiti ai sensi dell'art. 189 c.p.p., nel secondo caso, trattandosi di un atto che viene ad incidere sulla riservatezza, si renderà necessaria un'autorizzazione con provvedimento motivato dell'autorità giudiziaria.

Una precisazione si impone con riguardo alla particolare ipotesi delle violenze sessuali. La Cassazione[433] ha infatti statuito che le riprese audiovisive, disposte previa autorizzazione del giudice, delle effusioni e dei rapporti sessuali tra l'indagato e la vittima di violenza sessuale, intrattenuti all'interno di un domicilio privato, sono utilizzabili, in quanto questi vanno considerati alla stregua di comportamenti comunicativi, ancorché di tipo non verbale, espressivi di interazione e idonei a trasmettere contenuti del pensiero o stati d'animo.

A questo punto, l'attenzione si sposta sulla nozione di "domicilio" di cui all'art. 14 Cost., che diviene così decisiva al fine di delimitare le videoriprese ammissibili. Sul punto le stesse Sezioni Unite del 2006 riconoscono che «non vi sono nella giurisprudenza e nella dottrina indicazioni univoche e si dubita pure che ci sia coincidenza tra l'ambito della garanzia costituzionale e quello della tutela penale» e «che la giurisprudenza tende ad ampliare il concetto di domicilio in funzione della tutela penale degli artt. 614 e 615-bis c.p., mentre tende a circoscriverlo quando l'ambito domiciliare rappresenta un limite allo svolgimento delle indagini». Ad onta di ciò, esse precisano che «il concetto di domicilio non può essere esteso fino a farlo coincidere con un qualunque ambiente che tende a garantire intimità e riservatezza», dovendo l'intensità del rapporto tra titolare del diritto e luogo domiciliare «essere tale da giustificare la tutela di questo anche quando la persona è assente». Per quanto concerne invece i luoghi "riservati", che, come si è detto, restano esclusi dalla nozione di domicilio, la Corte di Cassazione nega comunque che possano essere esposti ad ogni genere di intrusioni: più in particolare, facendo discendere il "diritto alla riservatezza" dagli artt. 2 Cost. e 8 CEDU, aggiunge alla tradizionale bipartizione tra luoghi domiciliari e luoghi aperti al pubblico una sorta di *tertium genus*, cui dovrà riconoscersi «una forma di tutela intermedia»[434].

[433] V. Cass., sez. III, 22 luglio 2020, n. 31515.

[434] *Ibidem*.

Un'importante puntualizzazione sul concetto di domicilio, in relazione allo strumento delle videoriprese, è stata offerta nel 2008 dalla Corte costituzionale[435], la quale ha escluso la tutela del domicilio e dei luoghi riservati nel caso in cui gli stessi non siano in concreto protetti da barriere visive idonee ad impedire la generalizzata visione di quanto ivi avviene. Ad avviso del Giudice delle leggi, infatti, non è sufficiente a far scattare la protezione dell'art. 14 Cost. la circostanza che un certo comportamento venga tenuto in luoghi di privata, dovendo piuttosto avvenire in condizioni tali da renderlo tendenzialmente non visibile a terzi. Sarà quindi equiparabile al luogo pubblico o aperto al pubblico quello che, difettando qualsiasi ostacolo visivo, renda possibile l'*inspectio* rispetto a quanto avviene al suo interno.

L'ultimo atto di questo percorso che ha interessato le videoriprese è rappresentato da una pronuncia della Cassazione del 2021[436], che si è trovata a dover rispondere all'interrogativo se lo spazio antistante l'opificio, riparato da barriere, possa essere considerato come domicilio. Nella ricostruzione prospettata dai ricorrenti, i luoghi oggetto di osservazione e captazione dovevano essere ricondotti alla nozione di privata dimora, con tutte le conseguenze del caso in punto utilizzabilità delle risultanze probatorie. Ad avviso della S.C., invece, la registrazione esterna di immagini, eseguita mediante l'installazione di videocamere sull'edificio antistante, è assimilabile ad un'operazione di appostamento della polizia giudiziaria svolta nell'ambito dell'autonomia investigativa, non potendo ogni luogo di lavoro qualificarsi come privata dimora o domicilio. A sostegno della sua tesi, la Corte, nel proporre una definizione privata dimora, pone l'accento su quei locali che assolvono attualmente e concretamente la funzione di proteggere la vita privata di coloro che li posseggono e rispetto ai quali questi ultimi sono titolari di un vero e proprio *ius excludendi alios*.

Non si può negare che le regole elaborate dalla giurisprudenza abbiano il merito di avere colmato il vuoto normativo in materia di videoriprese, ma è altrettanto evidente come il risultato sia quello di una disciplina su base casistica, a tratti farraginosa, che si regge su costruzioni teoriche caratterizzate da spiccato astrattismo e crea non poche incertezze sul piano applicativo[437]. In particolare, resta affidato all'interprete il delicato compito di

[435] C. cost., 7 maggio 2008, n. 149, in *Giur. cost*., 2008, p. 1832.

[436] Cass., sez. III, 8 ottobre 2021, n. 43609.

[437] In questo senso, A. SCALFATI-O. BRUNO, *Orientamenti in tema di videoriprese*, in *Proc. pen. giust*., 2011, 1, p. 92.

distinguere tra comportamenti comunicativi e comportamenti non comunicativi, cosicché l'utilizzabilità della prova risulta, di fatto, collegata a parametri evanescenti[438]. Non meno arduo è, come si è visto, qualificare correttamente determinati ambienti, ancora una volta con ricadute sul regime giuridico applicabile. In proposito, apre certamente uno scenario interessante la previsione di un *tertium genus*, che si aggiunge alla tradizionale bipartizione tra privata dimora e luogo pubblico, segnando un deciso passo in avanti nella direzione della tutela del diritto alla *privacy*. In questo senso, viene ad essere valorizzata quella giurisprudenza della Corte e.d.u., che da tempo ha adottato una nozione ampia di "vita privata", ricomprendente il diritto all'identità e allo sviluppo della persona, nonché il diritto di quest'ultima di stabilire e sviluppare relazioni con altri esseri umani e con il mondo esterno[439]. Si determina così l'esistenza, anche in un contesto pubblico, di una zona di interazione dell'individuo con gli altri suscettibile di essere ricondotta all'alveo dell'art. 8 CEDU, *sub specie* al diritto a una "vita sociale privata"[440]. In definitiva, la *privacy*, lungi dal restare confinata all'ambito prettamente domiciliare, finisce per ampliarsi al suo esterno, creando nuovi spazi meritevoli di tutela.

Ulteriore questione è quella delle videoriprese nell'ambito delle investigazioni difensive[441]. Il codice di rito tace al riguardo, limitandosi a disciplinare l'istituto dell'«accesso ai luoghi» agli artt. 391-sexies c.p.p. e 391-septies c.p.p. Mentre il difensore ed il suo ausiliario non incontrano ostacoli in ordine all'accesso ai luoghi pubblici o aperti al pubblico, l'accesso ai luoghi privati o non aperti al pubblico è subordinato al consenso di chi ne abbia la disponibilità, in difetto del quale si renderà necessaria l'autorizzazione del giudice, che fissa con decreto motivato le concrete modalità dell'accesso stesso. Alla luce di

---

[438] Secondo, A. CAMON, *Captazione di immagini*, in *dir. proc. pen.*, 2013, p. 144, la linea che divide i comportamenti "nudi" da quelli che trasportano messaggi è labile: «un gesto, una smorfia, parole pronunciate ad alta voce fra sé e sé, sovrappensiero, discorsi indirizzati ad un animale domestico, costituiscono una comunicazione? E i messaggi espressi in un codice convenzionale? Difficile dirlo».

[439] Molteplici sono le decisioni della Corte di Strasburgo che si esprimono nel senso di riconoscere la c.d. "vita sociale privata" dell'individuo. L'art. 8 CEDU, infatti, protegge anche il diritto all'autodeterminazione e allo sviluppo personale e il diritto di instaurare e sviluppare rapporti con gli altri individui e con il mondo estero e può includere altresì attività di natura professionale o commerciale. v. Corte e.d.u., GC, 5 settembre 2017, Bărbulescu c. Romania, § 71; Corte e.d.u., GC, 7 febbraio 2012, Von Hannover c. Germania, § 95; Corte e.d.u., 2 settembre 2010, Uzun c. Germania, § 43; Corte e.d.u., 17 luglio 2003, Perry c. Regno Unito, § 36; Corte e.d.u., 28 gennaio 2003, Peck c. Regno Unito, § 62.

[440] *Ibidem*.

[441] V., sul tema, N. TRIGGIANI, *Le videoriprese investigative e l'uso dei droni*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2019, p. 188 ss.

ciò, se può pacificamente escludersi la legittimità di videoregistrazioni clandestinamente realizzate dal difensore in occasione dell'accesso a luoghi privati o non aperti al pubblico[442], lo stesso non può dirsi con riguardo a quelle effettuate in luoghi pubblici, aperti o esposti al pubblico, che trovano nell'art. 327-bis c.p.p. il loro referente normativo.

3.5. *Il riconoscimento facciale e l'impiego del* SARI

Si parla di riconoscimento facciale con riferimento a quei *tool* che consentono, tramite un algoritmo basato sull'intelligenza artificiale, di associare alla foto o al video di un volto di uno sconosciuto una o più immagini, contenute in una banca dati di dimensioni variabili, di soggetti le cui generalità sono già note[443]. Questo tipo di operazioni può avvenire secondo due distinte modalità: si distingue, infatti, il riconoscimento facciale *real-time* da quello che si realizza su immagini o video già agli atti. La procedura di riconoscimento facciale si sviluppa in due fasi, delle quali la prima consiste nella raccolta dell'immagine e nella trasformazione della stessa in un *template* biometrico, mentre la seconda coincide con il riconoscimento dell'individuo grazie al confronto tra il *template* iniziale dello stesso con un o più *template* differenti. La procedura mediante la quale si accerta che una persona è realmente chi dice di essere prende il nome di "autenticazione" e si basa appunto, come nel caso della modalità di accesso ad alcune *app* in uso sugli *smartphone*, sul confronto tra il viso di quella persona e un *template* preesistente in un *database*. È invece definito "identificazione" il processo di riconoscimento del singolo soggetto rispetto ad un gruppo indistinto di individui, come avviene, ad esempio, nel contesto di una manifestazione pubblica. Tali strumenti ci consentono di cogliere come i nostri corpi siano divenuti «una "miniera a cielo aperto" dalla quale attingere dati ininterrottamente»[444], essendo ormai

[442] In tal senso, v., fra gli altri, A. CAMON, voce *Captazione di immagini (dir. proc. pen.)*, in *Enc. dir.*, Annali, vol. VI, Milano, 2013, p. 141; F. CAPRIOLI, *Riprese visive nel domicilio e intercettazione "per immagini"*, in *Giur. cost.*, 2002, p. 2187, nt. 63, il quale richiama il «generale principio che le attività di investigazione difensiva non possono incidere su diritti inviolabili».

[443] V., in proposito, J. DELLA TORRE, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, in G. DI PAOLO-L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale*, cit., p. 7 ss.

[444] S. RODOTÀ, *Trasformazioni del corpo*, in *Politica dir*., 2006, p. 6.

«oggetto di un processo di de-composizione ove ogni aspetto viene raccolto, conservato e consegnato ad una macchina»[445].

Negli Stati Uniti si discute dell'utilizzo del riconoscimento facciale all'interno del processo penale già dalla fine degli anni Novanta. Il vero *boom*, tuttavia, si è avuto nel 2020, a seguito del noto "scandalo *Clearview*", quando è emerso che la polizia americana si serviva di una *app* di riconoscimento facciale che operava su un *database* contenente miliardi di dati rubati da *social network* come *Facebook*, *Twitter* o *Instagram*. La vicenda *Clearview* offre certamente un saggio emblematico dei più rilevanti nodi critici posti dall'evoluzione tecnologica connessa alla raccolta e all'elaborazione dei dati, all'estrazione di conoscenze predittive e all'adozione di decisioni correlate. In particolare, traccia una vera e propria mappatura dei profili di criticità che compongono una delle maggiori sfide che il diritto si trova ad affrontare nel campo dei *Big Data*, offrendo l'occasione per evidenziare la "valenza euristica" del diritto alla protezione dei dati personali, in rapporto alla complessità delle sfide di ordine etico, sociale, politico e giuridico che lo sviluppo delle tecnologie pone. Le immagini conservate nel *database* della società statunitense risultano essere state elaborate mediante tecniche biometriche al fine di estrarre le caratteristiche identificative di ognuna di esse[446]: tali immagini sono poi arricchite con meta-dati associati – come il titolo dell'immagine o della pagina *web*, il *link* della fonte, la geolocalizzazione, il genere, la data di nascita, la nazionalità, la lingua –, in modo tale che, quando il *software* identifica una corrispondenza, estrae dal *database* tutte le relative immagini, presentandole al cliente del servizio come risultato della ricerca unitamente ai meta-dati e permettendo così di risalire ad ogni singola pagina sorgente. Di fronte alle censure avanzate dai reclamanti, che hanno denunciato un trattamento dei loro dati personali in assenza del consenso, la strategia difensiva di *Clearview* è stata nel senso che il servizio offerto dalla società risulterebbe, in fin dei conti, equivalente a quello offerto da *Google Search* e, in ogni caso, funzionale ad agevolare l'attività delle Forze di polizia in ordine alla repressione dei reati.

Il problema di fondo connesso al performante strumento di intelligenza artificiale in discorso è dato dal pesante impatto che esercita sui diritti fondamentali: accanto, naturalmente, al diritto alla *privacy*, tutelato all'art. 8 CEDU e agli artt. 7 e 8 della Carta di

[445] Cfr. F. PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *Media Laws – Rivista di diritto dei Media*, 2021, n. 1, p. 208.

[446] Per una più completa panoramica sulle modalità di funzionamento dell'algoritmo, cfr. il sito *web* della società all'indirizzo https://www.clearview.ai.

Nizza, risulterebbe infatti pregiudicati, fra gli altri, il diritto di riunione e associazione, il diritto di sciopero, nonché il diritto di manifestazione del pensiero. Di conseguenza, il sistema *de quo* sembra porsi in maniera stridente con il complesso di tutele dei dati personali previsto dall'UE allo scopo di arginare la tendenza ad una concezione "recessiva" del diritto alla *privacy*. Per altro verso, lo stesso strumento risulta assai più invasivo della normale videoripresa e necessita, per questo, un trattamento più rigoroso. In effetti, i connotati fisici o facciali di un individuo lo identificano in modo estremamente personale, incrementando in maniera esponenziale i rischi legati ad un utilizzo improprio, quando non del tutto illecito, della tecnologia in discorso. A questo proposito, viene in rilievo l'art. 52 della Carta di Nizza, in forza del quale eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali debbono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà, mentre limitazioni possono essere apportate, pur nel rispetto del principio di proporzionalità, solo laddove necessarie e rispondenti effettivamente a finalità di interesse generale riconosciute dall'UE o all'esigenza di proteggere i diritti e le libertà altrui.

Una disciplina più puntuale è possibile rinvenire nella Direttiva europea 2016/680[447] relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle Autorità competenti, a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. La Direttiva prevede che ogni trattamento di dati personali da parte delle Forze dell'ordine debba essere esplicitamente regolato dalla normativa nazionale, la quale deve altresì precisare le finalità di tale trattamento e le categorie di dati personali che ne fanno oggetto. In particolare, l'art. 10 prevede che il trattamento di categorie particolari di dati personali – inclusi i dati biometrici – sia unicamente consentito qualora strettamente necessario alla realizzazione degli obiettivi identificati e che debba essere soggetto a garanzie appropriate per tutelare i diritti e le libertà dell'interessato. Qualora autorizzata dalla legislazione nazionale di uno Stato Membro, tale tipologia di trattamento può essere solamente realizzata in due casi: qualora sia necessaria alla protezione degli interessi vitali dell'interessato o di un'altra persona oppure qualora il trattamento sia relativo a dati che sono resi manifestamente pubblici dallo stesso interessato. Gli Stati membri, d'altra parte, in tanto saranno legittimati a legiferare su tali materie, in quanto abbiano preventivamente consultato le relative Autorità nazionali di controllo per la protezione dei dati personali. Da non trascurare è, quindi, l'art. 6 della Direttiva, che impone

[447] Dir. (UE) 2016/680.

agli Stati membri di prevedere che il titolare del trattamento operi una differenziazione in ordine alle categorie dei soggetti interessati dall'utilizzo delle tecnologie di riconoscimento facciale. Ai sensi di tale disposizione, è necessario, ove possibile, operare una chiara distinzione tra:

a) «le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato»;
b) «le persone condannate per un reato»;
c) «le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato»;
d) «altre parti rispetto a un reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati o le persone in contatto o collegate alle persone di cui alle lettere a) e b)».

A rendere i contorni della questione ancora più delicati è la generale carenza di giurisprudenza in materia. A questo proposito, si segnala un'importante pronuncia della *High Court of Justice* dell'Inghilterra e Galles intervenuta nel 2019. Si tratta del caso *Bridges c. Regno Unito*[448], avente ad oggetto le doglianze di un cittadino gallese che lamentava di essere stato ripreso dalla forma *real-time* di un *tool* mentre camminava per le strade di Cardiff. La sentenza costituisce la prima decisione giudiziale a livello globale ad aver affrontato, in modo analitico, il tema della compatibilità con il diritto alla riservatezza dell'utilizzo da parte delle Forze di polizia di un *software* di riconoscimento facciale[449]. Secondo i giudici d'oltremanica, pur avendo il *software* di *facial recognition* determinato un'ingerenza nella vita privata del ricorrente, questa sarebbe da considerarsi del tutto legittima, in quanto consentita dall'art. 8, par. 2 della CEDU, ai sensi del quale, in tanto le autorità pubbliche possono compiere un'intrusione della *privacy* di un singolo, in quanto il comportamento che viene in rilievo sia previsto «dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al

[448] *High Court of Justice, Queen's Bench Division, Divisional Court*, 4 settembre 2019, *Case* No: CO/4085/2018, R (Bridges) v. CCSWP e SSHD.

[449] Per una più puntuale disamina del caso, cfr. J. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *Sistema Penale*, 2020.

benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui». Alla luce di questa previsione, non hanno pregio le ragioni avanzate dal ricorrente, secondo il quale la mancanza di una disciplina legislativa *ad hoc* in tema di riconoscimento facciale integrerebbe *sic et simpliciter* una violazione della riserva di legge *ex* art. 8, par. 2 CEDU: infatti, ad avviso dei giudicanti, «l'attività di raccolta e di conservazione di dati biometrici facciali tramite algoritmi (deve) essere fatta rientrare tra i poteri generali che il *common law* attribuisce alle forze di polizia per prevenire e contrastare la criminalità»[450] e gli strumenti di *facial recognition* «rientrano comunque nell'ambito di applicazione delle previsioni comuni (interne ed eurounitarie) di tutela della *privacy*, a cui vanno aggiunte una serie di disposizioni di rango regolamentare in tema di video sorveglianza e di *local policies*, adottate dalla *South Wales Police*»[451]. In questo modo, «il combinato disposto tra il *common law*, la *primary legislation* (generale) in materia di *privacy* e una serie di norme di rango non legislativo andrebbe a costituire quel "*clear and sufficient legal framework governing whether, when and how AFR Locate may be used*", idoneo a soddisfare lo *standard* di cui all'art. 8, par. 2, CEDU»[452].

In Italia esiste dal 2017 un sistema di riconoscimento facciale, in dotazione alla polizia giudiziaria, denominato SARI (Sistema Automatico di Riconoscimento Immagini). Si tratta di un sistema di intelligenza artificiale che opera attraverso algoritmi di riconoscimento delle sembianze facciali, comparando l'immagine captata con tutte quelle presenti nella banca dati del sistema, al fine di rinvenire quella corrispondente o più affine al soggetto ricercato. Il SARI opera in due modalità, *Entreprise* o *Real-Time*. Mentre la prima[453] «rappresenta la forma di automazione di un sistema di riconoscimento da sempre esistente, che non genera

[450] J. DELLA TORRE, *Novità dal Regno Unito*, cit., p. 237.

[451] *Ibidem*.

[452] *Ibidem*.

[453] Con l'identificazione attraverso SARI *Enterprise*, l'operatore inserisce in una banca dati di circa dieci milioni di elementi l'immagine di un soggetto, al fine di individuarne l'identità: il sistema si sostituisce all'operatore nella ricerca all'interno delle banche dati, comparando l'immagine del soggetto da ricercare con le altre presenti nell'archivio, in cerca di una possibile corrispondenza. Al termine della ricerca, il sistema propone un elenco di foto segnaletiche somiglianti al soggetto da identificare, tra cui l'operatore dovrà individuare quella più affine al ricercato. L'uso di tale modalità operativa velocizza le operazioni di riconoscimento, limitando l'apporto degli investigatori che non devono più inserire manualmente dati anagrafici o altri dati identificativi del soggetto agevolando l'attività d'indagine, così come accaduto nel caso di specie.

particolari lesioni dei diritti individuali, e, in quanto tale, è stato ritenuto utilizzabile dall'Autorità garante della protezione dei dati personali»[454], la seconda[455] «lungi dall'essere una semplice videoripresa, (*omissis*) crea problemi di invasività nella sfera della *privacy* del singolo, ben più rilevanti di quelli connessi ai semplici impianti preposti alla sorveglianza»[456].

Il difetto di un riferimento normativo, unitamente alla necessità di un inquadramento giuridico dello strumento *de quo*, induce a ricondurlo all'alveo delle pre-investigazioni – quali «atti e attività realizzate quando la *notitia criminis* non si è manifestata in alcuni o tutti i suoi contorni costitutivi»[457]– nei casi in cui la ricerca effettuata attraverso il SARI sia precedente alla formazione definitiva della notizia di reato, ovvero a quello delle indagini atipiche[458] laddove tale sistema automatico venga utilizzato per l'individuazione personale, dopo l'iscrizione della notizia di reato, in sostituzione dei "tradizionali" sistemi identificativi previsti dal codice di rito. I dati biometrici rilevati attraverso il SARI[459], idonei a identificare in modo univoco un soggetto, sono dati personali, così come indicati all'art. 4, lett. b) del Codice della *privacy*[460], che li qualifica come «qualunque informazione relativa ad una persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale». In particolare, una definizione di dati biometrici si rinviene all'allegato A del provvedimento del Garante della *privacy* 12/11/2014, che li definisce come dati ricavati da «proprietà

[454] L. SAPONARO, *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Arch. pen.*, 2022, n. 1, p. 6.

[455] Si tratta di un sistema di riconoscimento mobile, che può essere installato ovunque e fungere da sistema di videosorveglianza, in quanto prevede la possibilità di registrare le riprese mediante telecamere installate in una determinata area geografica. La procedura consente di analizzare in tempo reale i volti ripresi, in particolare alcuni dati biometrici degli stessi, di confrontarli con altri presenti in una banca dati predefinita (la c.d. *watch list*) e, qualora attra-verso un algoritmo di riconoscimento venga rilevata una corrispondenza tra il volto ripreso e quello presente nella *watch list*, generare un *alert* che consente agli operatori di intervenire. Diversamente, la procedura di identificazione genera una candidate list, cioè una lista di soggetti simili a quello da individuare dove, come nel caso precedente, sarà compito dell'operatore trovare il volto più affine al ricercato sulla base di vari parametri. In entrambe le ipotesi sarà un "uomo" e non il sistema ad effettuare l'individuazione, circostanza che, teoricamente, dovrebbe rappresentare una garanzia di tutela dei diritti individuali dei singoli.

[456] L. SAPONARO, *Le nuove frontiere tecnologiche*, cit., p. 7-8.

[457] A. SCALFATI, *Il fermento pre-investigativo*, in ID. (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, p. 1.

[458] In tema v., per tutti, A: SCALFATI (a cura di), *Le indagini atipiche*, II ed., Torino, 2019.

[459] Cfr. T. ALESCI, *Il corpo umano fonte di prova*, Milano, 2017, p. 89.

[460] D.lgs. 196/2003, modificato dal d.lgs.101/2018.

biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili, laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili»[461]. S'intuisce facilmente che, in ragione della loro particolare sensibilità, i dati biometrici, come consentono una rapida identificazione del soggetto, allo stesso tempo danno luogo ad una significativa lesione del diritto alla *privacy*.

In attuazione della ricordata Direttiva 2016/680, l'art. 7 del d.lgs. 51/2018, nel disporre l'assoluta necessità di una disciplina normativa, stabilisce che il trattamento dei dati biometrici possa essere autorizzato «solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea e da legge o, nei casi previsti dalla legge da regolamento», e, comunque, «necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato». Inoltre, l'art. 23 dello stesso decreto prevede che «se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali». In virtù di quest'ultima disposizione, il Ministero dell'Interno ha redatto e sottoposto al Garante della protezione dei dati personali, nella sua veste di autorità di controllo, un documento di valutazione relativo ai rischi per i diritti e la libertà delle persone fisiche derivanti dall'impiego del sistema di riconoscimento facciale. Nel pronunciarsi sulla questione, il Garante si è espresso negativamente[462] in ordine alla richiesta del Ministero concernente l'installazione del SARI *Real time* in spazi pubblici, ponendo l'accento sull'intrusività del sistema di captazione dei dati rispetto al «diritto alla vita privata e alla dignità delle persone, unitamente al rischio di ripercussioni negative su altri diritti umani e sulle libertà fondamentali», consentendo tale sistema di individuare tutti i soggetti presenti in un determinato luogo. Secondo l'Autorità di controllo, peraltro, «i riferimenti codicistici richiamati dal Ministero, a sostegno della legittimità del SARI, risultano troppo labili per

[461] A titolo esemplificativo, possono annoverarsi, tra i dati biometrici, la scansione della retina, l'immagine dell'iride, le caratteristiche vocali, le impronte digitali, il colore della pelle ovvero le caratteristiche comportamentali di un individuo come il modo di muovere le mani o di camminare.

[462] Provvedimento n. 127 del 25 marzo 2021.

consentire il sistema di riconoscimento biometrico facciale, né può effettuarsi un'applicazione analogica della disciplina utilizzata in tema di videoriprese»[463].

In definitiva, la mancanza di una disciplina espressa dedicata al SARI pone capo ad un irriducibile contrasto con la Carta di Nizza e con la CEDU, nonché con la Direttiva 2016/680. Inoltre, il difetto di dati che informino sull'utilizzo pratico del *tool* e su eventuali *bias* cognitivi sembra porsi in maniera stridente anche con la Carta etica del Consiglio d'Europa in tema di intelligenza artificiale[464]. Il rischio di una "sorveglianza di massa", segnalato dal Garante, può essere arginato solo con un'adeguata disciplina normativa, che impedisca un uso indiscriminato del sistema di captazione di immagini in discorso. In effetti, «legittimare il Sistema di riconoscimento facciale in tempo reale, senza alcun vincolo legislativo, ribalterebbe completamente il delicato rapporto tra individuo e autorità»[465], atteso che, mentre «nella videosorveglianza "comune" l'obiettivo è quello di controllare un luogo ed eventualmente, in un momento successivo, qualora si verifichino dei reati, cercare di individuare il colpevole», «nella sorveglianza "di massa" l'obiettivo non è più controllare un luogo, ma controllare le persone presenti in quel luogo, con l'effetto che i dati dei soggetti presenti potranno essere analizzati e utilizzati per valutazioni diverse»[466].

3.6. *Il cacciatore di* IMSI

Dopo aver colonizzato gli Stati Uniti, i c.d. *IMSI catchers*[467] sono da qualche anno sbarcati in Europa, occupando l'attenzione anche del nostro ordinamento[468]. Apparecchi portatili delle dimensioni di una valigetta, questi strumenti sfruttano alcune vulnerabilità delle reti di comunicazione, fingendo di essere un ponte radio, per indurre i cellulari nei

[463] L. SAPONARO, *Le nuove frontiere tecnologiche*, cit., p. 14.

[464] Ci si riferisce alla *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment* del dicembre 2018, promanante dall'*European Commission for the efficiency of justice* (CEPEJ).

[465] L. SAPONARO, *Le nuove frontiere tecnologiche*, cit., p. 17.

[466] *Ibidem*.

[467] Anche detti *cell-site simulators* o *Stingray* (dal nome del modello più famoso).

[468] Cfr., per una più completa disamina di questa nuova tecnologia, A. CAMON, *Il cacciatore di IMSI*, in *Arch. pen.*, 2020, n. 1, p. 177 ss.

dintorni ad agganciarsi e carpirne così i codici identificativi. La captazione dei codici costituisce, in realtà, solo l'antecedente di tutta una serie di operazioni ulteriori, che spaziano dalla realizzazione di un "pedinamento elettronico" fino all'inoculazione di un *trojan horse*. I modelli in commercio sono, per lo più, dotati anche di ulteriori funzioni aggiuntive: in particolare, «possono (*omissis*) interrompere il servizio, impedendo la connessione alla rete; registrare il contenuto delle comunicazioni inviate e ricevute; fare chiamate o mandare messaggini per conto del telefono "in ostaggio"; cambiare il contenuto dei messaggi inviati; esplorare e registrare quanto è archiviato nel dispositivo sotto controllo»[469].

Sebbene negli USA le agenzie di *law enforcement* utilizzino gli *IMSI catchers* da più di un ventennio, sporadici sono i casi in cui i giudici se ne sono occupati. Di qualche rilievo è, tuttavia, la presa di posizione del *Department of Justice*[470], che, sollecitato da stampa, associazioni di tutela delle libertà civili e giuristi, supera, dopo qualche perplessità iniziale, il suo orientamento "*liberal*" e, facendo applicazione analogica della disciplina del *Pen/Trap statute*, raccomanda ai *prosecutors* di munirsi preventivamente di un'autorizzazione giurisdizionale. Senonché, pur a seguito della modifica apportata nel 2001 al *Patriot Act*, resta assai agevole munirsi di un *pen-trap order*, essendo sufficiente dimostrare che le informazioni cercate sono pertinenti ad un'indagine in corso[471]. Questa è la situazione sino al 2018, quando la Corte Suprema[472], pur senza prendere una posizione espressa sugli *IMSI catchers*, statuisce che, per ottenere dalle compagnie telefoniche le registrazioni delle "celle" agganciate nel corso del tempo da un telefono, occorre un mandato fondato su una *probable cause*, salvo che il pedinamento sia di breve durata, come accade tipicamente con l'impiego dello *Stingray*. Lungi dal risolvere definitivamente tutte le questioni, la soluzione offerta nel caso *Carpenter* pone piuttosto in risalto le ambasce procurate dalle sempre più penetranti forme di controllo tecnologico. Accanto ai dubbi inerenti all'esigenza o meno di un mandato, questione di non poco conto è poi quella attinente all'estensione del controllo affidato al giudice, attese le peculiarità delle indagini condotte con lo strumento dello *Stingray*. In

[469] A. CAMON, *Il cacciatore di IMSI*, cit., p. 179-180.

[470] ELECTRONIC SURVEILLANCE UNIT, *Electronic Surveillance Manual: Procedures and Case Law Forms*, U.S. DEPT OF JUSTICE 40 (2005), reperibile anche online (https://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf), 46.

[471] Uno *standard* talmente basso che la funzione del giudice chiamato a rilasciare l'autorizzazione viene considerata «*ministerial in nature*».

[472] *Carpenter v. United States*, 585 U.S. (2018).

effetti, gli *IMSI catchers* sono in grado di registrare le informazioni provenienti dalla generalità dei telefoni che si trovano entro una determinata area, circostanza che ripropone, anzitutto in termini qualitativi, i rischi connessi al passaggio da una sorveglianza mirata ad una più ampia e indistinta[473].

Venendo allo scenario sul versante europeo, si registra come l'Italia faccia eccezione rispetto alla gran parte degli altri Paesi, in seno ai quali la discussione sull'impiego degli *IMSI catchers* a fini investigativi è sfociata in una vera e propria disciplina legislativa[474]. Ad onta di ciò, le Forze di polizia italiane si servono da anni dei c.d. cacciatori di IMSI, ma, quando la Cassazione, ormai qualche anno fa, si è confrontata con questo mezzo d'indagine[475], ha dovuto fare i conti con la mancanza di una solida riflessione scientifica in materia. Il caso prende le mosse da un procedimento contro un'associazione per delinquere finalizzata al traffico internazionale di stupefacenti: perlustrata la zona con lo *Stingray*, la polizia giudiziaria riesce a recuperare il codice IMEI del telefono di uno degli indagati e lo trasmette al pubblico ministero, che è così in grado di chiedere ed ottenere l'autorizzazione per l'intercettazione. Secondo la difesa, l'ordinanza cautelare disposta sulla base degli esiti dell'intercettazione sarebbe illegittima, in quanto, per mettere in campo lo *Stingray*, occorrerebbe l'autorizzazione di un magistrato. Tre sono i nuclei concettuali attorno ai quali gravitano le argomentazioni della S.C., la quale, dopo essersi domandata se lo strumento *de quo* possa essere accostato ad altri istituti tipici, respinge il ricorso:

1) in primo luogo, l'operazione risulta di per sé inidonea a svelare il contenuto delle comunicazioni e non può, pertanto, essere equiparata ad un'intercettazione;
2) in secondo luogo, non raccoglie informazioni sui contatti e telefonici, circostanza che preclude alla possibilità di un accostamento all'acquisizione dei tabulati;
3) in terzo luogo, non si pone in contrasto con alcuna delle disposizioni facenti parte della c.d. costituzione integrata.

[473] Lo scenario si fa anche più inquietante se si considera che lo *Stingray* è stato adoperato per controllare i partecipanti a manifestazioni politiche, con conseguente rischio di una schedatura su basi ideologiche.

[474] Tanto per fare degli esempi, il codice di procedura penale francese si occupa degli *IMSI catchers* nell'art. 706-95-20, modificato nel 2019; l'StPO tedesco, nell'art. 100i, introdotto nel 2002 e novellato nel 2017; in Austria una prima regolamentazione, per quanto blanda e collocata fuori dal codice, è intervenuta nel 2005, per poi essere ripensata nel 2018, quando le relative norme sono confluite all'interno del codice (§ § 132, 134 e 137 StPO).

[475] Cass., sez. IV, 12 giugno 2018, n. 41385, in *Mass. Uff.*, n. 273929-01.

Secondo gli Ermellini, quindi, l'operazione in questione non può che essere ricondotta agli atti investigativi atipici, suscettibili di essere compiuti dalla polizia giudiziaria di propria iniziativa. Che una simile conclusioni lasci alquanto insoddisfatti è forse superfluo rilevarlo, se non altro nella misura in cui la Corte dimostra di non avere alcuna consapevolezza dell'opportunità di una regolamentazione in via legislativa di questo strumento investigativo. I giudici, infatti, sembrano non comprendere fino in fondo le potenzialità insite nel cacciatore di IMSI, in quanto, se è forse eccessivo affermare che questo ponga in essere «una sorta di controllo online per cui ogni attività del soggetto monitorato viene captata»[476], certo è che alcuni suoi esemplari dispongono di capacità intrusive assai sofisticate, al punto da registrare il contenuto delle comunicazioni. Peraltro, questa tesi trova conforto nelle parole della Corte costituzionale, che, in una pronuncia del 1973[477], ha chiarito che il rispetto dell'art. 15 Cost. esige «garanzie che attengono alla predisposizione anche materiale dei servizi tecnici necessari per le intercettazioni (*omissis*), in modo che l'autorità giudiziaria possa esercitare anche di fatto il controllo necessario ad assicurare che si proceda alle intercettazioni autorizzate, solo a queste e solo nei limiti dell'autorizzazione». Senonché, mentre il legislatore si è mostrato ricettivo rispetto ai moniti della Corte, affidando ad un decreto ministeriale il compito di fissare i requisiti che debbono presentare i *softwares* al fine di essere impiegati per le intercettazioni mediante captatore[478], nulla di analogo è stato fatto, invece, per gli *IMSI catchers*, che restano, ad oggi, "scoperti" da un punto di vista legislativo e continuano a porre, in ragione dei loro connotati, interrogativi rispetto ai quali un intervento della dottrina risulta quant'altri mai auspicabile.

4. *L'agente segreto attrezzato per il suono*

Figura da non confondere con l'intercettazione, l'agente segreto attrezzato per il suono è il soggetto privato che, «su incarico dell'autorità inquirente e provvisto degli opportuni strumenti tecnici, avvicina le persone sospettate di un reato per provocarne e surrettiziamente

[476] W. NOCERINO, *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, Milano, 2018, p. 154.

[477] Corte cost., n. 34 del 1973.

[478] V., in particolare, l'art. 2, c. 3 d.l. 30 dicembre 2019, n. 161.

registrarne le dichiarazioni compromettenti»[479]. Sul punto, la Corte costituzionale[480] ha chiarito che la registrazione *de qua* costituisce "documentazione di un atto di indagine" – e non "prova documentale" –, tracciando, inoltre, una distinzione tra le due ipotesi differenti dell'ascolto contestuale della conversazione da parte della polizia giudiziaria e della mera registrazione della stessa. Quanto al primo caso, si tratta, secondo la giurisprudenza[481], di un'attività analoga all'intercettazione: pertanto, laddove la polizia giudiziaria abbia operato in assenza dei presupposti richiesti dalla disciplina desumibile dagli artt. 266 ss. c.p.p. e, segnatamente, difetti l'autorizzazione, l'atto è inutilizzabile, essendo state surrettiziamente aggirate le regole previste per le intercettazioni. Nell'ipotesi in cui, invece, il privato si limiti a registrare la conversazione e successivamente metta a disposizione della polizia quanto "fonicamente memorizzato" ai fini di un ascolto differito, la Cassazione[482] parla di un'attività di indagine atipica, che implica un'incidenza inferiore sulla segretezza della comunicazione, tutelata all'art. 15 Cost.: sussistendo infatti il consenso di uno dei partecipanti alla conversazione, sarà sufficiente, ai fini della legittimità delle operazioni, un decreto motivato del pubblico ministero[483].

Qualche considerazione ulteriore in merito alla necessità di un provvedimento autorizzativo da parte dell'autorità giudiziaria, per il ricorso alla figura dell'agente segreto attrezzato per il suono, s'impone. Esiste infatti un orientamento[484] secondo il quale l'essenziale incompatibilità tra la nozione di intercettazione e la partecipazione allo scambio comunicativo di colui che lo registra o lo trasmette a distanza porterebbe ad escludere che l'attività in esame richieda un'autorizzazione giudiziale ai sensi degli artt. 266 ss. del codice

[479] Così M. SCAPARONE, *In tema di indagini di polizia giudiziaria condotte per mezzo di un agente segreto "attrezzato per il suono"*, in *Giur. cost.*, 1988, II, p. 247.

[480] Corte cost., sent. 30 novembre 2009, n. 320.

[481] Cass., sez. VI, 6 novembre 2008, Napolitano, in *CED* 241610.

[482] Cass., sez. II, 14 ottobre 2010 – 4 gennaio 2011, n. 7, Biffis, in *Foro it.*, 2011, II, 224; Cass., sez. VI, 7 aprile – 21 giugno 2010, Angelini, in *CED* 247384 e in *Giur. it.*, 2011, 1, 183. Si tratta di una giurisprudenza prevalente; citiamo per tutte Cass., sez. IV, 18 ottobre 2017, B., in *CED* n. 271059.

[483] Si veda C. CONTI, *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. pen.*, 2011, p. 3638.

[484] Cass., sez. IV, 9 luglio 1996, n. 8237, Cannella, in *C.E.D. Cass*., n. 205799; Cass., sez. IV, 11 giugno 1998, n. 8759, Cabrini, *ivi*, n. 211465; Cass., sez. I, 14 aprile 1999, n. 6302, Iacovone, in *Giur. it.* 2001, 807; Cass., sez. V, 10 giugno 2002, n. 30078, Arena, inedita; Cass., sez. IV, 4 ottobre 2007, n. 40332, Picillo, in *C.E.D. Cass*., n. 237789; Cass., sez. VI, 24 febbraio 2009, n. 16986, Abis, *ivi*, n. 243256; Cass., sez. VI, 1° dicembre 2009, n. 49511, Ticchiati, *ivi*, n. 245774.

di rito. In questa prospettiva, si è talvolta considerata irrilevante pure la circostanza che, mercé l'invio di segnali radio o telefonici, la polizia giudiziaria sia messa in grado di effettuare un ascolto contestuale ed occulto dello scambio comunicativo[485], ovvero la stessa appartenenza alla polizia giudiziaria del soggetto che partecipa al colloquio, salvo il limite di utilizzabilità della documentazione prodotta con il concorso dell'inquirente derivante dalle norme in tema di prova dichiarativa nel dibattimento[486].

Secondo altro orientamento, invece, la sostanziale assimilazione tra la registrazione occulta "su intervento" della polizia giudiziaria e l'intercettazione telefonica o ambientale di uno scambio comunicativo esigerebbe sempre un previo provvedimento autorizzativo del giudice; ciò *a fortiori* nel caso in cui gli investigatori abbiano "provocato" il colloquio[487]. Come s'intuisce, il contrasto sorge dal peso che viene di volta in volta attribuito ad un profilo piuttosto che ad un altro: mentre nel primo caso appare decisiva la collaborazione del partecipe al colloquio, nel secondo caso si pone l'accento sull'"impronta genetica" che all'operazione viene impressa dall'iniziativa della polizia giudiziaria.

Vi è poi un terzo orientamento, sostenuto da chi si sofferma sulla tecnica di collocazione della ricetrasmittente. La teletrasmissione del suono – e, quindi, la possibilità di un ascolto contestuale e clandestino di persone non presenti alla conversazione – esigerebbe infatti un'autorizzazione dell'indagine da parte del giudice, ai sensi degli artt. 266 ss. c.p.p. Altro sarebbe, invece, la mera registrazione del colloquio, ancorché la stessa sia attuata su sollecitazione o con il sostegno tecnico della polizia giudiziaria: in questo caso, infatti, non occorrerebbe alcuna autorizzazione del giudice[488].

[485] Cass., sez. II, 5 novembre 2002, n. 42486, Modelfino, in *Arch. nuova proc. pen*. 2005, 80; Cass., sez. I, 19 febbraio 2009, n. 14829, Foglia, in *C.E.D. Cass*., n. 243741.

[486] Cass., sez. II, 24 gennaio 2006, n. 2829, Pistorio, in *Dir. pen. proc*. 2006, 457, con nota di F. PERONI, *Documentazione irrituale e utilizzabilità del dato nel giudizio abbreviato*.

[487] Cfr. ass., sez. II, 5 luglio 1988, Belfiore, in *Giur. it*. 1990, II, 6, con nota di G. DEAN, *In tema di indebita registrazione delle conversazioni tra persone detenute: dall'art. 225-quinquies c.p.p. 1930 all'art. 266 c.p.p. 1988*.

[488] Cass., sez. I, 13 gennaio 1999, n. 3458, Di Cuonzo, *ivi*, n. 213251; Cass., sez. I, 23 gennaio 2002, n. 30082, Aquino, in *Giust. pen.* 2003, III, 644; Cass., sez. I, 21 febbraio 2003, n. 8738, Lentini, inedita; Cass., sez. I, 7 novembre 2007, n. 46274, Ditto, in *C.E.D. Cass*. n. 238488.

Agli orientamenti sin qui esposti se ne aggiunge un quarto – e più recente – che ha fatto capolino in un'ordinanza del Tribunale di Milano[489]. Secondo i giudici meneghini, «l'effettuazione di registrazioni attraverso apparecchi forniti o predisposti dalla polizia giudiziaria, e collocati su persona destinata a partecipare a colloqui di interesse investigativo, deve essere autorizzata quanto meno mediante un provvedimento del pubblico ministero»[490], risultando inutilizzabili, in caso contrario, le registrazioni effettuate. La logica dalla quale muove questa pronuncia, che istituisce una «"speciale riservatezza" opponibile solo alla polizia giudiziaria»[491], non è quindi quella «di una protezione dei "contenuti" della privatezza, opponibili a chiunque, ma si orienta piuttosto alla specifica garanzia contro la forza pervasiva del potere pubblico, a titolo di bilanciamento tra le esigenze di accertamento dei reati e quelle di tutela dei diritti fondamentali degli individui»[492].

Qualunque di questi orientamenti si voglia seguire, resta il fatto che, come ha più volte ribadito la Corte di Strasburgo[493], «la registrazione di una conversazione (telefonica o tra presenti), per quanto operata da uno degli interlocutori, costituisce interferenza con la vita privata, qualora sia eseguita con strumenti procurati dall'autorità pubblica e nel contesto di un'indagine ufficiale»[494]. Di conseguenza, il compimento di attività del genere di quelle in esame, in assenza di una normativa puntuale, determina una violazione dell'art. 8 CEDU. È appena il caso di precisare che il riferimento della Corte non è tanto ad una legge in senso formale, quanto piuttosto ad una normativa «accessibile, comprensibile e sufficientemente dettagliata»[495], cosicché «la "estrazione" dall'art. 2 della Costituzione del precetto di un "livello minimo di tutela" per il diritto alla riservatezza, quando lo stesso è aggredito dall'autorità pubblica per fini di indagine, diviene il portato di una ricostruzione

[489] Trib. di Milano, ord. 13 marzo 2012, Est. Barazzetta. Si veda, in proposto, G. LEO, *Necessario il provvedimento autorizzativo dell'Autorità giudiziaria per il ricorso al c.d. «agente segreto attrezzato per il suono»*, in *Dir. pen. cont. 1/2012*, 2012, p. 163 ss.

[490] G. LEO, *Necessario il provvedimento autorizzativo dell'Autorità giudiziaria*, cit., p. 163.

[491] *Ibidem*, p. 166.

[492] *Ibidem*.

[493] Corte e.d.u., sent. 25 ottobre 2007, *Van Vondel c. Paesi Bassi*; sent. 1 marzo 2007, *Heglas c. Repubblica Ceca*; sent. 8 aprile 2003, *M.M. c. Paesi Bassi*.

[494] G. LEO, *Necessario il provvedimento autorizzativo dell'Autorità giudiziaria*, cit., p. 167.

[495] *Ibidem*.

convenzionalmente orientata del quadro normativo, tale da assicurarne congruenza con il precetto contenuto nell'art. 8 della Convenzione europea»[496].

4. *I tabulati telefonici*

Il c.d. tabulato non è che un prospetto contenente i dati esterni (data e ora, utenze, gestori, durata, posizione degli apparecchi nel caso in cui si tratti di utenze mobili) del flusso di chiamate riferibile a una o più utenze. Dal punto di vista dell'inquadramento costituzionale, la Consulta[497] ha da tempo ricondotto l'acquisizione dei dati esterni su traffico telefonico o telematico alla tutela dell'art. 15 Cost., affermando, nondimeno, che «la particolare disciplina predisposta dagli artt. 266-271 c.p.p. sulle intercettazioni di conversazioni o di comunicazioni telefoniche si applica soltanto a quelle tecniche che consentono di apprendere, nel momento stesso in cui viene espresso, il contenuto di una conversazione o di una comunicazione, contenuto che, per le modalità con le quali si svolge, sarebbe altrimenti inaccessibile a quanti non siano parti della comunicazione medesima».

Diversamente dagli altri mezzi atipici di ricerca della prova sino a qui considerati, il vuoto legislativo concernente l'acquisizione dei tabulati del traffico telefonico è stato colmato dall'art. 132 del codice *privacy*[498], oggetto di modifiche da parte di successive disposizioni di legge. Ai sensi del c. 1 di questa disposizione, «i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione». Entro lo stesso termine «i dati sono acquisiti presso il fornitore con decreto motivato del giudice su istanza del pubblico ministero o del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private». Il c. 1-bis prevede, invece, che «i dati relativi

[496] *Ibidem*.

[497] Corte cost., sent. n. 81 del 1993.

[498] D.lgs. n. 196 del 2003.

alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni». Come si vede, la norma prevede che siano conservati dal fornitore per periodi di tempo diversi i dati di tre tipi di traffico telefonico, cioè le chiamate senza risposta, i dati del traffico telematico ed i rimanenti dati del traffico telefonico in senso stretto. Se quelli illustrati sono i termini ordinari per i reati "comuni", l'art. 24 della l. n. 167 del 2017 ha esteso il periodo a settantadue mesi per i dati relativi al traffico telefonico, telematico e alle chiamate senza risposta, necessari ai fini dell'accertamento dei reati di cui agli artt. 51, c. 3-quater e 407, c. 2, lett. a) c.p.p. (terrorismo, mafia, omicidio volontario, sequestro di persona a fini di estorsione, armi, stupefacenti, tratta di persone, ecc.).

Resta un problema di fondo, rappresentato dal fatto che l'utilizzo dei tabulati telefonici non è circoscritto al perseguimento dei reati più gravi. In proposito, è intervenuta la Corte di Giustizia dell'UE[499], che, con le due pronunce *Digital Rights* e *Tele 2 Sverige*, ha dichiarato l'illegittimità della c.d. direttiva Frattini[500], sulla cui base è stata adottata la disciplina appena illustrata. Secondo la Corte, i dati in questione, presi nel loro complesso, consentono di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati. Di conseguenza, l'incidenza che la direttiva 2006/24 comporta nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta si rivela essere di vasta portata e particolarmente grave. Dall'altro lato, pur mirando a contribuire alla lotta contro la criminalità grave, la direttiva da ultimo richiamata non limita la conservazione dei dati a quelli relativi ad un determinato periodo di tempo e/o ad un'area geograficamente determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave né alle persone la conservazione dei cui dati, per altri

[499] Si allude a Corte di giustizia UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland, Seitlinger* (su domande di pronuncia pregiudiziale proposte dalla *High Court* irlandese e dalla *Verfassungsgerichtshof* austriaca); Corte di giustizia UE, sent. 21 dicembre 2016, *Tele2 e Watson*, cause riunite C-203/15 e C-698/15 (su domande di pronuncia pregiudiziale proposte dal *Kammarràtten* svedese e dalla *Court of Appeal* britannica).

[500] La quale, prevendendo misure di conservazione dei dati applicabili in via indifferenziata e generalizzata «all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta contro i reati gravi», si poneva in maniera stridente con il principio di proporzionalità.

motivi, potrebbe contribuire alla prevenzione, all'accertamento o al perseguimento di reati gravi. Da tutto ciò deriva che la direttiva 2006/24 non prevede norme chiare e precise, che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta: in ragione di ciò, la stessa comporta un'invasione nella sfera dei suddetti diritti fondamentali di ampia portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario. Ad onta di ciò, la Cassazione ha considerato la disciplina sui tabulati telefonici legittima e rispettosa del canone della proporzionalità per come accolto dalla Corte di Giustizia[501], in quanto «la norma interna enuncia la finalità della conservazione dei dati (repressione dei reati); delimita temporalmente l'attività di conservazione; prevede un intervento preventivo dell'"autorità giudiziaria" funzionale all'effettivo controllo della stretta necessità dell'accesso ai dati ed al rispetto del principio di proporzionalità in concreto»[502].

Qualche tempo dopo, la Corte di Giustizia è nuovamente intervenuta in tema di tabulati telefonici e telematici. Il riferimento è alla sentenza della Grande Camera del 20 marzo 2021, *H.K.*, C-746/18, che, rispondendo ad un rinvio pregiudiziale sollevato dalla Corte suprema estone, ha puntualizzato la sua giurisprudenza in materia di *data retention*. In particolare, i giudici europei hanno statuito in questa pronuncia che il diritto UE e, segnatamente, l'art. 15 della Direttiva 2002/58/UE, letto alla luce degli artt. 7, 8, 11 e 52 della Carta di Nizza, osta ad una disciplina nazionale che non circoscriva ai soli procedimenti, diretti a contrastare le forme gravi di criminalità ovvero a prevenire gravi minacce alla sicurezza pubblica, l'accesso da parte di pubbliche autorità a dati idonei a fornire informazioni su comunicazioni effettuate da un utente; parimenti, non è compatibile con il diritto UE una normativa che non affidi ad un soggetto terzo come un giudice, ma al pubblico ministero, la competenza ad autorizzare l'accesso a tali dati.

Al *dictum* della Corte di Giustizia ha quindi dato attuazione un recentissimo provvedimento del g.i.p. di Roma[503], il quale, «dopo aver rilevato la piena operatività anche

[501] In questo senso, Cass., sez. V, 24 aprile 2018, M., in *CED* 273892 e Cass., sez. III, 23 agosto 2019, n. 36380.

[502] P. TONINI, *Manuale di procedura penale*, cit., p. 422.

[503] G.i.p. Roma, decreto 25 aprile 2021, giud. Sabatini. Cfr., sul punto, J. DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in *Sistema Penale*, 2021.

nei confronti dell'Italia dei principi di diritto stabiliti dalla Corte di giustizia nell'ambito del rinvio pregiudiziale estone, ha (*omissis*) sconfessato la giurisprudenza tradizionale della Cassazione, rilevando la sussistenza di un "sopravvenuto contrasto tra l'art. 132 comma 3 del d.lgs. 196/2003 e la normativa dell'Unione Europa, così interpretata dal Giudice europeo»[504]. In effetti, al decreto in esame fa da sfondo quel filone giurisprudenziale, che, come si è detto, tendeva ad escludere, malgrado non fossero mancate le critiche sollevate dalla miglior dottrina[505], che il codice della *privacy* presentasse profili di frizione con il diritto comunitario. Nel dare applicazione al principio del primato del diritto comunitario, il giudice nostrano ha quindi sostenuto la necessità di una disapplicazione della previsione interna, senza necessità di attendere un intervento ablativo del legislatore nazionale: l'applicazione diretta della norma UE in luogo di quella italiana non sarebbe, peraltro, ostacolata dal fatto che la Corte di Giustizia non abbia indicato nella propria giurisprudenza un catalogo di reati specifico, in forza del quale la pubblica autorità sarebbe legittimata ad acquisire i dati in questione. In breve, ad avviso del giudicante, la sentenza *H.K.* imporrebbe non solo che l'apprensione dei dati sia autorizzata da un organo terzo, ma anche che gli stessi possano essere raccolti solo se si procede per fattispecie criminose suscettibili di intercettazione in senso proprio ai sensi degli artt. 266 e 266-bis c.p.p. Per quanto innegabile sia la natura creativa di questa pronuncia, «siffatta significativa svolta esegetica presenta il pregio di essere non solo garantista, ma anche pragmatica: suggerendo di applicare in modo sostanzialmente analogico la disciplina delle intercettazioni ai tabulati, il g.i.p. di Roma ha individuato un modo per evitare che l'autorità giudiziaria italiana non possa più avvalersi di uno strumento di importanza chiave nell'accertamento dei reati (se non al prezzo di rischiare di continuare a ledere i diritti fondamentali dell'individuo), nelle more di un (quantomai auspicabile) intervento normativo del legislatore nella materia *de qua*»[506].

L'arresto della Corte di Giustizia nel caso estone ha acceso, come conferma la pronuncia da ultimo ricordata del g.i.p. di Roma, un vivo dibattito in seno al nostro ordinamento sul tema dei tabulati telefonici; più in particolare, si sono profilate due questioni, strettamente interconnesse fra loro.

---

[504] J. DELLA TORRE, *L'acquisizione dei tabulati telefonici*, cit.

[505] Si veda, su tutti, L. LUPARIA, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio,* in *Dir. di internet*, 2019, p. 757.

[506] J. DELLA TORRE, *L'acquisizione dei tabulati telefonici*, cit.

In primo luogo, ci si è chiesti se i princìpi enucleati nella sentenza *H.K.* siano direttamente applicabili nell'ordinamento nostrano. Sul punto, si è delineato un contrasto giurisprudenziale. Secondo alcuni[507], infatti, «l'assenza di parametri e criteri idonei a delimitare con sufficiente precisione i casi nei quali deve ritenersi consentita l'apprensione dei dati esterni alle comunicazioni sarebbe di ostacolo ad un'efficacia immediata della pronuncia europea»[508]. Per contro, ad avviso di altri[509], «la genericità delle espressioni fatte proprie dalla Corte di Lussemburgo non avrebbe alcuna rilevanza ai fini della determinazione degli effetti della sentenza comunitaria, posto che l'espressione "forme gravi di criminalità", enucleata dai giudici sovranazionali, potrebbe essere agevolmente concretizzata attraverso il richiamo integrale alle ipotesi di cui all'art. 266 c.p.p.»[510].

In secondo luogo, è sorto l'interrogativo circa la rilevanza della pronuncia *de qua* alla luce del ruolo ricoperto dal pubblico ministero, rispettivamente, nell'ordinamento estone ed in quello italiano. Anche in questo caso, la giurisprudenza si è divisa fra quei giudici[511] che hanno negato la possibilità di una assimilazione tra le due autorità inquirenti e quelli[512] che, all'opposto, valorizzando il richiamo della Corte di Lussemburgo al canone della terzietà e neutralità del titolare del potere autorizzatorio, si sono espressi positivamente.

Il dibattito è culminato in un intervento da parte del legislatore, che ha riformato l'art. 132 del codice *privacy*. Nella prospettiva di adeguare la possibilità di acquisire i dati esterni alle comunicazioni al rispetto dei principi sanciti dalla sentenza comunitaria del 2021, il Governo ha infatti adottato il d.l. 30 settembre 2021, n. 132. Quanto all'ambito di applicazione oggettiva, si assiste ad una tipizzazione dei c.d. reati presupposto, legittimanti l'accesso alle informazioni di traffico, sulla base di un criterio al tempo stesso quantitativo

[507] Cfr. Trib. Milano, 22 aprile 2021; G.i.p. Tivoli, 10 giugno 2021; G.i.p. Roma, giudice Savio; G.i.p. Roma, 28 aprile 2021, nonché Cass. pen., 2 settembre 2021, n. 33116, in www.giurisprudenzapenale.com, 8 settembre 2021; Cass. pen., 15 aprile 2021, n. 28523, in www.ilpenalista.it, 5 agosto 2021, *Tabulati telefonici: la Suprema Corte si esprime dopo le indicazioni della CGUE*.

[508] A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, in *Sistema Penale*, 2021.

[509] Cfr. G.i.p. Roma, 25 aprile 2021; G.i.p. Bari, 1° maggio 2021.

[510] A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici*, cit.

[511] Trib. Milano, 22 aprile 2021; G.i.p. Tivoli, 10 giugno 2021; Trib. Rieti, 4 maggio 2021.

[512] Cfr. G.i.p. Roma, 25 aprile 2021; G.i.p. Roma, giudice Savio; G.i.p. Bari, 1 maggio 2021.

e qualitativo[513]. In ordine ai requisiti per l'acquisizione del c.d. traffico dati, vengono cristallizzati i due presupposti dei «sufficienti indizi di reato» e della «rilevanza ai fini della prosecuzione delle indagini». Con riferimento alla fase dinamica della disciplina, l'organo titolare del potere autorizzatorio viene identificato nella figura del giudice, in quanto soggetto indipendente, terzo e imparziale, così rimanendo disattesa l'interpretazione di quegli autori che avevano negato l'assimilazione tra i due organi inquirenti dell'ordinamento estone e di quello italiano. Una novità significativa è altresì quella concernente i "legittimati attivi" a richiedere l'apprensione dei tabulati telefonici, che vengono ad essere, oltre naturalmente al pubblico ministero, anche il difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private[514]. Simmetricamente a quanto previsto all'art. 267, c. 2 c.p.p., il nuovo c. 3-bis dell'art. 132 del codice *privacy* reintroduce[515] una procedura di apprensione "immediata", che consente al pubblico ministero, per il caso in cui sussistano ragioni d'urgenza, di disporre la diretta acquisizione dei tabulati telefonici presso l'ente gestore del servizio, salva la necessaria convalida *ex post* ad opera dell'organo giurisdizionale. Infine, con riguardo all'ambito di applicazione soggettiva della *data retention*, il legislatore italiano è rimasto silente di fronte alla troppo generica e indeterminata individuazione dei soggetti nei confronti dei quali l'organo giudicante potrebbe autorizzare l'apprensione dei dati di traffico, contenuta nella sentenza *H.K.*: si tratta di una scelta condivisibile, nella misura in cui ciò garantisce al pubblico ministero di poter accedere alle informazioni di tutti quei soggetti, diversi dall'indagato o dall'imputato, che siano a qualsiasi titolo legati ai fatti oggetto di accertamento. Com'era prevedibile, l'intervento del legislatore non è andato esente da critiche[516]. Nondimeno, si può convenire che, nel complesso, l'interpolazione normativa si lasci apprezzare, se non altro «per aver ricondotto a sistema una disciplina che, sino a poco tempo fa, mirava a

[513] È il caso dei «reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi».

[514] È appena il caso di precisare che, stante la nuova formulazione del c. 3 dell'art. 132 del codice *privacy*, risulterebbe esclusa la possibilità, in precedenza espressamente riconosciuta all'avvocato di parte, di richiedere direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito.

[515] Cfr. art. 4-bis, l. 31 luglio 2005, n. 155.

[516] V., in particolare, L. FILIPPI, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in *www.penaledp.it*, 1 ottobre 2021, p. 9 ss., ad avviso del quale sarebbe stata opportuna una "riserva di codice", inserendo le nuove disposizioni subito dopo gli artt. 266-271 c.p.p.

garantire esclusivamente l'efficienza delle indagini nell'ottica di una tutela indiscriminata dell'interesse collettivo alla repressione dei reati, risultando alquanto carente, viceversa, sotto il profilo della tutela dei diritti fondamentali della persona umana»[517].

Il d.l. 30 settembre 2021, n.132, recante la disciplina sull'acquisizione dei dati di traffico "esterno" telefonico e telematico, è stato convertito con modificazioni ad opera della legge 23 novembre 2021, n. 1781. Per quanto significative siano le modifiche apportate al testo originario del decreto-legge, si può dire che il prodotto finale lasci alquanto desiderare, soprattutto con riguardo al rispetto del canone di proporzionalità, enunciato dalla Corte di Giustizia[518]. Se, da un lato, appare evidente il tentativo di plasmare la disciplina relativa dell'acquisizione dei tabulati sulla base di quella, certamente più garantita, prevista in materia di intercettazioni di conversazioni o comunicazioni, dall'altro lato non si può che riscontrare come l'ossequio ai principi europei incontri un limite rappresentato dalla minore invasività dell'acquisizione di dati esteriori che prescindono dai contenuti delle comunicazioni. In altri termini, «il legislatore sembra ancora condizionato nelle sue scelte dal latente principio giurisprudenziale di non dispersione della prova per cui nel bilanciamento dei valori la tutela della riservatezza finisce per essere soccombente»[519].

Recentemente la Corte di Lussemburgo è di nuovo tornata a confrontarsi con la disciplina dei tabulati telefonici in occasione della sentenza del 5 aprile 2022 nel caso *G.D.*[520]. La pronuncia trae origine da un rinvio pregiudiziale della Corte suprema irlandese, che si è trovata a dover scrutinare la compatibilità della legge nazionale in tema di tabulati con il diritto UE. Per quanto da un punto di vista contenutistico non figurino aspetti di particolare novità, si tratta di un arresto interessante, in quanto consente di apprezzare in

[517] A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici*, cit.

[518] In questo senso, L. TAVASSI, *Acquisizione di tabulati, tutela della privacy e rispetto del principio di proporzionalità*, in *Arch. pen*. web, 2022.

[519] L. TAVASSI, *Acquisizione di tabulati*, cit.

[520] Corte giust. UE, 5 aprile 2022, G.D., C-140/20, con nota di F. IOVENE, *Nuova decisione della Corte di giustizia in materia di tabulati: quali conseguenze per l'ordinamento nazionale?*, in *Cass. pen*., 2022, p. 2363 ss. Per un resoconto dei contenuti della pronuncia, v. L. FILIPPI, *La Corte di Lussemburgo ribadisce lo stop ai tabulati: una fine annunciata*, in www.penaledp.it, 14 aprile 2022; G. SPANGHER, *Spangher: «La Corte di Giustizia della Ue ha sancito la fine del regime dei tabulati»*, in www.ildubbio.it, 20 aprile 2022; F. RESTA, *Dalla conservazione generalizzata a quella mirata e rapida: la Corte di giustizia ridelinea i contorni della data retention*, in www.giustiziainsieme.it, 7 aprile 2022; e, nella letteratura straniera, J. R. RODRIGUEZ LAINZ, *La Evolución de la Jurisprudencia del Tribunal de Justicia de la Unión Europea en Materia de Conservación Indiscriminada de Datos de Comunicaciones Electrónicas en la STJUE del Caso G.D. y Comissioner an Garda Síochána*, in *Diario La Ley*, 19 aprile 2022.

maniera dettagliata alcuni princìpi cardine elaborati dalla Corte sul tema nei suoi precedenti. Anzitutto, «la Corte ha posto ancora una volta in rilievo il divieto di una conservazione generalizzata e indifferenziata dei dati di traffico ai fini di lotta alla criminalità grave, chiarendo (*omissis*) che il tabulato telefonico non può essere qualificato alla stregua di un mezzo di ricerca della prova "retrospettivo"»[521]. Soffermandosi sul tema dell'efficacia empirica degli strumenti di *data retention* ai fini di contrasto alla criminalità, ha quindi precisato che l'efficacia delle azioni penali dipende, più che dal ricorso ad un unico strumento di indagine, dal complesso dei mezzi investigativi a disposizione delle autorità inquirenti. In definitiva, «esclusa la legittimità di una qualunque forma di *bulk data retention*, la "pietra angolare" del ragionamento adottato dalla Corte di giustizia, sin dalle pronunce più risalenti, è senz'altro costituita dalla cd. *targeted retention*, ovverosia da una conservazione mirata e limitata dei dati di traffico telefonico che, ad avviso dei giudici europei, risulterebbe conforme ai principi di proporzionalità e necessità»[522].

All'indomani dell'arresto comunitario *de quo* il dibattito sui tabulati telefonici si è riaperto. In effetti, i princìpi da ultimo enunciati dalla Corte di Giustizia sembrano indurre un ripensamento della neo-introdotta disciplina ad opera del d.l. n. 132/2021, che non sembra davvero adeguarsi ai *dicta* dei giudici comunitari[523]. Due sono, in particolare, le questioni che si pongono e, segnatamente, la possibilità di ottenere dai gestori telefonici la conservazione mirata, per un tempo definito, di tabulati telefonici, nonché l'individuazione dei criteri che giustifichino tale richiesta. Mentre rispetto alla prima non paiono sussistere ostacoli alla luce della disciplina relativa alla *data retention*, così come modificata dal legislatore del 2021, più complessa risulta la soluzione alla seconda questione, nella misura in cui, a voler accogliere gli insegnamenti della Corte di Giustizia e riconoscere così l'illegittimità di una conservazione generalizzata dei dati, si renderebbe opportuna una predeterminazione dei criteri in base ai quali l'autorità giudiziaria sia abilitata a chiedere la conservazione mirata. Ad oggi, quindi, sembra non esserci pace per la tormentata disciplina dei tabulati telefonici, destinata a subire, con buona probabilità, una nuova interpolazione da parte del legislatore.

---

[521] A. MALACARNE – G. TESSITORE, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di Giustizia: ancora inadeguata la disciplina interna?*, in *Arch. pen*. web, 2022, p. 28.

[522] *Ibidem*, p. 35.

[523] In questo senso, L. FILIPPI, *La Corte di Lussemburgo ribadisce lo stop ai tabulati: una fine annunciata*, in www.penaledp.it, 14 aprile 2022.

CAPITOLO IV
LA TENSIONE TRA TUTELA DEI DIRITTI FONDAMENTALI ED ESIGENZE REPRESSIVE

SOMMARIO: 1. Divieti di utilizzazione: le molteplici sfaccettature dell'art. 271 c.p.p. – 2. Le intercettazioni indirette *ex* art. 270 c.p.p. (c.d. intercettazioni a strascico): la nozione di "procedimento diverso". – 3. Il segreto *ex* art. 114 c.p.p. tra diritto di cronaca e tutela della riservatezza: la divulgazione abusiva del contenuto del captato. – 4. Un po' di numeri.

5. *Divieti di utilizzazione: le molteplici sfaccettature dell'art. 271 c.p.p.*

In materia di intercettazioni la categoria dell'inutilizzabilità trae origine dalla sentenza della Corte costituzionale n. 34 del 1973[524], con la quale il giudice delle leggi intervenne sull'art. 266 del codice di procedura penale del 1930. In linea generale, l'art. 191 del vigente codice di rito disciplina la c.d. inutilizzabilità generale, escludendo che possano essere utilizzate le prove «acquisite in violazione dei divieti stabiliti dalla legge». Per quanto concerne le intercettazioni, in luogo della norma generale di cui all'art. 191 c.p.p., trova applicazione quella *ad hoc* di cui all'art. 271 c.p.p., che delinea una forma di inutilizzabilità "speciale". Questa linea interpretativa è stata sposata dalle Sezioni Unite[525], che, valorizzando la particolare insidiosità dello strumento investigativo in discorso, hanno ritenuto di dover sottrarre alla conoscenza dell'organo giurisdizionale le risultanze di quelle captazioni acquisite in spregio ai limiti imposti dall'ordinamento a tutela dei diritti fondamentali. La giurisprudenza di legittimità[526] ha, nondimeno, ammesso che gli esiti captativi, dei quali sia stata riconosciuta l'inutilizzabilità *ex* art. 271 c.p.p., possano comunque valere come *notitia criminis* per l'espletamento di nuove indagini. In materia di inutilizzabilità non opera infatti il principio di cui all'art. 185 c.p.p., secondo il quale la nullità dell'atto travolge gli atti consecutivi dipendenti da quello dichiarato nullo[527], essendo la sanzione dell'inutilizzabilità dei mezzi probatori illegittimi riservata al solo momento

[524] Corte cost., sent. 4 aprile 1973, n. 34.

[525] Cass., sez. un., 27 marzo1996, n. 3, Monteleone; Cass., sez. un., 20 novembre 1996, n. 21, Glicora ed altri.

[526] Fra gli altri, Cass., 22 novembre 2007, n. 47109; Cass., 2 marzo 2010, n. 16293.

[527] V., in proposito, Cass., 29 aprile 2004, n. 26112, Canaj; nello stesso senso Cass., 10 ottobre 2019, n. 44114.

giurisdizionale; al contrario, delle informazioni assunte attraverso mezzi di prova illegittimi – e quindi inutilizzabili da parte del giudice – ben possono servirsi il pubblico ministero e la polizia giudiziaria a fini investigativi[528]. Questi principi hanno trovato l'avallo della Corte costituzionale[529], la quale ha escluso la configurabilità di un principio di "inutilizzabilità derivata" sulla falsariga di quanto è previsto, invece, in materia di nullità dall'art. 185 c.p.p.

L'art. 271 c.p.p., delineando una garanzia fondamentale in materia di intercettazioni, individua alcune norme la cui violazione comporta la sanzione dell'inutilizzabilità. Posto che la *ratio* sottesa a questa disposizione è quella di evitare un'elusione dei limiti previsti per il ricorso allo strumento delle intercettazioni, nei casi in cui al pubblico ministero non sarebbero consentite[530], il divieto probatorio in questione opera sia quando la norma è configurata in termini di proibizione sia quando è formulata in termini di permesso condizionato[531]. Ai sensi dell'art. 271 c.p.p., che attua il precetto generale di cui all'art. 191 c.p.p., si tratta delle ipotesi in cui le intercettazioni siano state eseguite fuori dai casi contemplati dalla legge (art. 266 c.p.p.) ovvero non siano state rispettate le regole in tema di autorizzazioni, proroghe e procedure d'urgenza (art. 267 c.p.p.) o le disposizioni in materia di registrazione, verbalizzazione e impianti utilizzabili (art. 268, c. 1 e 3 c.p.p.). In questi casi, il c. 3 dell'art. 271 c.p.p. prevede che, in ogni stato e grado del processo, il giudice disponga la distruzione della documentazione delle intercettazioni, salvo che costituisca corpo del reato. Tale forma di inutilizzabilità patologica si ispira all'esigenza di circoscrivere l'ambito di conoscenza dell'organo giurisdizionale alle prove legittimamente acquisite e, in particolare, a quelle ottenute nel rispetto del fondamentale e inviolabile diritto alla segretezza delle comunicazioni[532]. Il nuovo c. 1-bis dell'art. 271 c.p.p., introdotto ad opera del d.lgs. n. 216 del 2017 e dedicato al captatore informatico, sanziona poi con l'inutilizzabilità i dati catturati nel corso delle operazioni installazione del *software* all'interno del dispositivo da controllare (art. 268, c. 3-bis c.p.p.) e quelli acquisiti al di fuori dei limiti temporali e spaziali

[528] Cass., 10 febbraio 2004, n. 16499, Mache; Cass., sez. un., 31 ottobre 2001, Policastro, n. 42792.

[529] Corte cost., sent. 15 luglio 2019, n. 219.

[530] F. CAPRIOLI, *Intercettazioni illecite, intercettazioni illegali, intercettazioni illegittime*, in AA. VV., *Le intercettazioni un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti: atti del Convegno, Milano, 5-7 ottobre 2007*, Milano, 2009, p. 139 ss.

[531] V. GREVI, *Prove*, in G. CONSO-V. GREVI, *Profili del nuovo Codice di procedura penale*, Padova, 1990, p. 156.

[532] F. RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001, p. 7.

stabiliti dal giudice (art. 267, c. 1 c.p.p.). In parziale analogia con quanto previsto per la testimonianza indiretta (art. 195, c. 6 c.p.p.), il c. 2 dell'art. 271 c.p.p. prevede, infine, l'inutilizzabilità delle captazioni che coinvolgano soggetti appartenenti alle categorie vincolare al segreto professionale (art. 200 c.p.p.), «salvo che le stesse persone abbiano deposto sugli stessi fatti o li abbiano in altro modo divulgati». Un divieto ulteriore, alla cui inosservanza consegue la sanzione dell'inutilizzabilità, è specificamente previsto dall'art. 103, c. 7 c.p.p. in rapporto alle conversazioni o comunicazioni dei difensori, degli investigatori privati, dei consulenti tecnici e loro ausiliari ovvero in relazione alle conversazioni o comunicazioni tra i medesimi e le persone da loro assistite (art. 103, c. 5 c.p.p.).

Il primo quesito che sorge dalla lettura dell'art. 271 c.p.p. concerne la natura dell'elenco ivi contemplato: in particolare, si tratta di capire se si sia in presenza di un catalogo di ipotesi di inutilizzabilità tassativo ovvero se l'interprete sia abilitato a individuare ulteriori casi di omologa invalidità. Secondo alcuni[533], l'articolo in questione, attraverso il rinvio agli artt. 267 e 268, c. 1 e 3 c.p.p., porrebbe capo ad una distinzione tra le inosservanze determinanti inutilizzabilità e quelle, non afferenti alle medesime clausole, alternativamente riconducibili alla categoria della nullità o della mera irregolarità. Inoltre, se si considera lo scopo ultimo perseguito dall'art. 271 c.p.p., ovvero di evitare che risultati illegittimamente ottenuti possano essere valutati dal giudice per formare il proprio convincimento, si può arrivare alla conclusione che si tratta di ipotesi tassative di inutilizzabilità.

Mentre non vi è dubbio che l'ipotesi di inutilizzabilità prevista per le intercettazioni eseguite fuori dai casi consentiti dalla legge costituisca attuazione della riserva di legge *ex* art. 15, c. 2 Cost.[534], qualche considerazione in più merita quella concernente la violazione delle norme di cui all'art. 168, commi 1 e 3, del codice di rito, le quali impongono che le comunicazioni siano registrate e subito verbalizzate e che le operazioni avvengano mediante impianti installati presso la procura della Repubblica. Quanto alla violazione del c. 1, l'inutilizzabilità consegue sia alla mancanza del verbale relativo alle operazioni sia al difetto delle indicazioni prescritte per lo stesso verbale[535]: in questo modo, il richiamo al primo

[533] Cfr., in tal senso, C. DI MARTINO-T. PROCACCIANTI, *Le intercettazioni telefoniche*, Padova, 2001, p. 220.

[534] P. BALDUCCI, *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Milano, 2002, p. 189.

[535] *Ibidem*, p. 188.

comma dell'art. 268 c.p.p. finisce per ricomprendere anche l'osservanza dell'art. 89, c. 1 delle disposizioni di attuazione, che definisce il contenuto del documento in questione, richiedendo l'indicazione degli estremi del decreto che ha disposto l'intercettazione, la descrizione delle modalità di registrazione, l'annotazione del giorno e dell'ora di inizio e di cessazione dell'intercettazione, nonché i nominativi delle persone che hanno preso parte alle operazioni[536]. Secondo una parte della dottrina[537], tuttavia, il richiamo a questa disposizione non è corretto, non comminando la stessa alcuna invalidità per il mancato rispetto delle prescrizioni che detta; per altro verso, essendo la materia delle invalidità improntata al canone di tassatività, la portata dell'inutilizzabilità non potrebbe essere dilatata al punto da ricomprendere le disposizioni dettate da una norma a cui non fa espresso rinvio l'art. 271 c.p.p.

Alla luce di tali considerazioni, può essere evocata una controversa pronuncia della Cassazione, intervenuta proprio sulla questione della mancata sottoscrizione del verbale delle operazioni relative ad intercettazioni[538]. La decisione trae origine dal ricorso presentato dall'indagato avverso l'ordinanza del Tribunale di Catanzaro, che confermava la custodia cautelare in carcere disposta dal g.i.p. Figura nel ricorso, fra gli altri motivi, l'asserita inutilizzabilità di tutti i verbali riportanti le trascrizioni delle comunicazioni telefoniche intercettate, stante la mancata sottoscrizione dei ridetti atti da parte dell'interprete nominata dal pubblico ministero. In particolare, secondo la difesa, l'invalidità deve desumersi dal combinato disposto degli artt. 268, c. 1 c.p.p. e 89 disp. att. c.p.p. Sul punto, la Cassazione[539], che respinge il ricorso, è di avviso contrario: infatti, «la mancata sottoscrizione del verbale da parte del pubblico ufficiale che ha proceduto alle operazioni non determina inutilizzabilità, in quanto tale inosservanza non rientra tra i casi di cui all'art. 271 c.p.p., ma si configura, invece, come una ipotesi di nullità relativa, eccepibile nei termini e nei modi stabiliti dagli artt. 181 e 182 c.p.p.». La sentenza *de qua* ha determinato una spaccatura in dottrina tra chi, accogliendo la ricordata massima giurisprudenziale, ha ritenuto che la mancata sottoscrizione del verbale integri una nullità relativa – e non una forma di

[536] F. CORDERO, *Procedura penale*, Milano, 1992, p. 315.

[537] Così C. DI MARTINO-T. PROCACCIANTI, *Le intercettazioni telefoniche*, cit., p. 224.

[538] V., sul punto, C. R. BLEFARI, *La Corte di Cassazione si pronuncia sulla questione della mancata sottoscrizione del verbale delle operazioni relative ad intercettazioni, in Proc. pen. giust., 2018, p. 341 ss.*

[539] Cass., sez. III, 24 gennaio 2017, n. 13661.

inutilizzabilità –, non essendo detta irritualità ricompresa nell'elenco dell'art. 271 c.p.p.[540], e chi, al contrario, valorizzando il rapporto sussistente tra gli artt. 268, c. 1 c.p.p., 271 c.p.p. e 89 disp. att. c.p.p., ha asserito di doversi estendere l'inutilizzabilità a qualsiasi ipotesi di difformità dal modello legale[541].

Soffermiamoci adesso sul c. 3 dell'art. 271 c.p.p. e, segnatamente, sulla fase di operatività della disposizione *de qua*. Per quanto la norma faccia riferimento al solo «processo», in passato si disquisiva circa la sua possibile applicazione già nella fase delle indagini preliminari. Oggi i dubbi sono stati fugati dall'istituzione della nuova procedura di acquisizione *ex* art. 268 c.p.p., in forza della quale, all'esito della procedura di selezione e acquisizione delle conversazioni, il giudice procede, anche d'ufficio, allo stralcio delle registrazioni di cui rileva l'inutilizzabilità. Dato che questo materiale è destinato a rimanere custodito nell'archivio digitale di cui all'art. 269 c.p.p., risulta inimmaginabile un'applicazione dell'art. 271, c. 3 c.p.p. nella fase delle indagini preliminari. Occorre, precisare, peraltro, che la distruzione di cui alla disposizione in esame diverge da quella prevista ai commi 2 e 3 dell'art. 269 c.p.p. Anzitutto, quanto all'oggetto, mentre l'art. 271, c. 3 c.p.p. si riferisce alle intercettazioni eseguite fuori dai casi consentiti dalla legge o senza l'osservanza delle disposizioni previste dagli artt. 267 e 268, c. 1 e 3 c.p.p., la distruzione *ex* art. 269 c.p.p. inerisce ai verbali e alle registrazioni non acquisite in quanto irrilevanti e/o non trascrivibili *ex* art. 268, c. 2-bis c.p.p., quindi diverse da quelle inutilizzabili poc'anzi menzionate. Inoltre, mentre l'art. 269, c. 2 c.p.p. riconosce, a tutela della riservatezza, la facoltà agli interessati di domandare la distruzione della documentazione non acquisita, l'art. 271 c.p.p. prevede un'attività di distruzione "doverosa", che può essere disposta anche d'ufficio. Quanto alle modalità della distruzione, infine, diversamente dall'art. 271, c. 3 c.p.p., ai sensi del quale l'ordine di distruzione è dato dal giudice in ogni stato e grado del processo, senza indicazione di una particolare procedura da osservare, l'art. 269, c. 2 c.p.p. prevede la conservazione nell'archivio riservato delle registrazioni non acquisite «fino alla sentenza non più soggetta a impugnazione», mentre rispetto ad eventuali istanze di distruzione il giudice decide in camera di consiglio all'esito di un sub-procedimento, da svolgersi nelle forme di cui all'art. 127 c.p.p.

[540] In tal senso C. DI MARTINO-T. PROCACCIANTI, *Le intercettazioni telefoniche*, cit., p. 125; E. APRILE, *Intercettazioni di comunicazioni*, in A. SCALFATI (a cura di), *Trattato di procedura penale* Vol. II, Tomo I, Torino, 2009, p. 512 ss.

[541] Così P. BALDUCCI, *Le garanzie nelle intercettazioni*, cit., p. 187.

Ciò che più interessa, tuttavia, è la specifica scansione temporale in cui può essere disposta la distruzione. A questo riguardo, si segnala l'ormai consolidato orientamento pretorio secondo il quale, per poter addivenire alla distruzione delle intercettazioni, è necessario che sia divenuto irrevocabile il provvedimento che ne dichiara l'inutilizzabilità. Il punto è stato chiarito dalla Cassazione[542], ad avviso della quale «la distruzione della documentazione delle intercettazioni inutilizzabili presuppone che l'inutilizzabilità sia dichiarata con decisione processualmente insuscettibile di modifiche e, pertanto, non può essere ordinata nel caso in cui detta decisione sia intervenuta nel giudizio abbreviato richiesto solo da alcuni dei coimputati». Sempre la S.C. ha precisato che «la distruzione della documentazione delle intercettazioni, i cui risultati non possono essere utilizzati a norma dell'art. 271, commi primo e secondo, c.p.p., non può essere disposta in esecuzione di una dichiarazione di inutilizzabilità intervenuta nel procedimento incidentale "de libertate", perché presuppone una statuizione di inutilizzabilità processualmente insuscettibile di modifiche, che faccia escludere la possibilità di utilizzazione futura di quelle conversazioni nell'ambito del processo»[543] e che «in tema di intercettazioni telefoniche, il giudice delle indagini preliminari non può disporre, ai sensi dell'art. 271, comma 3, c.p.p., la distruzione delle intercettazioni dichiarate inutilizzabili in sede di riesame, essendo necessaria una decisione in ordine all'inutilizzabilità adottata nell'ambito del processo di cognizione ed insuscettibile di modifiche»[544].

La clausola di salvezza contenuta nel c. 3 dell'art. 271 c.p.p. contempla un'eccezione all'obbligo generale di distruzione della documentazione avente ad oggetto i dialoghi inutilizzabili: è il caso in cui si tratti del corpo del reato, sul quale è intervenuto la nota sentenza "Floris"[545]. A questo riguardo, le Sezioni Unite hanno chiarito che «in tema di intercettazioni, la conversazione o comunicazione intercettata costituisce corpo del reato allorché essa integra di per sé la fattispecie criminosa e, in quanto tale, è utilizzabile nel processo penale». Alla luce di ciò, è chiaro che l'art. 271, c. 3 c.p.p. non si riferisce alle intercettazioni abusive che fuoriescono dal perimetro della disciplina codicistica, ma

[542] Cass., 21 gennaio 2009, n. 14461.

[543] Cass., 25 novembre 2015, n. 8953.

[544] Cass., 2 dicembre 2019, n. 51021.

[545] Cass., sez. un., 26 giugno 2014 – 23 luglio 2014, n. 32697, Floris.

concerne quelle intercettazioni, inutilizzabili *ex* art. 271 cpp, in cui la conversazione stessa integri reato.

6. *Le intercettazioni indirette* ex *art. 270 c.p.p. (c.d. intercettazioni a strascico): la nozione di "procedimento diverso"*

Se i profili illustrati riguardano l'inutilizzabilità all'interno del procedimento stesso, è questione dai contorni assai più delicati quella concernente l'utilizzazione delle intercettazioni in procedimenti diversi. Il codice di rito dedica a questa particolare ipotesi una norma specifica, l'art. 270 c.p.p., che stabilisce, in via generale, che «i risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti». La *ratio* sottesa a tale disposizione è insita nel particolare rilievo che la Costituzione accorda all'intangibilità della sfera privata e dal quale scaturisce il rigore delle condizioni di validità alle quali soggiace l'attività captativa. A garanzia del corretto bilanciamento delle contrapposte esigenze di accertamento penale e tutela della riservatezza, infatti, l'atto dell'autorità giudiziaria con cui vengono autorizzate le intercettazioni dev'essere munito di adeguata e specifica motivazione: onde evitare che un'indiscriminata utilizzazione degli esiti captativi in procedimenti diversi da quello nel quale gli stessi sono stati attivati si risolva in un'elusione della garanzia in discorso, ovvero nel difetto di un preventivo vaglio giudiziale circa l'effettiva sussistenza dei presupposti stabiliti dalla legge nel caso concreto, l'art. 270 c.p.p. fissa quindi un generale divieto probatorio, impedendo l'impiego dei ridetti esiti captativi al di fuori della loro sede naturale. In caso contrario, i presupposti legali costituirebbero oggetto di controllo nell'ambito del solo procedimento *a quo* – ma non in quello *ad quem* –, con buona pace della *privacy* di quei soggetti terzi, completamente estranei al reato per cui si procede, che rimangono accidentalmente coinvolti nel "tritacarne" dell'intercettazione.

Il divieto di cui all'art. 270 c.p.p. sconta, tuttavia, una rilevante eccezione, rappresentata dai risultati «rilevanti e indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza», ai quali la legge n. 7 del 2020 ha aggiunto i reati «di cui all'art. 266, c. 1». Quanto alla tradizionale deroga al divieto *ex* art. 270 c.p.p., la Corte costituzionale si è espressa, in tempi ormai lontani, positivamente in punto di compatibilità con la Carta

fondamentale: secondo il giudice delle leggi[546], infatti, sussisterebbe un nesso diretto tra l'art. 270 c.p.p. e l'art. 15 Cost.; inoltre, il requisito della "indispensabilità" si ergerebbe a garanzia del contemperamento fra i vari interessi in gioco e assicurerebbe la stretta necessarietà rispetto al concreto soddisfacimento dell'interesse alla repressione dei reati. È appena il caso di precisare che la novella del 2020 ha giustapposto all'originario presupposto della "indispensabilità" quello della "rilevanza", innalzando il livello di tutela riservato alla libertà e segretezza delle comunicazioni.

Fermo restando il divieto generale di trasmigrazione extra-procedimentale degli esiti captativi, il legislatore, attraverso il rinvio ai reati di cui all'art. 266, c. 1 c.p.p., ha, però, dato luogo ad una ambiguità interpretativa, che ha generato due orientamenti contrapposti: infatti, mentre taluni[547] propendono per una tesi restrittiva, ovvero per la necessità di una sussistenza congiunta dei due requisiti tipizzati dalla norma, secondo altri[548] la presenza, dopo la congiunzione "e", della locuzione "dei reati", in prosecuzione del precedente sintagma "dei delitti", indurrebbe a concludere che ci si debba riferire a due distinte categorie di deroghe. In attesa di una presa di posizione della giurisprudenza, pare preferibile, in ossequio alla *littera legis*, accogliere la seconda linea ermeneutica. Accanto al problema del carattere cumulativo o alternativo della deroga al generale divieto in esame, si pongono almeno altre due questioni di ordine applicativo. La prima attiene alla possibilità di utilizzare le intercettazioni nell'ambito di un procedimento, caratterizzato da una pluralità di imputati e imputazioni, in cui l'arresto in flagranza risulta obbligatorio solo per taluni imputati e talune imputazioni. In altri termini, si tratta di stabilire se le intercettazioni provenienti dal procedimento *a quo* siano utilizzabili o meno per la prova di tutti i reati contestati nel procedimento *ad quem* e nei confronti di tutti gli imputati, quindi anche per i reati rispetto ai quali l'arresto obbligatorio in flagranza non è previsto. La seconda questione concerne, invece, l'ipotesi della riqualificazione dell'imputazione originaria nell'ambito del procedimento *ad quem*, qualora il reato per cui si procede fuoriesca dai casi nei quali l'art. 380 c.p.p. prevede l'arresto obbligatorio in flagranza. Al quesito la giurisprudenza[549] ha

[546] Corte cost., sent. 10 febbraio 1994, n. 63.

[547] L. FILIPPI, *Intercettazioni: finalmente una legge! (ma in vigore a settembre), in Penale, diritto e procedura, 2020.*

[548] F. ALVINO, *La circolare delle intercettazioni e la riformulazione dell'art. 270 c.p.p.: l'incerto pendolarismo tra regola ed eccezione, in Sistema penale, 5/2020, 2020.*

[549] Tra le tante, Cass., 28 febbraio 1994, n. 5331, Roccia ed altri.

risposto focalizzando l'attenzione sul momento dell'acquisizione nel procedimento *ad quem* degli atti assunti nel procedimento *a quo*: di conseguenza, i risultati dell'atto originariamente legittimo conservano tale caratteristica anche se la modifica della qualificazione giuridica del reato fa diventare, all'esito di una valutazione *ex post*, non più conforme alla previsione legale l'intercettazione eseguita. In definitiva, se il titolo di reato per cui si procedeva al momento dell'acquisizione dei risultati di intercettazioni effettuate in altro procedimento rientrava nell'elenco di cui all'art. 380 c.p.p., allora la sua eventuale modifica successiva non incide sull'utilizzabilità di tali risultati[550].

Nozione assai spinosa in materia di intercettazioni c.d. indirette è quella di "procedimento diverso". A questo riguardo, non si può prescindere dagli insegnamenti delle Sezioni Unite "Cavallo" del 2020[551], che hanno composto il contrasto fra i diversi indirizzi giurisprudenziali emersi sul tema, affermando che non si è innanzi ad "altro procedimento" con riguardo a tutti quei reati «che risultano connessi *ex* art. 12 c.p.p. a quelli in relazione ai quali l'autorizzazione era stata *ab origine* disposta, sempreché rientrino nei limiti di ammissibilità previsti dalla legge». Per meglio comprendere il *dictum* della S.C., è forse opportuno ripercorrere sommariamente i vari orientamenti che si sono formati nel corso del tempo in materia.

Secondo il filone interpretativo maggioritario[552], ispirato ad un criterio di natura sostanzialistica, il concetto di "procedimento diverso" non era coincidente con quello di reato diverso, essendo il primo più ampio del secondo. Laddove tra il contenuto dell'originaria notizia di reato, che aveva legittimato il ricorso all'intercettazione, e quello degli altri reati per i quali si procedeva vi fosse stata una stretta connessione sotto il profilo oggettivo, probatorio e finalistico, il procedimento relativo a questi ultimi veniva considerato identico e, pertanto, non assoggettabile alle limitazioni di cui all'art. 270 c.p.p. Questo orientamento aveva trovato l'avallo della stessa Cassazione in un precedente nomofilattico[553], che, sia pure incidentalmente, aveva ancorato la nozione di "procedimento diverso" al criterio sostanzialistico prescindendo da elementi formali, quali il numero di

[550] Cass., 24 giugno 2005, n. 33751, Bellato ed altri.

[551] Cass., sez. un., 28 novembre 2019 – 2 gennaio 2020, n. 51, Cavallo, in *CED*, n. 277395.

[552] Cass., 23 settembre 2014, n. 52503, Sarantsev; Cass., 19 gennaio 2010, n. 7320, Verdoscia; Cass., 19 gennaio 2004, n. 9579, Amato; Cass., 4 novembre 2004, n. 46075; Cass., 11 gennaio1998, n. 6242, Tomasello; Cass., 16 maggio 1997, n. 1972, Pacini Battaglia.

[553] Cass., sez. un., 26 giugno 2014, n. 32697, Floris.

iscrizione del procedimento nel registro *ex* art. 335 c.p.p., e considerando decisiva, ai fini dell'individuazione dell'identità dei procedimenti, l'esistenza di una connessione tra il contenuto dell'originaria *notitia criminis*, in relazione alla quale erano state disposte le intercettazioni, e gli altri reati per i quali si procedeva.

Altro indirizzo giurisprudenziale, di stampo maggiormente formalistico[554], poneva invece l'accento su una nozione formale di "procedimento diverso", valorizzando l'inerenza delle risultanze relative ai reati diversi da quelli oggetto del provvedimento autorizzativo al procedimento in cui era stato disposto il mezzo di ricerca della prova in discorso. In questo modo, elemento dirimente veniva ad essere l'unitarietà iniziale, con la conseguenza che i risultati dell'intercettazione autorizzata nell'ambito di un determinato procedimento concernente uno dei delitti *ex* art. 266 c.p.p. risultavano utilizzabili anche per tutti gli altri reati oggetto del medesimo procedimento, a prescindere da condizionamenti di altro genere[555].

Un terzo orientamento, più risalente e rigoroso[556], negava, infine, l'utilizzazione dei risultati intercettivi al di fuori dei casi tassativamente elencati all'art. 270, c. 1 c.p.p., ancorché il procedimento *a quo* e quello *ad quem* risultassero strettamente connessi sotto il profilo oggettivo o probatorio. In altri termini, l'opzione ermeneutica in esame equiparava la nozione di "procedimento" a quella di "reato", così risultando inidoneo a superare il divieto *ex* art. 270 c.p.p. qualsivoglia legame sostanziale tra il reato rispetto al quale l'intercettazione era stato autorizzato ed il reato accertato per mezzo dei risultati della stessa.

Sul punto, come ricordato, sono intervenute le Sezioni Unite, ad avviso delle quali l'autorizzazione del giudice costituisce non solo «il fondamento di legittimazione del ricorso all'intercettazione», ma rappresenta anche il «limite all'utilizzabilità probatoria dei relativi risultati ai soli reati riconducibili alla stessa autorizzazione», a pena di trasformare il provvedimento *de quo* in un'autorizzazione in bianco. Il criterio di natura sostanzialistica, elaborato dalla Corte, conduce quindi ad escludere la diversità dei procedimenti nei casi di connessione *ex* art. 12 c.p.p., ma non in quelli di collegamento probatorio *ex* art. 371, c. 2 lett. b) e c). In merito all'ulteriore *quaestio iuris* relativa alla necessità o meno che il diverso reato emerso nel corso dell'intercettazione rientri nei limiti di ammissibilità dettati dall'art.

[554] Cass., 10 ottobre 2013, n. 3253; Cass., 15 luglio 2015, n. 41317; Cass., 23 febbraio 2016, n. 9500; Cass., 4 marzo 2016, n. 26817.

[555] Cass., 4 ottobre 2012, n. 49745.

[556] Cass., 11 dicembre 2008, n. 4169; Cass., 11 dicembre 2012, n. 49930.

266 c.p.p., la Corte ha chiarito che, attraverso la predeterminazione dei reati rispetto ai quali l'intercettazione può essere autorizzata, il legislatore ha inteso circoscrivere il raggio applicativo di questo mezzo di ricerca della prova, costituendo la previsione dei limiti di ammissibilità delle intercettazioni espressione della riserva assoluta di legge di cui all'art. 15 Cost. In definitiva, il divieto ex art. 270 c.p.p. non opera, secondo le Sezioni Unite "Cavallo", nel caso in cui ricorrano queste due condizioni: i reati emersi dalle intercettazioni disposte nel procedimento *a quo* risultano connessi, ai sensi dell'art. 12 c.p.p., a quelli in relazione ai quali l'autorizzazione era stata concessa *ab origine*; tali reati rispettano i limiti di ammissibilità previsti dall'art. 266 c.p.p. Di conseguenza, nel caso in cui sussista connessione *ex* art. 12 c.p.p. tra il contenuto dell'originaria *notitia criminis* alla base dell'autorizzazione ad intercettare e i reati emersi in fase captativa, deve ritenersi che il procedimento sia "identico" e, in quanto tale, non assoggettabile alle limitazioni previste dall'art. 270 c.p.p. Al contrario, troverà applicazione il dispositivo dell'art. 270 c.p.p. in difetto di una connessione *ex* art. 12 c.p.p., dovendosi in questo caso valutare, al più, la sussistenza di una delle eccezioni al divieto di ordine generale previste dalla stessa norma.

La Cassazione è recentemente tornata a confrontarsi coi limiti all'utilizzabilità degli esiti delle intercettazioni all'interno di un diverso procedimento[557]. In risposta alla Procura generale, che ha addotto una serie di argomenti tesi a sollecitare un superamento del principio di diritto enunciato dalle Sezioni Unite "Cavallo", la S.C.[558] ha negato che il limite all'utilizzabilità dei risultati delle intercettazioni, per come interpretato da quest'ultima giurisprudenza, sia il frutto di un'opera creativa *praeter* o *contra legem*. Al contrario, ha affermato che l'esclusione dell'utilizzabilità dei risultati delle intercettazioni per reati non ricompresi fra quelli che consentono il ricorso a tale mezzo di ricerca della prova costituisce «una "piena applicazione" della legge, considerato che l'art. 266 c.p.p. vieta l'impiego delle intercettazioni per i reati che non superino una soglia minima di gravità e per quelli tassativamente indicati».

Problematiche specifiche pone poi la circolazione extra-procedimentale delle intercettazioni nel caso in cui le stesse siano state eseguite mediante captatore informatico. Alla questione è dedicato il c. 1-bis dell'art. 270 c.p.p., inserito dal d.lgs. 29 dicembre 2017, n. 216, e poi modificato dal d.l. n. 161 del 2019. Ai sensi di tale disposizione, «fermo

[557] Cfr., per un esame più approfondito, D. ALBANESE, *La Cassazione ritorna sui limiti all'utilizzabilità degli esiti delle intercettazioni nell'ambito del "medesimo procedimento": una parola definitiva, ma non per il futuro in Sistema Penale, 2021.*

[558] Cass. sez. V, 17 dicembre 2020 - 15 gennaio 2021, n. 1757.

restando quanto previsto dal c. 1, i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione qualora risultino indispensabili per l'accertamento dei delitti indicati dall'art. 266, c. 2-bis». In merito alla clausola di salvaguardia con cui esordisce la disposizione, ci si domanda se il rinvio al c. 1 si riferisca, oltre che alla deroga tradizionale al divieto generale, anche alla ulteriore deroga introdotta dalla novella. Dalla lettura del testo della norma, che evoca i delitti di cui all'art. 266, c. 2-bis c.p.p., pare potersi desumere che l'unica deroga cui il c. 1-bis dell'art. 270 c.p.p. rinvia sia quella concernente i delitti per i quali è obbligatorio l'arresto in flagranza: in effetti, i delitti di cui all'art. 266, c. 2-bis c.p.p. sono solo parzialmente riconducibili al catalogo di cui all'art. 266 c.p.p., cosicché il c. 1-bis dell'art. 270 c.p.p. pone capo ad un'ulteriore ipotesi di utilizzabilità extra-procedimentale dei risultati intercettivi ottenuti mediante captatore informatico. Le intercettazioni *de quibus*, in altri termini, saranno utilizzabili per la prova di reati diversi da quelli per i quali è stata disposta l'autorizzazione, oltre laddove indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza, anche ove risultino indispensabili per l'accertamento dei delitti *ex* art. 266, c. 2-bis c.p.p. In conclusione, pare potersi affermare che, fermo restando il generale divieto di circolazione delle intercettazioni in procedimenti diversi, mentre per le intercettazioni "classiche", oltre alla tradizionale deroga al divieto in questione, opera, a seguito della novella del 2020, l'ulteriore deroga che consente la trasmigrazione degli esiti captativi in un procedimento diverso ove gli stessi risultino indispensabili per l'accertamento dei delitti di cui all'art. 266, c. 1 c.p.p., per le intercettazioni eseguite mediante captatore informatico il c. 1-bis dell'art. 270 c.p.p. consente, oltre alla ricordata eccezione di cui al c. 1 della stessa disposizione, l'utilizzo extra-procedimentale dei risultati intercettivi, laddove essi siano indispensabili, solo per l'accertamento di delitti per i quali l'impiego del captatore risulta sempre consentito. Si tratta, come s'intuisce, di una deroga assai limitata, in quanto riferita ai soli delitti di cui all'art. 51, c. 3-bis e 3-quater c.p.p., nonché ai delitti dei pubblici ufficiali e degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni.

Consideriamo, a questo punto, l'acquisizione delle intercettazioni nel procedimento *ad quem*. Il c. 2 dell'art. 270 c.p.p. stabilisce che «ai fini della utilizzazione prevista dal c. 1, i verbali e le registrazioni delle intercettazioni sono depositati presso l'autorità competente per il diverso procedimento». Dal momento che la norma menziona *expressis verbis* soltanto

i verbali e le registrazioni – e non anche i decreti di autorizzazione, convalida o proroga dell'intercettazione – sono sorti alcuni problemi di ordine interpretativo, che hanno dato luogo a contrasti giurisprudenziali. A comporre tali contrasti sono state le Sezioni Unite "Esposito"[559], che hanno fatto luce sulla distinzione tra i due momenti dell'ammissione dell'intercettazione e della selezione dei verbali e delle registrazioni rilevanti. Pur considerando l'art. 270 c.p.p. soltanto il secondo di tali momenti, resta il fatto che è tutt'altro che irrilevante ai fini del giudizio *ad quem* la legalità del procedimento di autorizzazione ed esecuzione delle intercettazioni disposte nel procedimento *a quo*: di conseguenza, l'illegalità della procedura di ammissione delle intercettazioni renderà inutilizzabile la prova ottenuta anche in altri procedimenti. Discorso diverso vale, invece, con riguardo alla mancata trasmissione al giudice *ad quem* del provvedimento di autorizzazione o proroga delle intercettazioni: infatti, formulando il c. 2 dell'art. 270 c.p.p. un giudizio di sufficienza del deposito dei soli verbali e delle registrazioni, i decreti autorizzativi emessi nel procedimento *a quo* verranno prodotti nel procedimento *ad quem* solo da parte di chi vi abbia interesse, in quanto il controllo sulla conformità alla legge della procedura di ammissione è demandata dalla legge all'iniziativa delle parti e non vi è obbligo alcuno di depositare nel procedimento *ad quem* i decreti autorizzativi. Per altro verso, la Cassazione[560] ha chiarito che il mancato deposito nel procedimento *ad quem* dei verbali e delle registrazioni, in difformità rispetto a quanto previsto dal c. 2 dell'art. 270 c.p.p., dà luogo ad una nullità di ordine generale a regime intermedio, ai sensi del combinato disposto degli artt. 178, lett. c) e 180 c.p.p.

Quanto alle modalità di acquisizione delle intercettazioni nel procedimento diverso vengono in rilievo i commi 6, 7 e 8 dell'art. 268 c.p.p., richiamati dal c. 2 dell'art. 270 c.p.p. Queste previsioni risultano utili per rispondere all'interrogativo inerente all'ipotesi in cui gli esiti captativi, trasmigrati in altro procedimento, vengano dichiarati inutilizzabili dal giudice del procedimento *a quo* e, per l'effetto, l'inutilizzabilità si "propaghi" anche al procedimento *ad quem*. Sul punto, la giurisprudenza si è espressa in termini negativi, sostenendo che la valutazione compiuta dal primo giudice non valga a condizionare l'analogo vaglio operato dal secondo, il quale ben potrebbe ritenere utilizzabili intercettazioni dichiarate inutilizzabili nel procedimento di partenza, essendo l'inutilizzabilità una forma di invalidità a carattere relativo e non assoluto[561]. Per questa ragione, l'art. 270 c.p.p. prevede *expressis verbis*, anche

[559] Cass., sez. un., 17 novembre 2004, n. 45189, Esposito.

[560] In questo senso, Cass., 22 marzo 2001, n. 20919, Zhezha; Cass., 13 marzo 2009, n. 14783, Badescu.

[561] Cass., 10 novembre 2001, n. 13151, Ginfreda.

nel procedimento *ad quem*, la procedura di garanzia costituita dal deposito della documentazione relativa alle operazioni di intercettazione, dall'acquisizione in contraddittorio e dallo stralcio. Diversamente argomentando, le previsioni in questione risulterebbero prive di significato e verrebbe pregiudicata la possibilità di verificare la regolarità formale e sostanziale delle intercettazioni eseguite nel procedimento *a quo* all'interno del procedimento *ad quem*.

Dato che l'art. 270 c.p.p. si riferisce, oltre che al processo in senso stretto, anche, più in generale, al procedimento, i risultati delle intercettazioni eseguite nel procedimento *a quo* non possono, di regola, essere posti a fondamento di una misura cautelare nel procedimento *ad quem*. In altri termini, si ritiene che la disposizione in questione trovi applicazione anche con riguardo alla fase delle indagini preliminari. Tuttavia, secondo un principio ormai consolidato, nulla impedisce che gli esiti captativi del procedimento *a quo* vengano utilizzati come *notitia criminis* ai fini dell'espletamento di accertamenti diretti ad acquisire nuovi elementi di prova. La tesi è confermata sia dalla giurisprudenza costituzionale[562], in base alla quale la disciplina dell'art. 270 c.p.p. è estranea «al tema della possibilità di dedurre "notizie di reato" dalle intercettazioni legittimamente disposte nell'ambito di altro procedimento», sia da quella di legittimità[563], secondo la quale «l'inutilizzabilità delle intercettazioni in ambito processuale non ne esclude la funzione di notizia di reato, come tale utilizzabile dalla pubblica accusa per l'espletamento delle necessarie indagini volte all'acquisizione di elementi di prova sulla cui base potrà successivamente esercitare l'azione penale».

Ultima questione è quella concernente l'ipotesi in cui la comunicazione intercettata integri essa stessa una condotta criminosa. In punto di applicabilità del divieto di utilizzazione di cui all'art. 270 c.p.p. si è determinato un contrasto giurisprudenziale. Un primo orientamento[564] negava che la disposizione *de qua* potesse trovare applicazione, dal momento che in questi casi «la bobina della registrazione viene ad essere essa stessa corpo di reato». A detto orientamento se ne contrapponeva un altro, di segno opposto[565], secondo il quale bisognerebbe tenere distinto il risultato dell'intercettazione dalla cosa materiale che

[562] Corte cost., sent. 11 luglio 1991, n. 366.

[563] Cass., sez. un., 26 giugno 2014, n. 32697.

[564] Cass., 7 maggio 1993, n. 8670, Olivieri; nello stesso senso, Cass., 18 dicembre 2007, n. 5141, Cincavalli.

[565] Cass., 5 aprile 2001, n. 33187, Ruggiero.

documenta il fatto di reato, altrimenti realizzandosi una sovrapposizione tra la condotta criminosa e l'attività esterna di documentazione. Il nodo è stato sciolto dalle già ricordate Sezioni Unite "Floris"[566], le quali hanno ulteriormente precisato che le bobine delle intercettazioni si sottraggono al divieto *ex* art. 270 c.p.p., allorquando costituiscano esse stesse corpo del reato. In particolare, questa pronuncia ha offerto il destro alla S.C. per definire la nozione di "corpo del reato": intendendola nella sua accezione ampia, essa ha quindi affermato che «la comunicazione o conversazione oggetto di registrazione costituisce corpo del reato, unitamente al supporto che la contiene, solo allorché essa stessa integri ed esaurisca la fattispecie criminosa, mentre deve essere escluso che sia tale una comunicazione o conversazione che si riferisca a una condotta criminosa o che ne integri un frammento, venendo portata a compimento la commissione del reato mediante ulteriori condotte rispetto alle quali l'elemento comunicativo assuma carattere meramente descrittivo». Alla luce di ciò, la registrazione o la trascrizione del dato dichiarativo o comunicativo, che integra la fattispecie criminosa, costituisce corpo del reato e, in quanto tale, dovrà acquisirsi agli atti del procedimento ai sensi dell'art. 431 c. 1 lett. h) c.p.p. e sarà utilizzabile come prova nel processo penale. La presa di posizione delle Sezioni Unite trova conforto, peraltro, nel c. 3 dell'art. 271 c.p.p., che sottrae all'obbligo di distruzione la documentazione delle intercettazioni costituente il corpo del reato.

7. *Il segreto* ex *art. 114 c.p.p. tra diritto di cronaca e tutela della riservatezza: la divulgazione abusiva del contenuto del captato*

«In una moderna democrazia liberale l'amministrazione della giustizia non è una variabile indipendente che risponde soltanto alle norme che la governano e alla capacità dei giudici di darne corretta applicazione, ma è attività che intrattiene con la vita sociale profonde connessioni e reciproci condizionamenti. Tra l'accertamento dei fatti criminali e i media si è instaurata (*omissis*) una relazione osmotica che ha assunto modalità proteiformi, talune fortemente discutibili per contenuti e conseguenze: l'ansia di conoscenza della collettività con riguardo ai fatti che più turbano la convivenza sociale è una troppo appetibile "domanda" perché i mezzi di comunicazione non siano tentati di apprestare una qualsiasi

[566] Cass., sez. un., 26 giugno 2014, n. 32697.

"offerta" che abbia almeno l'apparenza di volerla soddisfare»[567]. Con queste efficaci parole Glauco Giostra delinea i tratti della narrazione della giustizia penale in Italia, un aspetto assai delicato nella vita democratica di un Paese, se si considera la vocazione più intima del processo penale, ovvero quella di realizzare una funzione di coesione sociale[568]. L'art. 101 Cost. prevede che la giustizia sia amministrata in nome del popolo: ciò implica che al cittadino debba essere garantita l'*inspectio* rispetto all'esercizio della *iurisdictio*. Il problema è che «l'informazione giudiziaria, almeno attualmente, è uno specchio che non si limita a riflettere le vicende processuali raccontate, ma spesso ne rimanda un'immagine distorta»[569], cosicché «non soltanto tra la giustizia reale e la giustizia "percepita" vi è uno iato che altera la circolarità democratica (*omissis*), ma la giustizia senza il suo racconto mediatico talvolta sarebbe diversa nel suo svolgimento e nei suoi approdi»[570]. Inoltre, dato che «l'attenzione dei media puntata soltanto sui primi attimi del procedimento finisce per caricarli di un significato probatorio "improprio" e di un'attendibilità che non dovrebbero avere», «troppo spesso matura presso l'opinione pubblica un orientamento colpevolista, che a sua volta non manca di condizionare l'azione e il contributo degli stessi soggetti processuali»[571]. Il che finisce per generare un cortocircuito informativo, oltre che produrre un effetto deformante della narrazione giudiziaria. Ciò è emblematizzato dalla c.d. giustizia mediatica, che costituisce ormai un foro alternativo nel quale si celebrano impropri giudizi con un *iter* informale e rapido: in questo modo, si annulla l'apparato simbolico della procedura e lo si sostituisce con una presunta rappresentazione diretta della realtà, molto più efficiente rispetto alle "lungaggini" del processo. Senonché, mentre il processo è il luogo deputato al "logos", i media sono il luogo del "pathos" e producono una verità, autonoma e immediata, talvolta confliggente con quella processuale[572].

Posto che il procedimento penale è un mondo a sé stante, che nasce e vive in una separazione rispetto alla realtà, il problema è se e come il mondo esterno debba conoscere

[567] G. GIOSTRA, *Prima lezione sulla giustizia penale*, Bari, 2020, p. 161.

[568] V., in questo senso, G. GIOSTRA, *Prima lezione sulla giustizia penale*, cit., p. 25.

[569] G. GIOSTRA, *Prima lezione sulla giustizia penale*, cit., p. 30.

[570] *Ibidem*.

[571] *Ibidem*, p. 32.

[572] Molteplici sono le influenze dei media rispetto al processo penale reale: dalla pressione sugli inquirenti all'effetto perturbatore sugli attori del processo, fino alla subornazione mediatica, che ha luogo quando i testimoni finiscono per rielaborare inconsapevolmente i loro ricordi alla luce degli *input* provenienti dai media.

ed entrare nella dimensione processuale. A questi interrogativi tenta di dare risposta l'art. 114 c.p.p., norma dedicata alla segretezza c.d. esterna degli atti processuali, virtualmente contrapposta all'art. 329 c.p.p., riguardante invece la segretezza c.d. interna. Bisogna premettere che la tensione tra esigenze repressive e tutela dei diritti fondamentali si "scarica" nella contrapposizione tra esigenze sottese al segreto sul procedimento ed esigenze sottese alla pubblicità: se militano a favore delle prime la tutela dell'efficacia dell'azione di accertamento del reato (art. 112 Cost.), il diritto alla riservatezza (artt. 2 e 117 Cost. e art. 8 CEDU), la presunzione di innocenza (art. 27, c. 2 Cost.) e la tutela del contraddittorio e della verginità cognitiva del giudice (art. 111, c. 4 Cost.), per contro rispondono alle seconde il diritto-dovere del popolo di controllare l'amministrazione della giustizia (art. 101, c. 1 Cost.) e il diritto di cronaca (art. 21 Cost.). Ciò detto, non si può tacere che l'art. 114 c.p.p., nel tentativo di trovare un bilanciamento tra queste opposte e contrapposte esigenze, risulti una norma assai controversa e, per questa ragione, oggetto di plurimi ripensamenti da parte del legislatore, a partire dalla stessa rubrica, «divieto di pubblicazione di atti e di immagini», che è stata sostituita dalla l. 16 dicembre 1999, n. 479.

Come si diceva, la norma tutela il c.d. segreto esterno degli atti del procedimento, ponendo dei divieti, in alcuni casi assoluti e in altri relativi, alla pubblicazione mediante la stampa o altri mezzi di comunicazione. Si configura come assoluto il divieto di cui al c. 1, che proibisce la pubblicazione sia del testo che del contenuto degli atti, qualora questi costituiscano oggetto di segreto investigativo: in questo caso il segreto "esterno" si ricollega e rinforza quello "interno", impedendo qualsivoglia forma di riproduzione, anche parziale o per riassunto, degli atti. La distinzione tra atti e contenuto degli atti assume particolare rilievo rispetto agli atti non coperti (o non più coperti) dal segreto investigativo: ai sensi del c. 2 dell'art. 114 c.p.p., infatti, è inibita la pubblicazione del solo testo – ma non anche del contenuto – fino a quando non siano concluse le indagini preliminari (ad esempio, con la notifica dell'avviso di conclusione delle indagini di cui all'art. 415-bis c.p.p.) ovvero fino al termine dell'udienza preliminare. A seguito del d.lgs. 29 dicembre 2017, n. 216, la norma fa salva l'ordinanza cautelare, che non soggiace al richiamato limite di pubblicità: a far data dal 1 settembre 2020, pertanto, tale deroga consente la pubblicazione dell'ordinanza di cui all'art. 292 c.p.p. anche prima del termine indicato per gli altri atti non coperti dal segreto investigativo.

Particolarmente controverso il nuovo c. 2-bis, inserito ad opera del d.l. 30 dicembre 2019, n. 161, e convertito, con qualche modifica, dalla l. 28 febbraio 2020, n. 7, che spiega

efficacia in relazione ai procedimenti penali iscritti successivamente al 31 agosto 2020. Il divieto in questione ha ad oggetto la pubblicazione, anche parziale, del contenuto delle intercettazioni, non acquisite ai sensi degli artt. 268, 415-bis o 454 c.p.p. È bene precisare fin da subito che la norma, mossa dall'esigenza di evitare che venga divulgato il contenuto di intercettazioni irrilevanti ai fini dell'accertamento penale, è destinata ad operare anche oltre i termini indicati nel c. 4 dell'art. 114 c.p.p., al quale non viene fatto alcun rinvio. Più problematica l'attribuzione di un preciso contenuto normativo, anche considerate le prese di posizione di segno opposto che la sua introduzione ha suscitato. Da un lato, infatti, c'è chi sostiene che la novella, introducendo un vero e proprio segreto a tutela della riservatezza sulle intercettazioni prima dello stralcio e poi su quelle stralciate, abbia dato vita ad una disposizione inutile e perfino contraddittoria[573]; dall'altro, c'è chi argomenta che, proprio in forza di essa, il legislatore del 2020 non avrebbe introdotto un segreto sugli atti contenuti nell'archivio *ex* art. 89-bis disp. att. c.p.p.[574] Invero, dal punto di vista della *ratio*, si può forse lodare la scelta del riformatore di «dedicare una regolamentazione speciale volta a introdurre uno specifico bilanciamento tra diritto-dovere di informare e l'interesse a non divulgare conversazioni irrilevanti per l'accertamento penale»[575], non essendo a ciò sufficiente la previsione di cui al c. 1 dell'art. 114 c.p.p., «dal momento che possono venir in rilievo delle intercettazioni non più segrete, ma non ancora depurate dal materiale irrilevante, che è assolutamente ragionevole non pubblicare, nel testo o nel contenuto»[576]. Se un tanto è vero, è possibile trarre dalla disposizione del c. 2-bis una norma speciale, avente ad oggetto il divieto di pubblicare sia il complessivo materiale intercettato prima che sia intervenuto lo *screening* acquisitivo di cui agli artt. 268, 415-bis e 454 c.p.p. sia i verbali e le registrazioni non acquisite in quanto ritenute inutilizzabili o irrilevanti, cioè quella documentazione destinata a confluire nello spazio digitale di cui all'art. 89-bis disp. att. c.p.p. Si può desumere, in altri termini, che il contenuto normativo specifico ed originale del

[573] G. SANTALUCIA, *Il diritto alla riservatezza nella nuova disciplina delle intercettazioni*, in *Sistema Penale*, 2020/1, p. 57.

[574] F. CAPRIOLI, *La procedura di filtro delle comunicazioni rilevanti nella legge di riforma della disciplina delle intercettazioni*, in *Cass. pen*., 2020, p. 1409, ad avviso del quale, con la disposizione *de qua*, il legislatore conferma che le intercettazioni irrilevanti «benché non acquisite, non sono più atti coperti da segreto, dal momento che, in caso contrario, sarebbe bastato l'art. 114 comma 1 c.p.p. a vietare la pubblicazione, anche parziale, del loro contenuto».

[575] M. GIALUZ, *Segreto a tutela della riservatezza e divieto speciale di pubblicazione delle intercettazioni*, in ID. (a cura di), *Le nuove intercettazioni*, cit., p. 70.

[576] *Ibidem*.

c. 2-bis – come tale, non desumibile dal c. 1 – riguardi, in particolare, le intercettazioni utilizzate nella fase delle indagini preliminari per fondare, ad esempio, un provvedimento cautelare, il cui testo dovrà essere sterilizzato con riguardo ai brani intercettati, i quali non potranno essere riferiti neanche indirettamente: in questo modo, gli inviti al *self-restraint* contenuti negli artt. 291, c. 1-ter e 292, c. 2-quater c.p.p., indirizzati rispettivamente al pubblico ministero e al giudice, concernenti l'inserimento nella richiesta e nell'ordinanza cautelare dei soli brani essenziali delle comunicazioni e conversazioni intercettate, si risolvono in due moncherini normativi, figli della mai entrata in vigore riforma Orlando.

Superfluo rilevare, poi, che, laddove riferita al solo contenuto e non anche al testo – come parrebbe potersi inferire dalla *littera legis* – il c. 2-bis rischierebbe di apparire una norma irragionevole, motivo per il quale sembra preferibile un'interpretazione della disposizione *de qua* nel senso di un divieto assoluto di pubblicazione, anche del contenuto delle intercettazioni. A ben vedere, però, la valorizzazione del richiamo al solo "contenuto" da parte del c. 2-bis conduce a prospettare una diversa opzione esegetica della norma, suscettibile di ridimensionarne sensibilmente la portata. Infatti, muovendo dall'assunto che il legislatore abbia compiuto una scelta volontaria e consapevole, si arriva a concludere «che la norma speciale vada circoscritta ai soli casi nei quali viene in rilievo la facoltà di divulgare il contenuto e non il testo di un atto contenente il riferimento alle intercettazioni»[577]. Così inteso, il c. 2-bis non potrebbe trovare applicazione con riguardo all'ordinanza cautelare – ma solo agli atti di indagine –, risultando la prima sicuramente pubblicabile anche nel testo. Ciò detto, non potendosi negare che la tesi da ultimo prospettata desti più di una perplessità, l'ultima parola spetterà, com'è naturale, alla giurisprudenza, onerata del delicato compito di chiarificare il contenuto normativo del divieto di pubblicazione in esame.

Se proseguiamo nella lettura dell'art. 114 c.p.p., incontriamo, al c. 3, il divieto di pubblicare gli atti contenuti nel fascicolo del pubblico ministero: si tratta di una norma, posta a presidio del principio di separazione delle fasi, la cui *ratio* è quella di proteggere la verginità cognitiva del giudice del dibattimento. A differenza degli atti contenuti nel fascicolo per il dibattimento, pertanto, che sono liberamente pubblicabili fin dal momento della formazione del fascicolo[578], i primi sono generalmente pubblicabili nel contenuto, mentre il testo può essere pubblicato solo dopo che è stata pronunciata la sentenza in grado

[577] *Ibidem*, p. 71.

[578] Così Corte cost., n. 59 del 1995.

di appello. Risulta sempre consentita, invece, la pubblicazione degli atti utilizzati per le contestazioni. Nel caso in cui il dibattimento sia celebrato a porte chiuse, è vietata, ai sensi del c. 4, la pubblicazione, anche parziale, degli atti e il giudice, sentite le parti, può estendere il divieto di pubblicazione anche agli atti o parte di atti utilizzati per le contestazioni. In ogni caso, il divieto in questione è destinato a cessare allorché siano trascorsi i termini stabiliti dalla legge sugli archivi di Stato[579] ovvero sia trascorso il termine di dieci anni dalla sentenza irrevocabile e la pubblicazione sia autorizzata dal Ministro della giustizia. Il c. 6 vieta, quindi, la pubblicazione di generalità e immagini dei minorenni testimoni, persone offese o danneggiati dal reato fino a quando non sono divenuti maggiorenni, mentre il c. 7 sancisce un divieto di pubblicazione di immagini della persona *in vinculis* ripresa mentre è ammanettata o sottoposta ad altri mezzi di coercizione fisica.

Quid iuris in caso di violazione dei divieti *de quibus*? L'art. 115 c.p.p., limitandosi a prevedere una sanzione disciplinare[580], rende del tutto ineffettivo il presidio posto a salvaguardia della disposizione precedente, che si rivela una norma *minus quam perfecta*, così come, del resto, le altre sanzioni «previste dalla legge penale». In effetti, l'art. 684 c.p., dedicato alla pubblicazione arbitraria di atti di un procedimento penale, prevede una contravvenzione punita con l'ammenda o l'arresto oblazionabile, mentre solo gli artt. 326 e 379-bis c.p., che incriminano le violazioni del segreto investigativo da parte di soggetti vincolati[581], comminano sanzioni gravi. A questo riguardo, si è ciclicamente lamentata l'insufficienza delle norme incriminatrici poste a presidio della segretezza o della riservatezza del contenuto delle intercettazioni, anche in relazione alla divulgazione di colloqui di cittadini terzi finiti nella rete delle captazioni seppur estranei alle indagini. Alla luce di ciò, il Garante per la protezione dei dati personali aveva manifestato l'esigenza di «una più puntuale selezione del materiale investigativo assicurando, nel doveroso rispetto dei diritti della difesa, che negli atti processuali non siano riportati interi spaccati di vita

[579] D.p.r. 30 settembre 1963, n. 1409, nonché d.lgs. 22 gennaio 2004, n. 42, che fissa in quarant'anni dopo la data di conclusione del processo il termine ordinario di scadenza e in settanta anni se si tratta di dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare.

[580] Ai sensi dell'art. 115 c.p.p., è prevista la responsabilità disciplinare quando il fatto sia commesso da impiegati dello Stato o di altri enti pubblici ovvero da persone esercenti una professione per la quale è richiesta una speciale abilitazione dello Stato.

[581] Si tratta della rivelazione ed utilizzazione di segreti di ufficio e della rivelazione di segreti inerenti ad un procedimento penale.

privata (delle parti ma soprattutto dei terzi), del tutto estranei al tema di prova»[582]. Sul punto, vengono in rilievo almeno due profili inerenti al diritto alla riservatezza dei soggetti coinvolti nelle captazioni: accanto all'interesse alla non divulgazione delle conversazioni irrilevanti ai fini dell'accertamento penale (riservatezza in senso lato)[583], si può distinguere anche un più specifico interesse alla non divulgazione di conversazioni che si riferiscono a dati strettamente personali, come quelli sensibili (riservatezza in senso stretto o *privacy*). Sotto il versante della tutela della riservatezza, bisogna dire che la novella del 2020 ha dato vita ad un articolato normativo che, nel suo complesso, si lascia apprezzare: in particolare, per quanto concerne il diritto a informare e a essere informati, la chiusura netta contenuta nel nuovo c. 2-bis dell'art. 114 c.p.p. «segna un'inversione di rotta – soprattutto per quel che riguarda l'ostensione del materiale intercettato richiamato nell'ordinanza cautelare – rispetto al 2017»[584].

Qualche considerazione ulteriore merita il profilo concernente il diritto di accesso del giornalista agli atti non segreti. Al riguardo, infatti, accanto agli illustrati e controversi confini che il legislatore pone in capo ad esso, rileva l'ineffettività dell'art. 116 c.p.p., ai sensi del quale «chiunque vi abbia interesse può ottenere il rilascio a proprie spese di copie, estratti o certificati di singoli atti», che dovrebbe garantire una condizione di parità in ordine all'accesso agli atti non segreti. Questa circostanza ha ridotto i cronisti giudiziari a «nobili accattoni»[585], incoraggiando «un malsano reticolo tra operatori della giustizia e operatori dell'informazione»[586]. Così, «i giornalisti giudiziari da "cani da guardia della democrazia", secondo una felice espressione della Corte di Strasburgo, si sono trasformati in "cani da salotto delle Procure", in attesa del boccone informativo[587]». Il problema è stato attenzionato dal Consiglio Superiore della Magistratura, che, predisponendo *Linee-guida per l'organizzazione degli uffici giudiziari ai fini di una corretta comunicazione istituzionale*

[582] V., al riguardo, l'*Audizione alla Commissione Giustizia del Senato del garante per la protezione dei dati personali*, 4 febbraio 2020, 3.

[583] Cfr., per tutti, P. FERRUA, Privacy *e riservatezza nella riforma delle intercettazioni*, in ID., *Studi sul processo penale*, vol. III, Torino, 1997, p. 119.

[584] M. GIALUZ, *Segreto a tutela della riservatezza e divieto speciale di pubblicazione delle intercettazioni*, in ID. (a cura di), *Le nuove intercettazioni*, cit., p. 72.

[585] L'espressione stigmatizzante è di L. FERRARELLA, *Più trasparenza alle notizie per difendere sul serio i segreti*, in *Deontologia giudiziaria*, Napoli, 2006, p. 255.

[586] G. GIOSTRA, *Prima lezione sulla giustizia penale*, cit., p. 173.

[587] *Ibidem*, p. 173-174.

(11 luglio 2018), ha avvertito la necessità di garantire, in conseguenza del carattere democratico dell'ordinamento, la più ampia trasparenza dell'attività degli uffici, nella prospettiva di incrementare la fiducia dell'opinione pubblica nella magistratura e, al contempo, la sua indipendenza. Certo è che, se non si può guardare all'istituzione degli uffici stampa presso le procure della Repubblica come una panacea, sarà piuttosto il riconoscimento in forma piena del diritto di accedere alle notizie non segrete a tutti i giornalisti su un piano di parità, così come auspicato dalla Raccomandazione (2003)13 del Consiglio d'Europa, a restituire dignità al giornalismo giudiziario del nostro Paese.

8. *Un po' di numeri*[588]

Da ultimo, vista la riscoperta dell'importanza dell'elemento statistico[589], si ritiene opportuno dare conto dei *trend* più significativi che hanno riguardato, nell'ultimo ventennio, lo strumento delle intercettazioni. Sul piano metodologico, l'analisi dei dati e delle statistiche giudiziarie costituisce, in effetti, un presupposto indefettibile per una ricerca che aspiri ad essere anche propositiva e che dunque intenda farsi carico, operata la diagnosi delle disfunzioni, delle esigenze di riforma all'interno del campo di indagine in esame.

A partire dal 2003, la Direzione Generale di Statistica presso il Ministero della Giustizia ha avviato un monitoraggio statistico concernente le intercettazioni, mezzo di ricerca della prova divenuto, per le ragioni che si sono esaminate, sempre più decisivo ai fini dell'accertamento penale. Quella che si va ora a proporre è, quindi, una panoramica ragionata dei risultati prodotti da questo monitoraggio, condotto sulla base di tre variabili principali:

1) numero di "bersagli" sottoposti ad intercettazione;
2) importo liquidato dagli uffici giudiziari al netto dell'IVA;
3) durata media delle intercettazioni.

[588] I dati che si vanno ora ad illustrare sono tratti dal rapporto statistico dell'anno 2020 del Ministero della Giustizia-Direzione generale di statistica e analisi organizzativa, reperibile all'indirizzo *web* https://webstat.giustizia.it/Analisi%20e%20ricerche/Rapporto%20su%20Intercettazioni%20fino%20al%202020.pdf.

[589] Si veda, su tutti, M. GIALUZ – J. DELLA TORRE, *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022.

Osservando il *trend* storico dei "bersagli", emerge come tra il 2003 e il 2020, il numero di questi sia aumentato del 37%, con un tasso medio annuo del 1,9%. In particolare, si è registrata una forte crescita nel corso dei primi sei anni, mentre, a partire dal 2013, si è assistito ad una flessione della curva, che nel 2020, a seguito dell'emergenza pandemica, ha raggiunto un valore inferiore a quello del 2006. Quanto alla tipologia dei "bersagli", mentre si è riscontrata una riduzione con riguardo a quelli telefonici (83.454 nel 2020) e ambientali (15.427 nel 2020), sono invece aumentate le altre tipologie di intercettazione, come quelle informatiche e telematiche (7.632 nel 2020). Questo dato conferma la crescente importanza assunta dai c.d. mezzi atipici di ricerca della prova, che giocano ormai nel procedimento penale un ruolo cruciale, spodestando i tradizionali strumenti investigativi. Ad onta di ciò, nel 2020 la distribuzione percentuale dei "bersagli" per tipologia di intercettazione mostra ancora una netta prevalenza di quelle telefoniche (78%) rispetto alle ambientali (15%) e alle telematiche (7%). Se si guarda alla tipologia di ufficio, poi, emerge che la quasi totalità delle intercettazioni viene disposta dalla Procura ordinaria, con più di un terzo dei "bersagli" intercettato dalle DDA (38%) e il resto dalle sezioni ordinarie; risulta invece marginale, per quanto non trascurabile, il dato relativo alle intercettazioni disposte dalle sezioni antiterrorismo. Considerando, invece, l'area geografica, questi sono i numeri totali di "bersagli" relativi all'anno 2020: 17.637 nel nord-ovest, 9.499 nel nord-est, 19.742 nel centro, 37.592 nel sud e 22.043 nelle isole. In percentuale, la distribuzione territoriale dei "bersagli" intercettati mostra che il 56% dei bersagli viene disposto nel sud (35,3%) e nelle isole (20,7%), mentre da un'analisi della tipologia si può notare che in tali aree geografiche l'uso delle intercettazioni telefoniche è più contenuto rispetto al centro-nord. Guardando ai "bersagli" per distretto, occupa la vetta della classifica quello di Napoli, che registra per l'anno 2020 un numero pari a 14.587, seguito dal distretto di Roma, che arriva a 12.070 nello stesso anno. Il dato più rilevante, però, è che i primi 6 distretti in graduatoria (nell'ordine, Napoli, Roma, Palermo, Catania, Milano, Torino, Reggio Calabria) intercettano da soli oltre il 50% dei "bersagli" totali sul territorio nazionale.

Veniamo al *trend* dei costi, in discesa dal 2009. Tra il 2015 e il 2016 si registra una riduzione, seguita da un lieve incremento, imputabile probabilmente all'introduzione dell'obbligo, a decorrere dal giugno 2014, della fatturazione elettronica, che potrebbe aver causato un blocco temporaneo delle liquidazioni, poi parzialmente recuperato. È invece al 2020, anno dell'emergenza pandemica, che si riferisce l'importo più basso. Quanto alla tipologia dei costi, nell'anno 2020 il 65% è stato liquidato per il noleggio degli apparati,

l'8% per il traffico telefonico, il 21% per la videosorveglianza e la localizzazione GPS, il 6% per le intercettazioni informatiche, mentre assai marginale (0,4%) è l'importo per l'acquisizione dei tabulati, voce ad esaurimento residuale di vecchie pendenze in quanto ora gratuita. Considerando i costi per area geografica, si osserva come la spesa per le intercettazioni si concentri soprattutto al sud e nelle isole (64% dell'importo nazionale): in particolare, sempre con riferimento all'anno 2020, l'importo liquidato per intercettazioni al netto dell'IVA è stato di € 19.281,061 nel nord-ovest, € 15.373,618 nel nord-est, € 18.133,214 nel centro, € 51.063,117 nel sud e € 41.471,742 nelle isole. Guardando invece ai costi per distretto, occupano le prime sei posizioni in graduatoria quelli di Palermo, Napoli, Catanzaro, Milano, Roma e Reggio Calabria: questi sei distretti liquidano da soli oltre la metà (54%) dell'importo nazionale. Il costo di un "bersaglio" viene calcolato come rapporto tra gli importi liquidati nell'anno e i bersagli dello stesso anno, ipotizzando che la liquidazione avvenga mediamente nello stesso anno di intercettazione: il *trend* è discendente fino al 2015, mentre nei cinque anni successivi si registra una lieve crescita. Per quanto riguarda il costo unitario per distretto, ci si muove, con riguardo all'anno 2020, da un minimo di € 771 in quello di Roma ad un massimo di € 3.005 in quello di Palermo. È appena il caso di sottolineare che il costo unitario, calcolato come rapporto tra gli importi liquidati in un anno e i "bersagli" dello stesso anno, è influenzato dalla modalità di intercettazione utilizzata, atteso che le diverse tipologie di "bersaglio" presentano costi differenti. A questo proposito, le intercettazioni ambientali risultano le più costose (€ 2.198,58 nel 2020), seguite dalle informatiche (€ 1.190,71 nel 2020) e, infine, da quelle telefoniche (€ 853,31 nel 2020).

Dall'analisi dei dati illustrati è possibile trarre alcune conclusioni. Nel periodo compreso tra il 2003 e il 2020 il numero totale dei "bersagli" intercettati è aumentato del 37%, con un tasso di crescita medio annuo pari al 1,9%: se il *trend* è stato positivo per i primi sei anni, si è registrata, a decorrere dal 2013, una flessione del numero dei "bersagli", che, in occasione dell'emergenza pandemica, ha toccato un valore inferiore a quello del 2006. La riduzione del 2020 è dovuta ai "bersagli" telefonici e ambientali, mentre quelli relativi ad altre tipologie di intercettazione, sempre in crescita, raggiungono l'apice proprio nel 2020. Sul piano dei costi, un *trend* discendente si è avuto a partire dal 2009 con un punto di minimo nel 2015, forse dovuto al blocco delle liquidazioni avvenuto in seguito all'introduzione dell'obbligo della fatturazione elettronica; l'importo più basso è riferito al 2020, anno dell'emergenza pandemica. L'analisi tipologica delle intercettazioni evidenzia la netta prevalenza di quelle telefoniche (78%), forse anche in quanto meno costose, sebbene sia

invalsa, negli ultimi anni, la tendenza ad un maggiore impiego di quelle telematiche. L'analisi per area geografica mostra che il 56% dei "bersagli" viene disposto nel sud e nelle isole, dove è concentrata la maggior parte della spesa sostenuta per intercettazioni (64% dell'importo nazionale). Inoltre, nel sud e nelle isole si fa un uso maggiore delle intercettazioni ambientali e telematiche rispetto al centro-nord: il più frequente ricorso a questo genere di intercettazioni, più costose delle telefoniche, può anche spiegare il più elevato costo unitario per bersagli osservato in alcuni distretti.

BIBLIOGRAFIA

AA. VV., *Electronic evidence*, a cura di MASON, London, LexisNexis, Butterworths, 2007.

AGOSTINO L. – PERALDO M. (a cura di), *Le intercettazioni con captatore informatico: ambito di applicazione e garanzie procedurali*, in M. GIALUZ (a cura di), *Le nuove intercettazioni*, in *Diritto di Internet*, 2020, p. 74 ss.

ALBANESE D., *La Cassazione ritorna sui limiti all'utilizzabilità degli esiti delle intercettazioni nell'ambito del "medesimo procedimento": una parola definitiva, ma non per il futuro* in *Sistema Penale*, 2021.

ALESCI T., *Il corpo umano fonte di prova*, Milano, 2017.

ALONZI F., *Le attività del giudice nelle indagini preliminari. Tra giurisdizione e controllo giudiziale*, Padova, 2011.

ALONZI F., *L'*escalation *dei mezzi di intrusione nella sfera privata,* in *Rev Bras. de Direito Processual Penal*, 2019, p. 1425 ss.

ALVINO F., *La circolare delle intercettazioni e la riformulazione dell'art. 270 c.p.p.: l'incerto pendolarismo tra regola ed eccezione,* in *Sistema penale*, 5/2020, 2020.

AMATO G., *Individuo e autorità nella disciplina della libertà personale*, Milano, 1967.

AMATO G., *Le riprese video di comportamenti non comunicativi effettuate in luoghi privati sono illegittime*, in *Il quotidiano giuridico* del 21 settembre 2006.

AMATO G., *Manuale di diritto pubblico*, Bologna, V ed., 1984.

AMATO G., *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un "captatore informatico"*, in *Guida dir*., 2016, n. 34-35, p. 79.

ANDOLINA E., *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Padova, 2018.

APRATI R., *La delega della riforma Orlando in tema di intercettazioni*, in *Il libro dell'anno del diritto 2018*, all'indirizzo http://www.treccani.it/enciclopedia/la-delega-della-riforma-orlando-in-tema-di-intercettazioni_%28Il-Libro-dell%27anno-delDiritto%29/.

APRILE E., *Intercettazioni di comunicazioni*, in A. SCALFATI, (a cura di), *Trattato di procedura penale*, Vol. II, Tomo I, Torino, 2009, p. 512 ss.

APRILE E., *Per la Consulta resta illegittima l'acquisizione del contenuto della corrispondenza epistolare dei detenuti effettuata senza le formalità dell'art. 18-ter ord. penit.*, in *Cass. pen.*, 2017, p. 1877 ss.

APRILE E. – SPEZIA F., *Le intercettazioni telefoniche ed ambientali: innovazioni tecnologiche e nuove questioni giuridiche*, Milano, 2004.

ASCARELLI T., *Processo e democrazia*, in *Riv. trim. dir. proc.*, 1958, p .858.

ATERNO S., *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ss.

ATERNO S – MATTIUCCI M., *Cloud Forensics e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen*., 2013, p. 865.

AULETTA T. A., *Riservatezza e tutela della personalità*, Milano, 1978.

BALDASSARRE A., *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974.

BALDUCCI P., *Le garanzie nelle intercettazioni tra Costituzione e legge ordinaria*, Milano, 2002.

BALSAMO A., *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen*., 2015, p. 2274 e nt. 3.

BARBERA A., *I principi costituzionali della libertà personale*, Milano, 1971.

BARILE P., *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984.

BAUMANN Z. – LYON D., *Sesto potere. La sorveglianza nella modernità liquida*, Bari, 2015.

BELTRANI S., *Le videoriprese? Sono una prova atipica. Ma le Sezioni unite non sciolgono il nodo*, in *Dir. & Giust.*, 2006, n. 34, p. 40.

BENE T., *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali*, in A. SCALFATI (a cura di), *Le indagini atipiche*, Torino, 2019, p. 443 ss.

BENE T. (a cura di), *L'intercettazione di comunicazioni*, Bari, 2018.

BENE T., *La legge delega per la riforma delle intercettazioni*, in A. SCALFATI (a cura di), *La riforma della giustizia penale*, Torino, 2017, p. 289 ss.

BENTHAM J., *Panopticon – Ovvero la casa di ispezione*, Venezia, III ed., 2002.

BLASBERG S., *Law and technology of security measures in the wake of terrorism*, in 8, *Boston University Journal Science & Technology Law*, 721 (2002).

BLEFARI C. R., *La Corte di Cassazione si pronuncia sulla questione della mancata sottoscrizione del verbale delle operazioni relative ad intercettazioni*, in *Proc. pen. giust*., 2018, p. 341 ss.

BLITZ J., *Video surveillance and the constitutional public space: fitting the fourth Amendment to a world that tracks image and identity*, in 82, *Texas Law Review*, 1349 (2004).

BOCCHESE D., *Il diritto alla privacy nell'era dei droni*, in *El transporte como motor del desarrollo socioeconomico*, di M. V. PETIT LAVALL – A. PUETZ (a cura di), *Instituto Universitario de Derecho del Transporte (IDT)*, 2018, p. 395 ss.

BONETTI M., *Riservatezza e processo penale*, Milano, 2003.

BONINI V., *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Proc. pen. giust.*, 2019, p. 338 ss.

BONTEMPELLI M., *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont.*, 2018, p. 5 ss.

BORRELLI G., *Interpretazione delle norme ed evoluzione degli strumenti tecnici di indagine: il rischio del "travisamento tecnologico"*, in *Cass. pen.*, 2002, p. 944 ss.

BORRELLI G., *Riprese filmate nel bagno di un pubblico esercizio e garanzie costituzionali*, in *Cass. pen.*, 2001, p. 2439 ss.

BOTTI C., *Ma il sensore posto nell'autoveicolo potrebbe violare il domicilio*, in *Dir. & Giust.*, 2002, n. 22, p. 16.

BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen*., 1967, p. 112.

BRICCHETTI R., *Spetta al legislatore regolamentare le riprese di tipo non comunicativo*, in *Guida al diritto*, 2002, n. 20, p. 73.

BROGAN J., *Facing the music: the dubious constitutionality of facial recognition technology*, in 25, *Hasting Comm. & Ent. Law Journal*, 65 (2002-2003).

BRONZO P., *L'impiego del* trojan horse *informatico nelle indagini penali*, in *Riv. it. scienze giur*., 2017, f. 8, p. 3.

BUZZELLI S., *Le nuove intercettazioni tra selettività arbitraria e ridimensionamento delle garanzie difensive*, in *La rivista di diritto dei media*, 2018, p. 214 ss.

CAJANI F., *L'odissea del captatore informatico*, in *Cass. pen.*, 2016, p. 4139 ss.

CALDIROLA D., *Il diritto alla riservatezza*, Padova, 2006.

CAMALDO L., *Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico,* in *Dir. pen. cont.*, 24 settembre 2019, p. 1 ss.

CAMON A., *Captazione di immagini*, in *dir. proc. pen.*, 2013, p. 142.

CAMON A., *Cavalli di Troia in Cassazione,* in *Arch. nuova proc. pen.*, 2017, p. 91 ss.

CAMON A, *Forme, destinazione e regime della documentazione,* in G. GIOSTRA – R. ORLANDI (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, p. 79.

CAMON A., *Il cacciatore di IMSI*, in *Arch. pen.*, 2020, n. 1, p. 177 ss.

CAMON A., *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, p. 594.

CAMON A., *Le intercettazioni nel processo penale*, Bologna, 1996.

CAMON A., *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, p. 1192 ss.

CAMON A., *Le sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e dubbi nuovi*, in *Riv. it. dir. proc. pen.*, 2006, p. 1550.

CAMON A., *Primi appunti sul nuovo procedimento d'acquisizione dei risultati delle intercettazioni,* in *Arch. pen.*, 2018, p. 449 ss.

CAMON A., *Sfondi*, in AA. VV., *Fondamenti di procedura penale*, Padova, 2021, p. 7 ss.

CAMON A., sub *art. 270 c.p.p.*, in CONSO G. – ILLUMINATI G. (cur.), *Commentario breve al codice di procedura penale,* II ed., Padova, 2015, p. 1052 ss.

CANTONE R. – D'ANGELO L. A., *Una nuova ipotesi di intercettazione preventiva*, in A. A. DALIA (a cura di), *Le nuove norme di contrasto al terrorismo*, 2006, p. 54.

CANZIO G., *Prova scientifica, ragionamento probatorio e libero convincimento nel processo penale,* in *Dir. pen. proc.,* 2003, p. 1193 ss.

CANZIO G., *Prova scientifica, ricerca della «verità» e decisione giudiziaria nel processo penale,* in *Decisione giudiziaria e verità scientifica*, Quaderni della rivista trimestrale di diritto e procedura civile, n. 3, Milano, 2005, p. 55 ss.

CAPOGRASSI G., *Giudizio, processo, scienza, verità*, Milano, 1959.

CAPRIOLI F., *Colloqui riservati e prova penale*, Torino, 2000.

CAPRIOLI F., *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. bras. dir. proc. pen.*, vol. 3, 2/2017, p. 491.

CAPRIOLI F., *Intercettazioni illecite, intercettazioni illegali, intercettazioni illegittime*, in AA. VV., *Le intercettazioni un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti: atti del Convegno, Milano, 5-7 ottobre 2007*, Milano, 2009, p. 139 ss.

CAPRIOLI F., *La procedura di filtro delle comunicazioni rilevanti nella legge di riforma della disciplina delle intercettazioni*, in *Cass. pen.*, 2020, p. 1384 ss.

CAPRIOLI F., *Riprese visive nel domicilio e intercettazione "per immagini"*, in *Giur. cost.*, 2002, p. 2187, nt. 63.

CARNEVALE S., *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in D. NEGRI, *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, 2007, p. 5.

CARRARA F., *Il diritto e la procedura penale*, pubblicato in *Opuscoli di diritto criminale*, III ed., Prato, 1889, p. 19.

CASEY E., *Digital Evidence and Computer Crime. Forensic science, computer and the Internet*, Second Edition, Elsevier, 2004.

CESARI C., *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, vol. 5, n. 3, 2019, p. 1174 ss.

CHENG E., KREIMER S., SIMMONS R., LEDERER F., *Symposium: the powers and pitfall of technology*, in 60, N.Y.U. *Annual Survey of American Law*, 675 (2002).

CIAMPI A., *L'assunzione di prove all'estero in materia penale,* Padova, 2003.

CIAMPI S., *La riforma delle intercettazioni e le sue ricadute sulla conclusione delle indagini preliminari*, in *Arch. pen. 2020*, n. 2, p. 3.

CIAMPI S., *L'archivio delle intercettazioni tra presidio della riservatezza, tutela del diritto di difesa e svolta digitale*, in M. GIALUZ (a cura di), *Le nuove intercettazioni*, in *Diritto di Internet*, 2020, p. 21 ss.

CISTERNA A., *Intercettazioni: i rischi di una delega troppo generica*, in *Guida dir.*, 2017, 32, p. 65.

CISTERNA A., *Spazio ed intercettazioni, una* liaison *tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, in *Arch. pen.*, 2016, p. 331.

CLANCY T., *Coping with technological change: Kyllo and the proper analytical structure to measure the scope of Fourth Amendment analysis and individual rights*, in 72, *Miss. Law Journal*, 1 (2002-2003).

CLANCY T., CLOUD A. M., MACLIN T., SLANSKY D., SLOBOGIN C., TOMKOVICZ J., URBONYA K., *Symposium: The effect of technology on Fourth Amendment analysis and individual rights*, in 72, *Miss. Law Journal*, 1-564 (2002-2003).

CONTI C., *Accertamento del fatto e inutilizzabilità del processo penale*, Padova, 2007.

CONTI C., *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. Pen*., 2011, p. 3638 ss.

CONTI C., *La riservatezza delle intercettazioni nella "delega Orlando"*, in *Dir. pen. cont.*, 2017, p. 78 ss.

CONTI C., *Le nuove norme sulla riservatezza delle intercettazioni: anatomia di una riforma discussa*, in *Giur. it*., 2018, p. 1754 ss.

CONTI C., *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati"*, in *Dir. pen. proc.*, 2006, p. 1354.

CONTI C., *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. proc.*, 2018, p. 1210.

CONTI C., *Sicurezza e riservatezza*, in *Dir. pen. proc.*, 2019, p. 1585.

CORBETTA, *Le nuove misure per contrastare le intercettazioni illegali: profili di diritto penale e processuale*, in *Il quotidiano Giuridico*, n. 26 del 2006.

CORDERO F., *Diatribe sul processo accusatorio*, in ID, *Ideologie del processo penale*, Milano, 1966, p. 220.

CORDERO F., *Gli osservanti. Fenomenologia delle norme*, Milano, 1967.

CORDERO F., *Privacy viziosa*, in ID., *L'opera italiana da due soldi*, Torino, 2012, p. 44.

CORDERO F., *Procedura penale*, IX ed., Milano, 2012.

CORDERO F., *Prove illecite*, in *Tre studi sulle prove penali*, Milano, 1963.

CORDERO F., sub *art. 234*, in *Codice di procedura penale commentato*, II ed., Torino, 1992.

COSTANZO P., *Il ruolo del fattore tecnologico e le trasformazioni del costituzionalismo*, in *Associazione italiana dei costituzionalisti. Costituzionalismo e globalizzazione. Atti del XXVII Convegno annuale. Salerno, 22-24 novembre 2012*, Napoli, 2014, p. 43.

COSTANZO P., *L'impatto della tecnologia sui diritti fondamentali*, in P. COSTANZO – T. E. FROSINI – O. POLLICINO – E. APA – M. BASSINI (a cura di), *Diritti e libertà in internet*, Milano, 2017, p. 11.

CURTOTTI D. – NOCERINO W., *Le intercettazioni tra presenti con captatore informatico*, in G. M. BACCARI– C. BONZANO – K. LA REGINA – E. MANCUSO (a cura di), *Le recenti riforme in materia penale: dai decreti di depenalizzazione (d. lgs. n. 7 e n. 8/2016) alla «legge Orlando» (l. n. 103/2017) e relativi decreti attuativi (3 ottobre 2017)*, Padova, 2017, p. 557 ss.

DAMASKA M., *Il diritto delle prove alla deriva*, Bologna, 2003.

DANIELE M., *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Riv. dir. proc.*, 2011, p. 1288 ss.

DANIELE M., *La sfera d'uso delle prove raccolte*, in M. DANIELE M.- R. E. KOSTORIS (a cura di), *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017*, Torino, 2018, p. 184 ss.

DAVOLA A., *L'acquisizione di dati da parte dei privati nelle operazioni con SAPR*, in E. PALMERINI – M. A. BIASIOTTI – G. F. AIELLO (a cura di), *Diritto dei droni. Regole, questioni e prassi*, Milano, 2018, p. 137 ss.

DE AMICIS G., *Dalle rogatorie all'ordine europeo di indagine: verso un nuovo diritto della cooperazione giudiziaria penale*, in *Cass. pen.*, 2018, p. 37.

DE AMICIS G, *Organismi europei di cooperazione e coordinamento investigativo*, in *Cass. pen.*, 2017, p. 120 ss.

DE FALCO G., *Sulle videoriprese più ombre che luci. Non basta il* dictum *delle Sezioni Unite*, in *Dir. & Giust.*, 2006, n. 45, p. 70.

DELLA TORRE J., *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in *Sistema Penale*, 2021.

DELLA TORRE J., *La nuova disciplina della circolazione del captato: un nodo arduo da sciogliere*, in M. GIALUZ (a cura di), *Le nuove intercettazioni*, in *Diritto di Internet*, 2020, p. 90 ss.

DELLA TORRE J., *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice (ma raccoglie le critiche del garante privacy d'oltremanica)*, in *Sistema Penale*, 2020.

DELLA TORRE J., *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, in G. DI PAOLO – L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale*, Trento, 2022, p. 7 ss.

DI BITONTO M. L., *Le riprese video domiciliari al vaglio delle Sezioni unite*, in *Cass. pen*., 2006, p. 3950.

DI BITONTO M. L., *Lungo la strada per la riforma della disciplina delle intercettazioni*, in *Cass. pen*., 2009, p. 18

DI MARTINO C. - PROCACCIANTI T., *Le intercettazioni telefoniche*, Padova, 2001.

DI PAOLO G., *Tecnologie del controllo e prova penale*, Padova, 2008.

DITZION R., *Electronic surveillance in the Internet age: the strange case of pen registers*, in 41, *American Crim. Law Review* (2004), 1321.

DOMENICALI C., *Tutela della persona negli spazi virtuali: la strada del "domicilio informatico"*, in *federalismi.it*, n. 7/2018, p. 13.

DOMINIONI O., *In tema di nuova prova scientifica*, in *Dir. pen. proc.*, 2001, p. 1061.

DOMINIONI O., *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005.

ETZIONI A., *Implications of selected new technologies for individual rights and public safety*, in 15, *Harvard Journal of Law and Technology*, 261 e 274 (2001-2002).

FABIANO N., *Gdpr e privacy, consapevolezza e opportunità*, Firenze, 2020.

FANUELE C., *La localizzazione satellitare nelle investigazioni penali*, Milano, 2019.

FANCHIOTTI V., *Il cyberorecchio di Dionisio*, in *Cass. pen*., 2015, p. 1646.

FEBBRARO M. F., *La procedura di "stralcio" nell'ambito delle intercettazioni di conversazioni e comunicazioni*, in *La giustizia penale differenziata. Gli accertamenti complementari*, coord. da MONTAGNA M., Torino, 2011.

FERRAJOLI L., *Diritto e ragione. Teoria del garantismo penale*, III ed., Bari, 1996.

FERRARELLA L., *Più trasparenza alle notizie per difendere sul serio i segreti*, in *Deontologia giudiziaria*, Napoli, 2006, p. 255.

FERRUA P., *Il contraddittorio tra declino della legge e tirannia del diritto vivente*, in D. NEGRI – R. ORLANDI (a cura di), *Le erosioni silenziose del contraddittorio*, Torino, 2017, p. 15 ss.

FERRUA P., Privacy *e riservatezza nella riforma delle intercettazioni*, in ID., *Studi sul processo penale*, vol. III, Torino, 1997, p. 119.

FERRUA P., *Un giardino proibito per il legislatore: la valutazione delle prove*, in *Quest. giust.*, 1998, p. 587 ss.

FILIPPI L., *Attuazione della delega sulle intercettazioni. Un'altra occasione mancata*, in *il Penalista*, 2018.

FILIPPI L., *D.L. intercettazioni: abrogata la riforma Orlando, si torna all'antico*, in *Quotidiano giuridico*, 10 gennaio 2020, p. 8.

FILIPPI L., *Intercettazioni: finalmente una legge! (ma in vigore a settembre)*, in *Pen. dir. proc.*, 2020, p. 23 ss.

FILIPPI L., *Intercettazioni:* habemus legem*!*, in *Dir. pen. proc*., 2020, p. 457.

FILIPPI L., *Intercettazioni: una riforma complicata e inutile*, in *Dir. pen. proc*., 2018, p. 305.

FILIPPI L., *L'intercettazione di comunicazioni*, Milano, 1997.

FILIPPI L., *L'home watching: documento, prova atipica o prova incostituzionale?*, in *Dir. pen. proc.*, 2001, p. 92.

FILIPPI L., *La delega in materia di uso del captatore informatico*, in G. SPANGHER (a cura di), *La riforma Orlando*, Pisa, 2017, p. 151 ss.

FILIPPI L., *La legge delega sulle intercettazioni*, in G. M. BACCARI – C. BONZANO – K. LA REGINA – E. MANCUSO (a cura di), *Le recenti riforme in materia penale: dai decreti di depenalizzazione (d. lgs. n. 7 e n. 8/2016) alla «legge Orlando» (l. n. 103/2017) e relativi decreti attuativi (3 ottobre 2017)*, Padova, 2017.

FILIPPI L., *La Corte di Lussemburgo ribadisce lo stop ai tabulati: una fine annunciata*, in www.penaledp.it, 14 aprile 2022.

FILIPPI L., *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in www.penaledp.it, 1 ottobre 2021, p. 9 ss.

FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. ec*., 3/2009, p. 705.

FLOR R., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo* jus excludendi alios, in *Dir. pen. proc*., 2005, p. 81.

FLORIDI L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

FORMICI G., *Tutela della riservatezza delle comunicazioni elettroniche*, in *Osservatorio costituzionale*, 2018, p. 453 ss.

FOUCAULT M., *Sorvegliare e punire*, Torino, 2005.

FROSINI, *Le prove statistiche nel processo civile e penale*, Milano, 2002.

GAITO A., *I nuovi orizzonti*, in ID. (a cura di), *Riservatezza e intercettazioni tra norma e prassi*, Roma, 2011, p. 213 ss.

GAITO A., *In tema di intercettazioni delle conversazioni in abitazioni private*, in *Giur. it.*, II, 1991, p. 466.

GALANTINI N., *L'inutilizzabilità della prova nel processo penale*, Padova, 1992.

GALGANI B., Habeas data *e garanzie fondamentali*, in *Arch. pen*. web, 2019, p. 1.

GHIRARDINI A.-FAGGIOLI G., *Computer forensics*, Milano, 2007.

GIALUZ M., *Intercettazioni di colloqui riservati e libertà funzionali del parlamentare: qualche riflessione sulla portata della prerogativa dell'art. 68, comma 3, Cost*., in *Cass. pen*., 2004, p. 3682 ss.

GIALUZ M., *La cooperazione informativa quale motore del sistema europeo di sicurezza*, in *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, p. 15 ss.

GIALUZ M., *Premessa*, in ID. (a cura di), *Le nuove intercettazioni*, in *Diritto di Internet*, 2020, p. 1 ss.

GIALUZ M., *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei* risk assessment tools *tra Stati Uniti ed Europa*, in *Dir. Pen. Cont*., 2019, p. 1 ss.

GIALUZ M., *Segreto a tutela della riservatezza e divieto speciale di pubblicazione delle intercettazioni*, in ID. (a cura di), *Le nuove intercettazioni*, in *Diritto di Internet*, 2020, p. 61 ss.

GIALUZ M.– DELLA TORRE J., *Giustizia per nessuno. L'inefficienza del sistema penale italiano tra crisi cronica e riforma Cartabia*, Torino, 2022.

GIALUZ M.– DELLA TORRE J., *Lotta alla criminalità nel* cyberspazio*: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont.*, 2018, p. 281.

GIORDANO L., *La delega per la riforma delle intercettazioni*, in A. MARANDOLA – T. BENE (a cura di), *La riforma della giustizia penale*, Milano, 2017.

GIORDANO L., *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sistema penale*, 4/2020, p. 112.

GIOSTRA G., *I mali della libertà di stampa si curano solo con più libertà*, in AA. VV., *Ddl Alfano: se lo conosci lo eviti*, Roma, 2009, p. 102.

GIOSTRA G., *Il segreto estende i suoi confini e la sua durata*, in GIOSTRA G. – ORLANDI R. (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, p. 115 ss.

GIOSTRA G., *Prima lezione sulla giustizia penale*, Bari, 2020.

GIOSTRA G., *Processo penale e informazione*, Milano, 1998.

GIOSTRA G., *Su intercettazioni e segreto una disciplina impraticabile*, in *Il Sole 24 Ore*, 20 dicembre 2017, p. 33.

GIOSTRA G. – ORLANDI R. (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018.

GITTARDI C., *La riforma delle intercettazioni, dopo due anni, alla stretta finale con molte novità*, in *Giustizia Insieme*, 2020.

GIUNCHEDI F., *Appunti su alcune criticità della nuova disciplina delle intercettazioni*, in *Arch. pen.*, 2018, p. 513 ss.

GRAY D., *The Fourth Amendment in an Age of Surveillance*, Cambridge University Press, 2017.

GRAZIANI F., *L'acquisizione della prova digitale all'estero: verso un secondo Protocollo addizionale alla Convenzione di Budapest sul cybercrime*, in *Rev. Bras. de Direito Processual Penal*, 2019, p. 55 ss.

GREVI V., *Anomalie e paradossi in tema di intercettazioni «indirette» relative a membri del parlamento*, in *Cass. Pen.*, 2007, p. 3159 ss.

GREVI V., *La nuova disciplina delle intercettazioni telefoniche*, Milano, 1979.

GREVI V., *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost.*, 1974, p. 317.

GREVI V., *Prove*, in G. CONSO – V. GREVI, *Profili del nuovo Codice di procedura penale*, Padova, 1990, p. 156.

ILLUMINATI G., *Costituzione e processo penale*, in *Giur. it.*, 2008, p. 521.

ILLUMINATI G., *La disciplina processuale delle intercettazioni*, Milano, 1983.

ILLUMINATI G., *La tutela della segretezza delle comunicazioni tra vecchio e nuovo codice*, in *Processo penale e valori costituzionali nell'insegnamento di Vittorio Grevi*, Padova, 2013, p. 107.

ILLUMINATI G.– GIULIANI L., *Commentario breve al codice di procedura penale. Complemento giurisprudenziale*, III ed., Milano, 2020.

INGENITO M. – INNOCENTI D., *La videoregistrazione domiciliare di comportamenti comunicativi nella previsione e non comunicativi nei risultati*, in *Dir. pen. proc.*, 2013, p. 1337.

IOVENE F., *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont.*, n. 3-4/2014, 2014, p. 330.

IOVENE F., *Nuova decisione della Corte di giustizia in materia di tabulati: quali conseguenze per l'ordinamento nazionale?*, in *Cass. pen.*, 2022, p. 2363 ss.

IOVENE F., *Pedinamento satellitare e diritti fondamentali della persona*, in *Cass. pen.*, 2012, p. 3556.

LAFAVE W., *Search and seizure: A treatise on the Fourth Amendment*, IV ed., vol. I, 2004, p. 729 ss.

LAMON M. – BONAZZI M., *I droni a supporto della pubblica sicurezza*, in *Giureta – Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente*, 2021, p. 187.

LARINNI C., *La (contro)riforma delle intercettazioni*, in *Discrimen*, 2020.

LASAGNI G., *Difendersi dall'intelligenza artificiale o difendersi con l'intelligenza artificiale? Verso un cambio di paradigma*, in G. DI PAOLO – L. PRESSACCO (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, Trento, 2022, p. 64 ss.

LEO G., *Necessario il provvedimento autorizzativo dell'Autorità giudiziaria per il ricorso al c.d. «agente segreto attrezzato per il suono»*, in *Dir. pen. cont.* 1/2012, 2012, p. 163 ss.

LONGO A., *Le garanzie costituzionali delle intercettazioni visive: un'occasione mancata per la corte*, in *Giur. cost.*, 2002, p. 2208 ss.

LUPARIA L., Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Dir. di internet*, 2019, p. 757.

LUPARIA L., *L'inchiesta penale tra echi del passato e risvolti della modernità*, Intervento al convegno *"Inchiesta penale e pregiudizio. Una riflessione interdisciplinare"*, Teramo, 4 maggio 2006.

LUPARIA L., Privacy, *diritti della persona e processo penale*, in *Riv. dir. proc*., 2019, p. 1464 ss.

LUPARIA L.– MARAFIOTI L.– PAOLOZZI G. (a cura di), *Dimensione tecnologica e prova penale*, Torino, 2019.

LUPARIA L.-ZICCARDI G., *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007.

LYON D., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2001.

LYON D., *L'occhio elettronico.* Privacy *e filosofia della sorveglianza*, Milano, 1997.

MALACARNE A., *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, in *Sistema Penale*, 2021.

MALACARNE A. – TESSITORE G., *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di Giustizia: ancora inadeguata la disciplina interna?*, in *Arch. pen*. web, 2022, p. 28 ss.

MANCUSO E., *Le acquisizioni mediante captatore non disciplinate dalla legge*, in GIARDA A. – GIUNTA F. – VARRASO G. (a cura di), *Dai decreti attuativi della riforma "Orlando" alle novelle di fine legislatura*, Padova, 2018.

MANCUSO E., *Le perquisizioni* on-line, in *Jus – Rivista di Scienze Giuridiche*, 2017.

MANGIARACINA A., *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale*, in *Dir. pen. proc*., 2018, n. 2, p. 177.

MARCOLINI S., *Le cosiddette perquisizioni online (o perquisizioni elettroniche)*, in *Cass. pen*., 2010, p. 2855 ss.

MARINELLI C., *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007.

MARINELLI C., *Le videoriprese investigative al vaglio delle Sezioni Unite: i limiti di impiego negli spazi riservati di natura extradomiciliare*, in *Riv. it. dir. proc. pen.*, 2006, p. 1570.

MARINI, *La costituzionalità delle riprese visive nel domicilio: ispezione o libertà "sotto-ordinata"?*, in *Giur. cost.*, 2002, p. 1076.

MAZZA O., *Amorfismo legale e adiaforia costituzionale nella nuova disciplina delle intercettazioni*, in *Proc. pen. giust*., 2018, p. 683 ss.

MAZZA O. (a cura di), *Le nuove intercettazioni*, Torino, 2018.

MELILLO G., *L'acquisizione dei tabulati relativi al traffico telefonico fra limiti normativi ed equivoci giurisprudenziali*, in *Cass. pen.*, 1999, p. 473.

MILLIGAN C., *Facial recognition technology, video surveillance and privacy*, in 9, *Southern California Interdisciplinary Law Journal*, 295 (1999).

MIRAGLIA M., *Garanzie costituzionali nel processo penale statunitense. Tendenze e riflessioni*, Torino, 2008.

MIRAGLIA M., *Il IV emendamento alla rincorsa del progresso: perquisizioni e lotta alla droga nel diritto U.S.A.*, in *Dir. pen. proc.*, 2002, p. 105.

MIRAGLIA M., *Una nuova normalità: metamorfosi della giustizia penale statunitense dopo l'11 settembre*, in *Cass. pen.*, 2005, p. 2823.

NATALI K., *Sezioni unite e "legge Bonafede": nuove regole per l'uso trasversale delle intercettazioni*, in *Cass. pen.*, 2020, p. 18.

NEGRI D., *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen.*, p. 55 ss.

NICOLICCHIA F., *I controlli occulti e continuativi come categoria probatoria*, Milano, 2020.

NOBILI M., *Diritti per la fase che "non conta e non pesa"*, in *Scenari e trasformazioni del processo penale*, Padova, 1998, p. 35 ss.

NOBILI M., *La nuova procedura penale*, Bologna, 1989.

NOCERA A., *Il sindacato giurisdizionale interno in tema di ordine europeo di intercettazione*, in *Dir. pen. cont.*, 2018, p. 164.

NOCERINO W., *Il captatore informatico: un Giano bifronte. Prassi operative vs risvolti giuridici*, in *Cass. pen.*, 2020, p. 824.

NOCERINO W., *La riforma delle intercettazioni preventive d'intelligence*, in *Sistema Penale*, 2023.

NOCERINO W., *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, Milano, 2018.

NOCERINO W., *Prime riflessioni a margine del nuovo decreto legge in materia di intercettazioni*, in *Sist. pen*. 2020/1, p. 64.

NOCERINO W. – ZAMPINI A., *Vecchi e nuovi limiti di utilizzabilità delle intercettazioni nel sistema italiano*, in *Rev. Bras. de Direito Processual Penal*, v. 7, n. 2, 2021, p. 1411.

OLIVIERI R., *I sistemi di geolocalizzazione e l'analisi forense degli smartphone*, in G. COSTABILE – A. ATTANASIO – M. IANULARDO (a cura di), *IISFA Memberbook 2014. Digital forensics. Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER*, Forlì, 2015, p. 141 ss.

ORLANDI R., *Il processo nell'era di* internet, in *Dir. pen. proc.*, 1998, p. 140.

ORLANDI R., *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. pen. proc.*, 2014, p. 1157.

ORLANDI R., *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Arch. pen.* web, 25 luglio 2016.

ORLANDI R., *Rito penale e salvaguardia dei galantuomini*, relazione svolta a Lucca (dicembre 2004-bicentenario della nascita di Francesco Carrara), *Criminalia. Annuario di scienze penalistiche*, 2007, p. 304.

ORLANDI R., *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv.it. dir. proc. pen*., 2018, p. 554.

ORWELL G., *1984*, Milano, 2002.

PANZAVOLTA M., *Ordine di indagine europeo e indagini bancarie: spunti di riflessione sul concetto di caso interno analogo e atto di indagine alternativo*, in A. DIPIETRO – M. CAIANIELLO (a cura di), *Indagini penali e amministrative in materia di frodi IVA e di imposte doganali. L'impatto dell'European Investigation Order sulla cooperazione*, Bari, 2016, p. 380.

PAOLUCCI F., *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *Media Laws – Rivista di diritto dei Media*, 2021, n. 1, p. 208.

PARLATO L., *Le perquisizioni on-line: un tema che resta un tabù*, in G. GIOSTRA – R. ORLANDI (a cura di), *Revisioni normative in Tema di Intercettazioni: Riservatezza, Garanzie Difensive e Nuove Tecnologie Informatiche*, Torino, 2021, p. 344.

PARLATO L., *Problemi insoluti: le perquisizioni* on-line, in G. GIOSTRA – R. ORLANDI (a cura di), *Nuove norme in tema di intercettazioni: tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, p. 289 ss.

PARODI C., *Le intercettazioni: profili operativi e giurisprudenziali*, Torino, 2002.

PERETOLI P., *Controllo satellitare con GPS: pedinamento o intercettazione?*, in *Dir. pen. proc.*, 2003, p. 94.

PESTELLI G., *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161*, in *Sistema penale*, 2020, n. 2.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 80.

PICOTTI L., (voce) *Reati informatici*, in *Enc. giur. Treccani*, agg. VIII, Roma, 2000, p. 20 ss.

PITTIRUTI M., Digital evidence *e procedimento penale*, Torino, 2017.

PRETTI D., *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni*, 2020/2, p. 71 ss., in *Sistema Penale*, 2020.

PRETTI D., *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, in *Dir. pen. cont*., 2018/1, p. 189 ss.

QUATTROCOLO S., *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Espanola de derecho procesal*, 2019, p. 3.

RESTA F., *Dalla conservazione generalizzata a quella mirata e rapida: la Corte di giustizia ridelinea i contorni della* data retention, in www.giustiziainsieme.it, 7 aprile 2022.

RICCI G. F., *Le prove atipiche*, Milano, 1999.

RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014.

RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995.

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997.

RODOTÀ S., *Timori, ipotesi, realtà*, in *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, 1997, p. 27.

RODRIGUEZ LAINZ J. R., *La Evolución de la Jurisprudencia del Tribunal de Justicia de la Unión Europea en Materia de Conservación Indiscriminada de Datos de Comunicaciones Electrónicas en la STJUE del Caso G.D. y Comissioner an Garda Síochána*, in *Diario La Ley*, 19 aprile 2022.

RUGGIERI F., *Divieti probatori e inutilizzabilità della disciplina delle intercettazioni telefoniche*, Milano, 2001.

RUGGIERI F., *La giurisdizione di garanzia nelle indagini preliminari*, Milano, 1996.

RUGGIERI S., *Introduction to the Proposal of a European Investigation Order: Due Process Concerns and Open Issues*, in ID., *Transnational Evidence and Multicultural Inquiries in Europe*, 2014, p. 18 ss.

RUGGIERI S., *Transnational Inquiries and the Protection of Fundamental Rights* in *Comparative Law, in Criminal Proceedings. A study in memory of Vittorio Grevi and Giovanni Tranchina*, 2013, p. 559 ss.

SALTZBURG S., CAPRA D., *American criminal procedure. Cases and commentary*, VII ed., 2004, p. 64 ss.

SANDULLI A., voce *Proporzionalità*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, p. 4644, 4645.

SANTALUCIA G., *Il diritto alla riservatezza nella nuova disciplina delle intercettazioni*, in *Sistema Penale*, 2020, p. 47 ss.

SANTORIELLO C., *Il diritto alla traccia fonica*, in A. GAITO (a cura di), *Riservatezza e intercettazioni tra norma e prassi*, Roma, 2011, p. 225 ss.

SAPONARO L., *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Arch. pen.*, 2022, n. 1, p. 6.

SCALFATI A., *Il fermento pre-investigativo*, in ID. (a cura di), *Pre-investigazioni (Espedienti e mezzi)*, Torino, 2020, p. 1 ss.

SCALFATI A., *Intercettazioni: spirito autoritario, propaganda e norme inutili*, in *Arch. pen*. web, 2020, p. 1.

SCALFATI A. (a cura di), *Le indagini atipiche*, II ed., Torino, 2019.

SCALFATI A. – BRUNO O., *Orientamenti in tema di videoriprese*, in *Proc. pen. giust*., 2011, 1, p. 92.

SCAPARONE M., *In tema di indagini di polizia giudiziaria condotte per mezzo di un agente segreto "attrezzato per il suono"*, in *Giur. cost*., 1988, II, p. 247.

SIMMONS R., *The powers and pitfalls of technology, Technology enhanced surveillance by law enforcement officials*, in 60, *NYU, Ann. Survey of American Law*, 711 (2005).

SIRACUSANO F., *La prova informatica transnazionale: un difficile "connubio" tra innovazione e tradizione*, in *Proc. pen. giust.*, 2017, p. 179.

SLOBOGIN C., *Public privacy: camera surveillance of public spaces and the right to anonimity*, in 72, *Miss. Law Journal*, 213 (2002-2003).

SOLOVE D., *Privacy and power: computer databases and methafhors for information privacy*, in 53, *Stanford Law Review*, 1393-1398 (2001).

SPANGHER G., *Cosa prevede il dl intercettazioni,* trojan *ovunque e articolo 15 della Costituzione calpestato*, in *il Riformista*, 2020.

SPANGHER G., *La controriforma delle intercettazioni telefoniche*, in *Il penalista*, 10 gennaio 2020.

SPANGHER G., *La riforma sconta due mesi di proroga, in vigore dal 1 maggio,* in *Guida dir*., 2020, p. 13, 34.

SPANGHER G., *Spangher: «La Corte di Giustizia della Ue ha sancito la fine del regime dei tabulati»*, in www.ildubbio.it, 20 aprile 2022.

STELLA F., *Giustizia e modernità*, Milano, 2001.

TARUFFO M., *Le prove scientifiche nella recente esperienza statunitense*, in *Riv. trim. dir. proc. civ.*, 1996, p. 219.

TAVASSI L., *Acquisizione di tabulati, tutela della privacy e rispetto del principio di proporzionalità*, in *Arch. pen*. web, 2022.

TETI A., *Big Data. La guida completa per il Data Scientist*, Milano, 2017.

TONINI P., *Manuale di procedura penale*, XXI ed., Milano, 2020.

TONINI P., *Prova scientifica e contraddittorio*, in *Dir. pen. proc.*, 2003, p. 145.

TONINI P.– CAVALLI F., *Le intercettazioni nelle circolari delle procure della Repubblica*, in *Dir. pen. proc.*, 2017, p. 705.

TORRE M., *Il captatore informatico dopo la legge c.d. "spazza-corrotti"*, in *Dir. pen. proc*., 2019, p. 648 ss.

TORRE M., *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017.

TORRE M., *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc*., 2015, p. 1168.

TORRE M., *Indagini informatiche e processo penale*, Firenze, 2016.

TRIGGIANI N., *Le videoriprese investigative e l'uso dei droni*, in SCALFATI A. (a cura di), *Le indagini atipiche*, Torino, 2019, p. 161 ss.

TROISI P., *Il potenziamento della cooperazione transfrontaliera. Lo scambio di informazioni, in* AA. VV., *"Spazio europeo di giustizia" e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali*, 2012, p. 195 ss.

TROISI P., *La circolazione di informazioni per le investigazioni penali nello spazio giuridico europeo*, Padova, 2012.

TUCKER C., *Privacy, Algorithms and Artificial Intelligence*, in *The Economics of Artificial Intelligence: An Agenda, University of Chicago*, 2019, p. 423 ss.

UBERTIS G., *Sistema di procedura penale*, Torino, 2004.

VELE A., *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Padova, 2011.

VERGINE F., *La riforma della disciplina delle intercettazioni: un valzer con un'orchestra scordata*, in *Proc. pen. giust*., 2018, p. 787 ss.

VERONESI P., *Per un'interpretazione costituzionale del concetto di "domicilio"*, in *Ann. Univ. Ferrara*, XVII, Ferrara, 2003, p. 125.

WESTIN A. F., *Privacy and freedom*, London, 1967.

WOO C., SO M., *The case for Magic Lantern: September 11 highlights the need for increased surveillance*, in 15, *Harvard Journal of Law and* Technology, 521 (2002).

ZAMPAGLIONE A., *Delega in materia di intercettazioni: un costante bilanciamento di interessi*, in G. SPANGHER (a cura di), *La riforma Orlando*, Pisa, 2017.

ZICCARDI G., Internet, *controllo e libertà*, Milano, 2015.

ZICCARDI G. – LUPARIA L., *Investigazione penale e tecnologia informatica*, Milano, 2007.

ZUBOFF S., *Il capitalismo della sorveglianza*, Luiss University Press, Roma, 2019.