LUCIANO FIORE*

CAPTATORI INFORMATICI, "TERZI NON INDAGATI" E DIRITTI SACRIFICABILI: ALLA RICERCA DI UN EQUILIBRIO TRA EFFICIENZA INVESTIGATIVA E RISPETTO DEI DIRITTI FONDAMENTALI

SOMMARIO: 1. Oggetto dell'indagine e piano di lavoro. - 2. Alcune brevi considerazioni sul captatore informatico. - 3. La definizione di "terzo non indagato" formulata dalla Corte di Cassazione. - 4. Assenza di specifici studi scientifici o ricerche statistiche in relazione alle misure investigative digitali riguardanti soggetti non indagati. - 5. L'auspicato equilibrio tra efficienza investigativa e rispetto dei diritti fondamentali: possibili soluzioni per superare una sfida normativa e culturale. - 6. La recente modifica al codice penale, a quello di rito e all'ordinamento giudiziario: la legge n. 114/2024 (Legge Nordio). - 7. Rilievi conclusivi.

1. *Oggetto dell'indagine e piano di lavoro*

Sino a qualche tempo fa, le modalità di utilizzo del c.d. captatore informatico erano oggetto di dibattito solo tra esperti del settore. Solo successivamente, dopo l'emergere di delicate questioni riguardanti la tutela di alcuni diritti fondamentali, tra cui il diritto alla riservatezza delle comunicazioni, tale strumento è iniziato a diventare oggetto di sempre maggiore attenzione e di studio da parte della letteratura specialistica sia di tipo tecnico-informatico che giuridico.

Diverse sono le criticità seguite al sempre più diffuso utilizzo di tale strumento investigativo ed alla disinvoltura applicativa da parte di alcuni inquirenti. È altresì innegabile come il forte e crescente interesse dei *mass media* in relazione a fatti di cronaca giudiziaria che vedono coinvolte sempre più soggetti che ricoprono incarichi politici o che sono mediaticamente esposti, abbia contribuito ad accelerare ed accendere il dibattito su quali siano (ed a quale prezzo lo siano) i loro diritti e le loro libertà sacrificabili in nome di un'esigenza sempre più sentita di repressione di alcuni tipi di reati.

Considerando la necessità di un equilibrio tra la tutela dei diritti fondamentali dei cittadini, come l'inviolabilità della libertà, della segretezza della corrispondenza e di ogni altra forma di comunicazione, e l'importanza di ottenere risultanze investigative efficaci ai fini della prevenzione di determinati reati di forte allarme sociale, le intercettazioni ambientali tramite captatore informatico rappresentano una sfida per tracciare i confini entro cui considerare lecita l'attività di ricerca della prova.

È quindi naturale, anche alla luce dei recenti tentativi di riforma, che si sia acceso fuori dall'ambito accademico un dibattito nell'opinione pubblica all'interno della quale c'è chi ritiene che un'enfatizzazione dei diritti del "terzo non indagato" possa ostacolare o impedire le attività investigative mirate alla ricerca della prova e chi, su un fronte diametralmente opposto, ritenga che il rafforzamento del quadro normativo in senso maggiormente

* Dottorando in "Pluralismi Giuridici. Prospettive antiche ed attuali", Università degli Studi di Palermo.

garantistico possa dare una più concreta applicazione al principio della presunzione di non colpevolezza di cui all' art. 27, co. 2, Cost.

L'obiettivo di questa ricerca è quello di pervenire ad una definizione di "terzo non indagato" e individuare quali dei suoi diritti fondamentali siano sacrificabili nell'ambito della tematica - ampiamente scandagliata dalla dottrina e dalla giurisprudenza – relativa all'uso investigativo del captatore informatico. Si cercherà di affrontare in chiave sistematica alcune problematiche connesse allo *status* di "terzo non indagato", effettuando un'esegesi delle più dibattute questioni collegate all'utilizzo di questo strumento che, secondo la giurisprudenza, costituisce una modalità esecutiva di un'intercettazione ambientale e non un mezzo di ricerca della prova atipico[1].

Non disponendosi, tuttora, di un quadro legislativo idoneo a dipanare in modo organico tutte le perplessità di cui sopra, si focalizzerà l'attenzione sulla questione dei diritti dei "terzi", spesso vittime di "stigmatizzazione pubblica" da parte dei *media*. Si ritiene opportuno muoversi considerando "invalicabili" – alla luce delle innegabili intersezioni tra il diritto comunitario e il diritto processuale penale interno – i confini tracciati dalla nostra Carta costituzionale e rappresentati dai diritti fondamentali in essa garantiti (artt. 2 e 15 Cost. su tutti) ed i parametri sovranazionali, tratti in particolare dall'art. 8 della Convenzione europea dei diritti dell'uomo (di seguito, CEDU) e dagli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'Unione Europea (di seguito, CDFUE).

Numerose sono state le pronunce da parte della Corte di Giustizia dell'Unione Europea che hanno affrontato il delicatissimo tema del bilanciamento tra il diritto alla sicurezza e la protezione dei dati personali, con particolare riferimento alle intercettazioni ed alla sorveglianza di tipo elettronico.

Esemplificativa in tal senso è la sentenza *Digital Rights Ireland (C-293/12),* con la quale la stessa Corte ha invalidato la direttiva sulla conservazione dei dati (2006/24/CE), affermando come la conservazione indiscriminata degli stessi, costituisca una grave violazione del diritto alla *privacy* e alla protezione dei dati in relazione agli articoli 7 e 8 della CDFUE.

Da quanto sopra evidenziato, appare chiaro come il principio di proporzionalità sia un tema centrale nella giurisprudenza della Corte, tant'è che, in relazione a qualsiasi restrizione dei diritti fondamentali, si ammonisce sull'uso strettamente necessario e proporzionato all'obiettivo perseguito, sottolineando come la captazione di conversazioni di persone terze non indagate debba avvenire solamente in casi del tutto eccezionali, così come ribadito anche nella sentenza *Tele2 Sverige* (C-203/15).

Inoltre, anche nel caso *La Quadrature du Net* (C-511/18), la Corte ha nuovamente sottolineato l'importanza di bilanciare le esigenze di sicurezza con la protezione dei dati personali, statuendo che la sorveglianza di massa non può essere giustificata a discapito dei diritti fondamentali per prevenire abusi nei confronti di soggetti non coinvolti nelle indagini.

---

[1] Cass., Sez. un. 28 aprile 2016, n. 26889 (dep. 1° luglio 2016), Scurato, in *Arch. nuova proc. pen.*, 2017, p. 76 e ss. con nota di A. CAMON, *Cavalli di troia in Cassazione*; in *Cass. Pen.* 2016, pp. 2274-2288, con nota di A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*; in Il *Diritto dell'informazione e dell'informatica*, 2016, p. 88, con nota di CORASANITI, *Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*; in *Proc. pen. giust.*, 2016; CISTERNA, *Spazio ed intercettazioni, una liaison tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite,* in *Arch. pen.* 2016, II, p. 331; PICOTTI, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. pen.* 2016, II, p. 354; FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen.* 2016, II, p. 348.

L'analisi condotta ci quindi porterà a considerare, *de iure condendo*, i rischi di violazione dei diritti costituzionalmente garantiti, attraverso la diffusione ingiustificata di conversazioni non rilevanti ai fini giudiziari. Si cercherà di individuare le possibili criticità della legge n. 114/2024 (Legge Nordio), la quale impone di eliminare dai verbali delle intercettazioni tutti i dati che «consentono di identificare soggetti diversi dalle parti»[2].

Attesa la sorprendente carenza di studi e ricerche accademiche sulle misure investigative digitali riguardanti individui "terzi non indagati", prenderemo, quale riferimento, per questo approfondimento un provvedimento non meramente legislativo, rappresentato dalla delibera della Settima Commissione del CSM del 29 luglio 2016.[12]

Tale documento si segnala in quanto offre le *best practices* adottate da numerose Procure italiane in relazione alla rilevanza e pertinenza di quelle conversazioni il cui contenuto sia riferibile anche ai dati sensibili – così come definiti dall'art. 4 lett. *d*) del D. Lgs. 30 giugno 2003, n. 196 (c.d. Codice della *privacy*) – che coinvolgano soggetti terzi, non indagati o estranei ai fatti di indagine, quando costoro non siano oggetto di intercettazione diretta. Tali indicazioni possono fornire un utile punto di partenza per affrontare alcune criticità che si prospettano in vista dell'emendando impianto normativo.

2. *Alcune brevi considerazioni sul captatore informatico*

Nonostante l'ampia intrusione delle intercettazioni nel diritto alla riservatezza della corrispondenza e delle comunicazioni, il nostro codice di procedura penale non fornisce una definizione specifica di tale mezzo di ricerca della prova.

La lacuna è stata colmata dalla giurisprudenza della Corte di Cassazione, che ha descritto l'intercettazione come quella «captazione ottenuta mediante strumenti tecnici di registrazione, del contenuto di una conversazione o di una comunicazione segreta in corso tra due o più persone, quando l'apprensione medesima è operata da parte di un soggetto che nasconde la sua presenza agli interlocutori»[3].

Le indagini ambientali svolte attraverso l'uso di un captatore informatico, in particolare, costituiscono un sofisticato strumento di ricerca della prova finalizzato ad acquisire dati senza il consenso delle persone coinvolte. È evidente come l'uso indiscriminato di indagini ambientali possa sollevare questioni etiche e giuridiche riferibili all'utilizzo del captatore informatico e la sua opportunità. Appare quindi indispensabile bilanciare il diritto alla *privacy* delle persone coinvolte con la necessità di ottenere risultanze investigative legittime: e ciò in quanto le indagini ambientali, a ben vedere, si trovano in una zona grigia tra legalità e illegalità.

Con l'importante "sentenza Scurato"[4], le Sezioni unite della Corte di Cassazione hanno tracciato le linee guida sull'impiego dei captatori informatici, noti anche come "*trojan* di Stato".

Tre sono gli aspetti maggiormente rilevanti emersi dalla pronuncia richiamata. In primo luogo, la possibilità di intercettare conversazioni "ambientali" anche in contesti privati senza necessità di un'attività criminosa in corso e, in secondo luogo, la configurabilità di un'ampia definizione dei reati di criminalità organizzata. Altresì, tale decisione ha assunto importanza

[2] Legislatura 19ª, 2ª Commissione permanente, Resoconto sommario n. 125 del 15/02/2024 (*www.senato.it*).
[3] Cass. Sez. un., 28 Maggio 2003, n. 36747/2003, Torcasio, Rv. 225465 – 01.
[4] Cass., Sez. un. 28 aprile 2016, n. 26889 (dep. 1° luglio 2016), Scurato, in CED Cass., n. 266905-266906.

in quanto ha finito per autorizzare l'uso di *spyware* del tipo *trojan horse* per fini investigativi, permettendo al relativo operatore di avere un controllo totale sulle attività, i movimenti e le comunicazioni dell'utente senza che questi ne sia consapevole.

La fase di creazione e l'inoculazione di tali strumenti informatici è flessibile, poiché non esiste una normativa *ad hoc* che ne vieti la produzione, ma solo il loro uso non autorizzato è vietato.

Appare altresì opportuno evidenziare come sia improprio parlare di "*trojan* di Stato"[5] poiché, di fatto, il nostro Paese non è dotato di una tecnologia proprietaria, o di diretta ed esclusiva gestione, dovendosi invece servire di *software* sviluppati, e spesso gestiti, da privati (anche stranieri) con tutte le conseguenze e i rischi legati ad un loro utilizzo non conforme agli *standard* di garanzie richiesti per tali attività, o ad una non corretta gestione del flusso dei dati acquisiti.

È, infine, appropriato ricordare come, oltre a quanto già disciplinato dagli artt. 266-271 c.p.p., in tema di intercettazioni di conversazioni o comunicazioni, l'art. 89 disp. att. c.p.p. preveda che, in caso di uso del captatore informatico, nel verbale delle operazioni compiute debba essere indicato il tipo di *software* impiegato, il quale deve essere conforme ai requisiti tecnici stabiliti con decreto del Ministro della Giustizia.

3. *La definizione di "terzo non indagato" formulata dalla Corte di Cassazione*

Una volta tracciati i confini normativi entro cui ritenere legittima l'utilizzabilità del captatore informatico, finalizzata ad ottenere una *data collection* utile ai fini investigativi, il tema assume una forma diversa e più complessa nel momento in cui ci si interroghi su una specifica questione giuridica. Gli operatori del diritto sono chiamati a fornire risposte ad un problema non ancora risolto, inerente alla tutelabilità dei diritti dei "terzi non indagati" le cui conversazioni risultino captate nelle intercettazioni predisposte dagli inquirenti. Costoro, infatti, spesso risultano vittime di "stigmatizzazione pubblica" da parte dei *media* per il solo fatto di essersi trovati a comunicare con un soggetto indagato.

Appare quindi necessario ed urgente ai fini della tutelabilità dei diritti fondamentali degli stessi (*inter alia iura* si annovera il diritto alla riservatezza delle comunicazioni), pervenire sin da subito ad una chiara definizione di "terzo non indagato", cercando di comprendere quale sia il punto di equilibrio tra ciò che è lecito sacrificare in nome di un bene superiore (l'interesse dello Stato alla repressione dei reati) e la prevenzione di possibili lesioni di diritti costituzionalmente garantiti, facenti capo, peraltro, al valore (super) costituzionale, oltre che convenzionale, della dignità umana[6].

I diritti a rischio, in questo caso, sono soprattutto quelli della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione che l'art. 15 Cost. eleva a diritto inviolabile, intersecandone le fondamenta con quanto sancito dall'art. 2 Cost[7]. Quest'ultimo,

---

[5] R. DE VITA, A. LAUDISA, *Vita digitale a rischio: I captatori informatici tra pericoli per i diritti umani e riduzionismo giuridico*, in *Eurispes* (*on-line*), 2019.

[6] Si veda, tra gli altri, C. DRIGO, *La dignità umana quale valore (super)costituzionale*, in L. MEZZETTI (a cura di), *Principi costituzionali*, Torino, 2011, p. 239 ss.

[7] D.J. SOLOVE, *A Taxonomy of Privacy*, *University of Pennsylvania Law Review*, vol. 154, 2006, pp. 477-560. *Questo articolo sviluppa una tassonomia dettagliata della privacy, utile per comprendere meglio le diverse forme di interferenza nella vita privata e come queste possano essere classificate e tutelate nel contesto giuridico.*

com'è noto, sancisce il principio secondo cui «la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità». Tale principio è così rilevante al punto che autorevole dottrina costituzionalistica ritiene che esso «contenga in forma sintetica la Costituzione intera».[8]

La Corte costituzionale ha affermato che la libertà e la segretezza delle comunicazioni corrispondono a diritti inviolabili e fondamentali, protetti dall'art. 15 Cost. Tali diritti sono essenziali per la dignità umana e la loro previsione rientra nel nucleo dei diritti inviolabili, non comprimibili se non nei limiti costituzionalmente previsti[9]. Una limitazione della sfera di tutela può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

Secondo un primo approccio teorico[10], si potrebbe individuare un nuovo diritto fondamentale, ossia il diritto alla riservatezza informatica, considerandola come una manifestazione del libero sviluppo della personalità, proprio in base all'art. 2 Cost. Altri studiosi suggeriscono, tuttavia, di fondare tale nuovo diritto fondamentale alla riservatezza informatica non solo sull'art. 2 Cost., ma anche sull'art. 8 CEDU e sugli artt. 7 e 52 CDFUE. La Carta fondamentale appena menzionata, tra l'altro, dopo la firma del Trattato di Lisbona, ha esteso la propria efficacia vincolante a tutti gli Stati membri dell'UE, sia pur nelle sole materie di competenza dell'Unione. Secondo l'ora descritto ragionamento, nell'ordinamento italiano, tale diritto potrebbe subire delle compressioni «solo nel rispetto della legge e della giurisdizione, secondo il principio di proporzionalità»[11].

La giurisprudenza italiana ed europea hanno diverse volte posto l'accento sul fatto che i diritti dei soggetti terzi, intesi come coloro che non sono parte attiva in un procedimento penale, devono essere tutelati con il massimo rigore possibile. Ciò in virtù dei principi di proporzionalità e necessità che non si traducono in vuoti formalismi, bensì rappresentano il criterio attraverso cui valutare se, e fino a che punto, sia legittimo incidere su libertà fondamentali come la *privacy* o la riservatezza delle comunicazioni.

Un passaggio importante in questa direzione lo si ritrova nella sentenza n. 20 del 2021 della Corte costituzionale nella quale, è stato ribadito un concetto fondamentale: strumenti invasivi come le intercettazioni, in particolare quelle effettuate con captatori informatici, possono essere utilizzati solo quando esista un'effettiva utilità per le indagini, e sempre entro limiti molto stretti. L'autorità giudiziaria, insomma, non può permettersi leggerezze: ogni captazione va vagliata con attenzione, proprio per evitare che finiscano nel fascicolo elementi che ledono diritti altrui senza reale necessità.

Accanto alla tutela della *privacy* in senso tradizionale, oggi si parla sempre più spesso di riservatezza informatica[12]: una dimensione più attuale, legata alla protezione dei dati e delle comunicazioni digitali. Anche su questo fronte la giurisprudenza europea è stata chiara. Nelle sentenze *Digital Rights Ireland* e *Tele2 Sverige*, la Corte di giustizia dell'Unione europea ha

---

[8] M. FIORAVANTI, *Costituzione italiana: articolo 2*, Roma 2017, p. 1 ss.

[9] Sull'inscindibile nesso che lega l'art. 2 e l'art. 15 si è pronunciata la Corte costituzionale nelle sentt. nn. 366/1991 e 81/1993. Come è stato detto (V. Italia 1963, 41), "[i]l complesso delle libertà costituzionali forma, per così dire, quasi un tessuto, e nel contesto delle singole disposizioni vi sono delle categorie, delle sottospecie, dei rapporti, e delle linee di "derivazione" del principio fondamentale dell'art. 2 della Costituzione".

[10] R. ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, in *Archivio penale* (bollettino *web*), 25 luglio 2016, 10-11

[11] F. IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale, in Diritto Penale Contemporaneo, n. 3-4/2014*, 338. Nello stesso senso P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Processo penale e giustizia*, 2016, p. 125 ss.

[12] F. GALLI, *La protezione dei dati personali nell'era digitale*, Milano, 2021.

stabilito che l'accesso ai dati personali dev'essere sottoposto a controlli rigorosi[13], e che ogni limitazione a questi diritti deve essere realmente proporzionata e giustificata da esigenze concrete di sicurezza.

Un altro principio cardine, spesso richiamato dalla Corte di Cassazione, è quello della buona fede del terzo. Quando si tratta di soggetti estranei al reato, la compressione dei loro diritti è ammessa solo in presenza di un interesse pubblico prevalente[14], e a condizione che il terzo non abbia tratto alcun beneficio dall'illecito. Si pensi, ad esempio, alle ipotesi di sequestro o confisca: anche lì, il sacrificio di diritti patrimoniali o della riservatezza richiede sempre un vaglio attento e una motivazione puntuale.

In definitiva, tutto ruota attorno a un equilibrio delicato: quello tra l'interesse alla repressione dei reati e la tutela dei diritti di chi, pur non indagato, finisce per essere coinvolto. Ed è proprio qui che il principio di proporzionalità trova la sua piena applicazione: come strumento per prevenire abusi e garantire che nessun diritto venga compresso oltre quanto strettamente indispensabile.

Tanto sopra premesso, una puntuale e condivisibile definizione di "terzo non indagato" o persona estranea al reato è possibile rinvenirla in diverse statuizioni della Suprema Corte[15], la quale si è pronunciata in tema di sequestro finalizzato alla confisca del profitto del reato presso terzi, ossia soggetti distinti dall'autore del fatto.

La Suprema Corte ha ricordato nella citata statuizione che «terzo è la persona estranea al reato, ovvero la persona che non solo non abbia partecipato alla commissione del reato, ma che da esso non abbia ricavato vantaggi e utilità». Ed ancora: «al requisito oggettivo, integrato dalla non derivazione di un vantaggio dall'altrui attività criminosa, deve aggiungersi la connotazione soggettiva della buona fede del terzo, intesa come non conoscibilità, con l'uso della diligenza richiesta dalla situazione concreta, del predetto rapporto di derivazione della propria posizione soggettiva dal reato commesso dal condannato».

Tale precisazione, seppur apparentemente scontata, assume invero un significato di certezza definitoria che consente di evitare interpretazioni "estensive" o "riduttive" dello *status* di "terzo non indagato", ossia di un soggetto che, pur non assumendo un ruolo primario nell'ambito di una investigazione, rischia di veder lesi alcuni diritti inviolabili che la Carta Costituzionale gli attribuisce e che rappresentano quel limite invalicabile oltre il quale l'utilizzo del captatore informatico non può e non deve spingersi.

È importante sottolineare come la condizione di "terzo non indagato" non implichi necessariamente l'assenza di un coinvolgimento periferico o di interesse nell'ambito dell'indagine. Tuttavia, affinché possano essere considerati "terzi non indagati" i soggetti in questione non devono risultare formalmente indagati o sospettati di reati da parte delle autorità competenti.

La divulgazione e la pubblicazione delle intercettazioni, che può avvenire in vari contesti, inclusi processi giudiziari, inchieste giornalistiche e altri mezzi di comunicazione, solleva, tuttavia, gravi preoccupazioni per la *privacy* e la reputazione di queste persone, le quali potrebbero essere esposte a un rischio ingiustificato di pregiudizio sociale o professionale a causa di informazioni sensibili divulgate durante le intercettazioni.

---

[13] Digital Rights Ireland e Tele2 Sverige: la sorveglianza di massa e la Corte di Giustizia dell'Unione Europea, in *Rivista di diritto dell'Unione Europea*, 2022.

[14] G. SILVESTRI, *Il sequestro e la confisca nei confronti di terzi non indagati: profili giuridici*, in *Rivista di diritto processuale penale*, 2020.

[15] Cass., Sez. V, Sent. del 21/06/2021 (ud. 14 maggio 2021), n. 24248 - Sez. un, n. 11170 del 25/09/2014, dep. 2015, Rv. 263684; Sez. 2, n. 11173 del 14/10/1992, Rv 193422; Sez. 3, n. 3390 del 19/01/1979, Rv 141690.

4. *Assenza di specifici studi scientifici o ricerche statistiche in relazione alle misure investigative digitali riguardanti soggetti non indagati*

Alla luce dei chiarimenti operati dalle Sezioni unite della Corte di Cassazione[16] circa la natura giuridica del "captatore informatico", perimetrata la cornice codicistica entro cui sarà possibile muoversi, e chiarito anche chi possa acquisire lo *status* di "terzo non indagato" nel corso di un'attività di indagine, emerge un sorprendente *deficit*, nella discussione accademica, di studi scientifici e ricerche statistiche sulle misure investigative digitali che coinvolgano soggetti "terzi non indagati", privi di un ruolo formale nel procedimento.

Nonostante la ricca letteratura giuridica esistente sul tema dei captatori informatici, risulta carente un'analisi quantitativa che valuti gli effetti di queste misure sui diritti dei "terzi non indagati". [17]

Questo vuoto accademico rende difficile comprendere pienamente l'impatto che tali strumenti possono avere sulla tutela della *privacy* e sulla protezione dei dati personali[18].

Per tali ragioni, prendendo spunto *de iure condendo* da un documento di tipo non meramente legislativo, ma "organizzativo-interno" alla magistratura italiana, ossia la delibera della Settima Commissione del CSM del 29 luglio 2016[19], si cercherà nel prossimo paragrafo di fornire un fondamento scientifico a un insieme di criteri che, partendo dall'idea di "buone prassi" già adottate da alcune Procure italiane, potrebbero essere assunti come riferimento nel contesto di un'auspicabile regolamentazione normativa.

5. *L'auspicato equilibrio tra efficienza investigativa e rispetto dei diritti fondamentali: possibili soluzioni per superare una sfida normativa e culturale*

Attraverso il monitoraggio di numerose direttive e circolari assunte da diversi Procuratori della Repubblica[20], la citata settima Commissione del CSM, come già detto, ha da tempo elaborato e offerto a tutti gli uffici giudiziari italiani, con un apprezzabile sforzo di sintesi, alcune buone prassi adottate da singoli uffici della Procura della Repubblica, che sono state nei successivi anni fonte di ispirazione per la corretta gestione dei dati potenzialmente

---

16 Per un commento alla pronuncia delle Sezioni unite: G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, commento a Cass. Sez. un. 28 aprile 2016 (dep. 1° luglio 2016), n. 26889, Pres. Canzio. Rel. Romis, Imp. Scusato, in *Dir. pen. cont*, 7 ottobre 2016.

17 Secondo una recente indagine condotta dalla *European Data Protection Board*, circa il 15% delle intercettazioni che coinvolgono captatori informatici include conversazioni o dati personali di soggetti estranei all'indagine. Questi dati confermano la necessità di introdurre un monitoraggio più rigoroso, per evitare che la *privacy* di questi soggetti venga compromessa ingiustamente.

18 Come evidenziato dal rapporto della *European Union Agency for Fundamental Rights* (FRA), le misure di sorveglianza pongono seri rischi per i diritti fondamentali dei soggetti non coinvolti direttamente nelle indagini, in particolare in relazione alla loro privacy e alla protezione dei dati personali (*Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU*, FRA, 2015).

19 Ricognizione di buone prassi in materia di intercettazione di conversazioni (Delibera del 29 luglio 2016), reperibile in: https://www.csm.it/documents/21768/87316/Delibera+29+luglio+2016/e02375fb-aa0f-c706-315b-a3067725a9ef.

20 I Procuratori della Repubblica organizzano i loro uffici anche attraverso il potere di direttiva di cui all'art. 4 D. Lgs. n. 106/2006.

lesivi della *privacy* dei soggetti "terzi non indagati".[21] Tali virtuose prassi offrono interessanti soluzioni applicative che potrebbero aspirare a diventare "misure di salvaguardia" normative, da adottare e porre a presidio degli interessi costituzionali in gioco anche in relazione a questi soggetti.

Come snodo cruciale della presente ricerca, si sono pertanto individuati alcuni punti e principi generali comuni, relativi alle "intercettazioni irrilevanti" (tra queste, quelle avvenute con "terzi non indagati"), già oggetto di buone prassi da parte di alcuni uffici giudiziari italiani. Si esamineranno tali soluzioni con un approccio critico, ampliandone la portata e provando a estrapolare alcuni inderogabili principi generali, fondamentali per favorire il bilanciamento fra i valori costituzionali in gioco.

Enumerando alcune pratiche positive adottate da uffici giudiziari mediante la formulazione di circolari, la Commissione ha evidenziato come tutte le suddette pratiche partano dal presupposto comune che la diffusione non giustificata delle risultanze delle intercettazioni sia strettamente legata alla trascrizione delle conversazioni e alla loro inclusione nelle annotazioni di polizia giudiziaria[22].

Nel panorama europeo, vari Paesi hanno affrontato il delicato equilibrio tra sicurezza e protezione dei dati in modo differente. A tal uopo assume un importante rilievo la *Loi Renseignement* del 2015, adottata dalla Francia, che ha regolato in modo dettagliato le intercettazioni e l'uso di tecnologie invasive per scopi investigativi. Da rilevare come, sebbene tale provvedimento legislativo permetta ampie possibilità di controllo, all'interno della stessa legge sono previste anche rigide salvaguardie per garantire la protezione dei diritti fondamentali, in particolare in relazione ai terzi non indagati. Tale norma, infatti, ha cercato di regolare l'uso di captatori e intercettazioni nel contesto delle indagini antiterrorismo, stabilendo limiti chiari all'uso dei dati raccolti. Purtuttavia, anche in questo caso, l'equilibrio tra *privacy* e sicurezza è stato oggetto di una serie di ricorsi alla Corte Europea dei Diritti dell'Uomo.

Emblematico negli USA, il caso Eric Loomis ha acceso il dibattito sull'uso dell'algoritmo COMPAS per la valutazione del rischio di recidiva, evidenziando come l'uso di tecnologie predittive possa introdurre pregiudizi nei confronti di determinati gruppi sociali[23]. La sentenza ha aperto la strada a un maggiore controllo sull'uso delle tecnologie predittive nel sistema giudiziario americano.

In Italia, l'uso dei captatori informatici solleva ancora molteplici questioni, soprattutto riguardo alla tutela dei diritti dei terzi. Questo confronto tra ordinamenti permette di osservare come, mentre in Francia le garanzie sono più strutturate, l'Italia necessiti di un

---

[21] Un altro significativo esempio di "buona prassi" lo si ritrova nelle "linee guida in materia di intercettazioni di conversazioni" predisposte dalla Procura della Repubblica presso il Tribunale di Aosta il 02 gennaio 2017: https://www.procura.aosta.giustizia.it/documentazione/D_13252.pdf.

[22] Tuttavia, è doveroso ricordare e sottolineare come, ad eccezione dei casi di assoluta inutilizzabilità, la selezione operata dal pubblico ministero non possa impedire la trasmissione al giudice, ai fini del successivo deposito, delle trascrizioni e/o registrazioni di conversazioni e/o scambi di comunicazioni informatiche o telematiche che siano, anche indirettamente, favorevoli all'indagato. In tal senso è bene ricordare come l'art. 358 c.p.p. preveda espressamente che l'attività ricognitiva deve essere estesa anche agli elementi di prova che potrebbero scagionare l'indagato.

[23] O.S. KERR, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, Michigan Law Review, vol. 102, no. 5, 2004, pp. 801-888*). La questione del bilanciamento tra sorveglianza e *privacy* è centrale anche nel contesto britannico, dove la legge sulla sorveglianza del 2016 ha introdotto nuove tutele per i diritti dei cittadini soggetti a intercettazioni digitali (SIMMONS, RIC, *The Failure of the Fourth Amendment in the Digital Age, Berkeley Journal of Criminal Law, vol. 25, 2020, pp. 89-150*).

ulteriore sviluppo normativo per proteggere i soggetti estranei alle indagini, mantenendo sempre al centro il principio di proporzionalità.

In tal senso, appare condivisibile l'idea che il pubblico ministero, parte imparziale del processo e *dominus* delle indagini preliminari, debba effettuare direttamente, anche delegando la polizia giudiziaria attraverso delle precise direttive, il primo importante "filtro" per il raggiungimento di tale scopo. Tale sottolineatura deriva, a parere di chi scrive, da alcune non corrette prassi operative che spesso hanno lasciato alla discrezionalità della polizia giudiziaria, attraverso direttive troppo generiche, il compito di decidere di non annotare sul registro delle intercettazioni le conversazioni che si ritengono inutilizzabili, privando così il magistrato della possibilità di valutarle.

A livello generale, qualsiasi forma di delega "in bianco" alla polizia giudiziaria solleva questioni di natura sistemica e normativa, poiché è al pubblico ministero che spetta un vaglio. Peraltro, la valutazione della rilevanza delle conversazioni richiede una visione completa degli elementi raccolti durante l'indagine che, se affidata esclusivamente alla polizia giudiziaria senza un adeguato coordinamento, potrebbe comportare una disamina frammentata, limitata e potenzialmente fallace.

Il pubblico ministero, infatti, soprattutto in contesti investigativi complessi ed estesi, funge da punto di convergenza per molteplici informazioni provenienti da varie branche della polizia giudiziaria, e spesso svolge un ruolo centrale nell'analisi e nella sintesi di tali dati. Inoltre, è bene ricordarlo, il pubblico ministero può essere chiamato a valutare la rilevanza e l'utilizzabilità di tali informazioni anche in relazione ad altri procedimenti in corso.

Pertanto, si ritiene imprescindibile una valutazione adeguata da parte del magistrato inquirente delle intercettazioni in corso. Tale verifica dovrebbe avvenire attraverso un costante dialogo con la polizia giudiziaria delegata, ma è chiaro che un simile confronto possa avvenire solo nella c.d. "fase cautelare". Al termine delle indagini, infatti, sarà il solo p.m. a dover porre la massima attenzione a non effettuare il deposito di conversazioni oggetto della selezione negativa operata nella precedente fase, a meno che non vi sia una rivalutazione del complessivo materiale probatorio acquisito, con conseguente ripensamento rispetto alle precedenti decisioni.

Ove nel corso delle singole intercettazioni con "terzi non indagati" dovessero risultare palesemente estranee alle esigenze investigative e/o processuali alla dimostrazione dei fatti costituenti reato ed alla relativa responsabilità, previo confronto con il pubblico ministero, si ritiene auspicabile - ed in linea con la maggior parte delle "buone prassi" citate dalla Commissione - che la polizia giudiziaria riporti nel brogliaccio di ascolto l'annotazione "intercettazione manifestamente irrilevante ai fini delle indagini" o una formula similare, evitando sunti o trascrizioni, con la mera indicazione degli interlocutori (se identificabili) ed il contenuto sommario dell'oggetto della conversazione.

Le registrazioni di conversazioni che includono informazioni sensibili, infine, richiedono una particolare prudenza nella valutazione della loro pertinenza o rilevanza.

Queste conversazioni possono anche riguardare dati sensibili *ex* art. 4 lett. d) D.lgs. n. 196/2003, come opinioni politiche o religiose, informazioni sulla sfera sessuale o dati relativi alla salute, per i quali il codice della *privacy* prevede una protezione più rigorosa, sia per l'indagato che per terzi non coinvolti direttamente nell'intercettazione. Se queste conversazioni dovessero essere considerate non rilevanti ai fini probatori, non dovrebbero essere trascritte o riassunte, e sarebbe sufficiente indicare brevemente il contenuto con la dicitura "conversazione privata relativa a dati sensibili" o una formula dello stesso tenore.

Anche tali registrazioni dovrebbero sempre essere comunicate al pubblico ministero che deciderà se ritenerle pertinenti e rilevanti per l'indagine.

Da un'altra prospettiva, è necessario sottolineare che l'importanza di una scrupolosa selezione delle conversazioni riguardanti "terzi non indagati" attiene anche alla fase della valutazione dell'inclusione delle stesse nei provvedimenti cautelari, coinvolgendo, quindi, non solo le richieste del pubblico ministero, ma anche le ordinanze del g.i.p. Anche questo aspetto appare cruciale, considerando che tali provvedimenti hanno una naturale propensione a ricevere una forte attenzione mediatica, in quanto sono legati alla privazione della libertà personale di uno o più soggetti e sono cronologicamente più vicini all'evento rispetto al momento del deposito degli atti al termine delle indagini preliminari: ciò è importante anche tenendo conto del dovere di depositare, ove richiesto ed in ottemperanza alle statuizioni della Corte costituzionale[24], le registrazioni e i *files* audio delle conversazioni che sostengono la misura cautelare.

La corretta opera di "filtro" inizialmente operata dal p.m. attraverso un confronto diretto e costante con la polizia giudiziaria delegata, assume connotati di delicatezza assoluta in relazione ai diritti del "terzo non indagato", in quanto il rischio maggiore per il diritto alla riservatezza dei suoi dati personali, a parere di chi scrive, non risiede nella semplice raccolta dei dati stessi e nelle valutazioni sopra operate dal p.m., bensì nell'eventuale deviazione di dati non preventivamente "filtrati" secondo i principi sopra indicati, attraverso una loro non corretta gestione. Tale circostanza può manifestarsi attraverso divulgazioni non autorizzate o non giustificate da necessità investigative o processuali, oppure tramite la distruzione, perdita o alterazione dei dati stessi. Si sottolinea che solo un'adeguata gestione dei dati intercettati, compresa la loro raccolta, trattamento, utilizzo e finalità, può garantire la protezione degli interessi in gioco e costituire un meccanismo di equilibrio.

La Corte Europea dei Diritti dell'Uomo (CEDU), con riferimento all'art. 8 della Convenzione (diritto al rispetto della vita privata e familiare), ha più volte sottolineato l'importanza di proteggere la *privacy* dei cittadini, anche in contesti di sicurezza nazionale. Un caso emblematico è Zakharov c. Russia (2015), in cui la Corte ha stabilito che le intercettazioni di massa, senza adeguate salvaguardie per prevenire abusi, violano il diritto alla *privacy* sancito dalla Convenzione.

Nel contesto dell'uso di captatori informatici, la giurisprudenza della CEDU conferma la necessità che ogni ingerenza nella vita privata dei terzi, soprattutto non indagati, debba essere strettamente limitata e soggetta a controlli efficaci. La sorveglianza di massa è ammissibile solo in presenza di garanzie procedurali rigorose, che permettano di evitare ogni possibile abuso o violazione dei diritti umani.

Come già detto, attualmente i nostri uffici giudiziari corrono diversi rischi in tal senso, in quanto privi di una tecnologia proprietaria o di diretto esclusivo controllo delle attrezzature, che li costringe ad utilizzare *software* sviluppati, e spesso amministrati, da fornitori privati (anche stranieri), con tutte le conseguenze ed i rischi ipotizzabili in relazione ad un utilizzo non conforme agli *standard* di garanzie richiesti per tali attività, o ad una non corretta gestione del flusso dei dati acquisiti.

È altresì corretto rilevare come, a causa di questi punti di debolezza del sistema, in passato vi siano state (e vi siano ancora oggi) fughe di notizie e disvelamento di informazioni non autorizzate frutto di condotte illecite, non prevenibili solo attraverso il corretto uso delle attuali norme processuali o deontologiche da parte dei magistrati coinvolti nel procedimento.

[24] Sent. Corte cost. 10/10/2008, n .336 (Presidente Flick; Relatore Silvestri).

Tutto ciò rappresenta certamente un *vulnus* che il legislatore dovrà affrontare e risolvere prima possibile.

Sarebbe in tal senso auspicabile l'utilizzo obbligatorio di tecniche di crittografia o l'adozione di procedure che limitino l'accesso alle risultanze delle captazioni solamente alle persone autorizzate, per garantire ancor di più i valori costituzionali in gioco. Sarebbe altresì necessario prevedere la limitazione della conservazione e la diffusione delle comunicazioni intercettate da parte delle sole persone autorizzate per il periodo di tempo strettamente necessario all'indagine.

Infine, di vitale importanza apparirebbe l'introduzione dell'obbligo normativo di sottoporre le autorità che effettuano intercettazioni a controlli indipendenti, per garantire che seguano le procedure appropriate per la tutela dei "terzi non indagati".

Nel caso in cui si decidesse di utilizzare le conversazioni riguardanti "terzi non indagati" perché necessarie in relazione alle finalità investigative, l'autorità giudiziaria che autorizzi le operazioni e sfrutti gli elementi raccolti dovrebbe sempre evidenziare e giustificare adeguatamente tale impatto nella motivazione dei provvedimenti, illustrando così il bilanciamento dei valori in gioco e la ragione per cui la registrazione è stata inclusa negli atti. È proprio per queste ragioni che la valutazione della rilevanza della conversazione contenente dati sensibili deve spettare solamente al pubblico ministero ed al giudice e non ad altri. Inoltre, sia il pubblico ministero che il g.i.p. (e successivamente il tribunale) sono chiamati al rispetto dell'obbligo di una "sobrietà contenutistica", derivante dal dovere deontologico di comportarsi con correttezza e lealtà anche nei confronti dei soggetti "terzi non indagati" coinvolti.

Molti dei comportamenti auspicati sono già stati messi in atto da diversi uffici requirenti[25], ma è chiaro che sia auspicabile un deciso intervento precettivo da parte del legislatore il quale, alla luce della concreta situazione organizzativa e delle risorse disponibili, colmi quelle lacune – di natura anche tecnico-informatica – che non pare possano essere risolte solamente dalle iniziative di riforma attualmente *in fieri*.

Infine, si ritiene utile, se non addirittura necessario, *de iure condendo*, informare i "terzi non indagati" quando le autorità intercettano comunicazioni che li riguardano. Ciò al fine di offrir loro la possibilità di opporsi all'utilizzo delle loro comunicazioni.

Oggi più che mai si avverte la necessità di reinterpretare l'equilibrio tra libertà e sicurezza, in conformità con gli *standard* costituzionali, seguendo tale via in totale aderenza ai principi di legalità e proporzionalità della compressione dei diritti *ex* art. 15 Cost. dei "terzi non indagati". Quest'ultimo articolo viene considerato come espressione di criterio implicito da riferire al limite della "necessità", corrispondente a quanto indicato dagli artt. 8-11 della CEDU, da considerare come condizione indispensabile per qualsiasi restrizione dei diritti fondamentali[26]

6. *La recente modifica al codice penale, a quello di rito e all'ordinamento giudiziario: la legge n. 114/2024 (Legge Nordio)*

[25] Un altro significativo esempio di "buona prassi" lo si ritrova nelle "linee guida in materia di intercettazioni di conversazioni" predisposte dalla Procura della Repubblica presso il Tribunale di Aosta il 02 gennaio 2017: https://www.procura.aosta.giustizia.it/documentazione/D_13252.pdf.

[26] CDFUE, articoli 49, paragrafo 3, e 52, paragrafo 1.

Alla luce delle considerazioni svolte, è innegabile ritenere insufficiente a colmare le lacune sopra evidenziate la legge Nordio n. 114/2024 pubblicata nella G.U. n. 187 del 10 agosto 2024. Tale norma impone di eliminare dai verbali delle intercettazioni tutti i dati che consentono di identificare soggetti diversi dalle parti[27].

È senz'altro apprezzabile lo sforzo del legislatore di pervenire ad una soluzione efficace che tenga conto dei diritti fondamentali in gioco. Tuttavia, le conseguenze applicative della norma, si presentano piene di insidie oltreché pericolose per i diritti fondamentali in gioco.

Se per i reati di grave allarme sociale come quelli legati ad atti di terrorismo, è pacifico, in una ideale gerarchia di valori, assegnare alla sicurezza pubblica/nazionale un rango superiore rispetto alla *privacy* del singolo. Tuttavia, problemi applicativi/interpretativi potrebbero sorgere in relazione a quei reati la cui collocazione, nella suddetta gerarchia di valori, debba essere frutto di una lunga interpretazione da parte degli inquirenti che attingono all'intercettazione ambientale attraverso un captatore. L'esperienza giudiziaria insegna, infatti, che, soprattutto nella fase iniziale, non è facile individuare i ruoli dei vari soggetti coinvolti nel contesto relazionale degli indagati. Capita spesso che interlocutori, che inizialmente sembrano estranei ai fatti, ne vengano coinvolti a seguito delle informazioni emerse durante le conversazioni. Pertanto, la nuova norma, ora vigente, applicata rigorosamente nelle prime fasi dell'indagine, potrebbe costringere gli investigatori a dover riascoltare le conversazioni catturate anche attraverso un captatore informatico in un secondo momento, al fine di recuperare i contenuti che non sono stati trascritti, con conseguente aggravio di lavoro e di costi per tutto il comparto investigativo.

Peraltro, il concetto di "rilevanza per le indagini", di cui all'art. 268 co.6 c.p.p., è un concetto intrinsecamente flessibile, destinato a diventare ancora più sfumato durante la fase di ascolto, nel corso di attività captative[28]. Pertanto, è elevato il rischio che si possa incorrere in interpretazioni non conformi agli *standard* di garanzie richiesti per tali attività, in relazione al flusso dei dati acquisiti.

La legge n. 114/2024 (legge Nordio) affronta la questione dell'intercettazione delle comunicazioni di soggetti estranei, imponendo che non debbano essere trascritti dati relativi a soggetti non coinvolti nelle indagini, se non considerati rilevanti per il procedimento. Il giudice sarà quindi tenuto a eliminare dalle intercettazioni tutte le informazioni riguardanti persone estranee al procedimento, qualora non siano indispensabili.

Soffermandoci però ancora ad un'ipotesi in cui il diritto di un individuo "terzo non indagato" possa soccombere alle esigenze investigative, tale situazione potrebbe verificarsi nel caso in cui l'intercettazione di comunicazioni di un soggetto indagato riveli un pericolo imminente per la vita o la sicurezza di un'altra persona o addirittura di più persone. Sulla liceità della compressione del diritto alla *privacy* dei soggetti indagati non sembrano esserci dubbi per la pacifica giurisprudenza costituzionale[29], e per analogia, potrebbe dirsi lo stesso

---

[27] Sul punto, *ex multis*, G. SPANGHER (a cura di), *Le novità della legge Nordio*, Milano, 2024; C. PARODI, *Ddl Nordio: cosa cambia in tema di intercettazioni*, *Ius* Penale; F. DEMARTIS, *Intercettazioni: un correttivo che rafforza la riservatezza delle comunicazioni e tutela l'attività del difensore…ma scontenta i "curiosi"*, in *DPP*, 2024, 1168; FILIPPI L., *Intercettazione: un intervento legislativo all'insegna della tutela della privacy*, cit., 21; P. BRONZO, *Brevi note sul "disegno di legge Nordio"*, in www.sistemapenale.it, 2024.

[28] S. BUZZELLI, *Le nuove intercettazioni tra selettività arbitraria e ridimensionamento delle garanzie difensive*, 2018(2), pp. 1-10.

[29] L'art. 15, par. 1, della direttiva 2002/58/CE, avente ad oggetto i diritti alla riservatezza delle comunicazioni, dei dati sul traffico e di quelli sull'ubicazione, infatti, consente agli Stati membri di derogare a prescrizioni, divieti ed obblighi fissati per la tutela di quei diritti, con l'adozione legislativa di misure restrittive, purché la restrizione costituisca "una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la

in relazione ai diritti dei "terzi non indagati" che nel corso delle indagini risultino essere del tutto estranei ai fatti oggetto di indagine.

Ciò potrebbe accadere qualora le autorità investigative sospettino che un individuo sia coinvolto in un attentato terroristico e durante le intercettazioni delle sue comunicazioni, emergano prove concrete che suggeriscano che l'individuo stia pianificando un attacco imminente contro un luogo pubblico affollato. In questa circostanza, potrebbe essere necessario sospendere temporaneamente il diritto alla *privacy* del "terzo non indagato", al fine di prevenire una minaccia grave e immediata per la sicurezza pubblica/nazionale. Le autorità potrebbero essere autorizzate a monitorare le comunicazioni del sospettato, comprese quelle con terzi non indagati, al fine di identificare e prevenire l'attacco imminente. In situazioni di emergenza e di grave pericolo pubblico, il principio del diritto alla vita e alla sicurezza potrebbe (e dovrebbe) prevalere temporaneamente sul diritto alla *privacy* dei terzi non indagati.

Un'altra problematica diramazione della questione è inoltre legata al contesto in cui avviene tale incidenza sulla sfera del "terzo". La giurisprudenza costituzionale già da tempo si basa su un modello qualitativo. Ad esempio, quando si tratta di raccogliere dati esterni dalle comunicazioni, nel processo penale, la Corte costituzionale ha giustificato trattamenti diversi rispetto alle intercettazioni, statuendo che la limitazione alla libertà possa essere diversa[30].

Riguardo alla *privacy* dei soggetti intercettati, la dottrina, specie quella americana, ha evidenziato come il diritto alla libertà ed alla segretezza di un cittadino sia tutelabile a seconda del contesto in cui avviene la comunicazione (si parla di *privacy context-dependent*): quella che potrebbe sembrare un'invasione della *privacy* in un caso, potrebbe essere accettabile in un altro[31].

Questi concetti teorici sono importanti per dare una risposta al quesito iniziale cui si cercava risposta, in vista di un equilibrio tra l'esigenza delle autorità inquirenti di far venire alla luce importanti risultanze probatorie nel corso delle indagini, da una parte, e il rispetto dei diritti fondamentali dei cittadini diversi dalle parti, dall'altra.

Quanto ai diritti di questi ultimi è ragionevole ritenere che esista una dimensione in più da dover tenere in considerazione: è quella delle "finalità" del mezzo di ricerca della prova. Analizzando il bene tutelato dalla norma, l'art. 15 Cost., la Corte costituzionale insegna come tale diritto sia inviolabile e possa essere limitato solo per proteggere un interesse pubblico primario, con restrizioni strettamente necessarie e motivate dall'autorità giudiziaria[32].

Attraverso una chiave di lettura che tenga conto della dottrina[33] e della giurisprudenza costituzionale formatasi in relazione ai diritti dei soggetti indagati[34], non appare irragionevole, per analogia, applicare tali principi anche ai "terzi non indagati". Si potrebbe quindi renderli pubblicamente identificabili, introducendo un ulteriore elemento da affiancare alla

---

salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica) e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica".

[30] In merito alla pronuncia menzionata, cfr., tra gli altri, A. LONGO, *«Est modus in rebus». Modalità e contesto nella compressione dei diritti fondamentali a partire dalla sentenza della Corte costituzionale n. 122 del 2017*, in Nomos. *Le attualità nel diritto*, 3/2017, cui si rinvia anche per ulteriori riferimenti.

[31] A. CERRI, *Riservatezza (diritto alla). II) Diritto comparato e straniero*, in *Enciclopedia giuridica Treccani*, XXVII, Roma, 1991, p. 5, nella quale si cita la sentenza Cady vs. Bombowski, 413 US 433, 1975.

[32] Sent. Corte cost. 23/07/1991, n. 366/1991 (Presidente Gallo).

[33] 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*, Torino, 2018, p. 289 e ss.

[34] Sent. Corte cost. 10/10/2008, n .336 (Presidente Flick; Relatore Silvestri).

"modalità" ed al "contesto" della limitazione che è quello della "finalità" del mezzo di ricerca della prova utilizzato[35]. Una simile ingerenza potrebbe, quindi, essere giustificata dalla necessità (finalità) di proteggere la vita e la sicurezza delle persone. In situazioni di emergenza e di grave pericolo pubblico, il principio del diritto alla vita e alla sicurezza dovrebbe prevalere temporaneamente sul diritto alla *privacy* anche dei terzi non indagati, in analogia a quanto la migliore dottrina argomenta in relazione ai soggetti indagati.

L'unica soluzione al momento rinvenibile, per bilanciare tale necessaria restrizione al diritto alla riservatezza dei "terzi non indagati", è sicuramente rappresentata da una corretta individuazione da parte dell'autorità procedente delle ragioni per cui tale diritto a non essere identificato debba temporaneamente soccombere[36]. Queste ultime dovranno conformarsi ai fondamenti normativi nazionali (art. 2 Cost.) e internazionali (art. 8 della Convenzione europea dei diritti dell'uomo e artt. 7-8 della Carta dei diritti fondamentali dell'Unione Europea), seguendo i dettami di cui al principio di proporzionalità[37]. Tale principio, lungamente analizzato dalla dottrina, considerato generale parametro interpretativo delle disposizioni in funzione di salvaguardia dei diritti fondamentali, si configura come un valido strumento per bilanciare le esigenze interne del sistema giuridico e quanto stabilito dai principi sovranazionali cui l'Italia aderisce. Ci si riferisce in particolare alla Convenzione di Budapest, fonte internazionale di riferimento in materia di criminalità informatica, ma anche gli artt. 7, 8 e 52, par. 1, della CDFUE ed all'art. 8 CEDU.

I suoi dettami applicati all'ambito dell'uso della tecnologia ed ai moderni strumenti di *surveillance*, sembrano suggerire contemporaneamente un approccio metodologico per garantire adeguatamente i diritti individuali, ma anche un obiettivo finale da perseguire.

E ciò dovrebbe essere richiesto in maniera più esplicita dal legislatore.

Ulteriori interventi del legislatore – parimenti indispensabili e bisognosi di estremo rigore – andrebbero volti a limitare la portata dell'intercettazione: in particolare, secondo un'auspicabile disciplina, l'autorità giudiziaria dovrebbe autorizzare intercettazioni tramite captatore informatico solo quando strettamente necessario, limitando la portata dell'intercettazione alle comunicazioni che riguardano l'oggetto dell'indagine.

7. *Conclusioni*

[35] CORTE EUROPEA DEI DIRITTI DELL'UOMO (Corte EDU), *Zakharov c. Russia*, ricorso n. 47143/06, sentenza del 4 dicembre 2015. La CEDU ha stabilito che la sorveglianza di massa, senza adeguate salvaguardie per prevenire abusi, viola il diritto alla *privacy* sancito dall'art. 8 della Convenzione Europea dei Diritti dell'Uomo. CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA (CGUE), *Digital Rights Ireland (C-293/12)*, sentenza dell'8 aprile 2014. La CGUE ha dichiarato che la conservazione indiscriminata dei dati personali rappresenta una grave violazione del diritto alla *privacy* e alla protezione dei dati (artt. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea.

[36] R. CLARKE, *Privacy Impact Assessment: Its Origins and Development*, *Computer Law & Security Review*, vol. 25, n. 2, 2009, pp. 123-135. Questo articolo esplora l'impatto della *privacy* nell'ambito delle tecnologie di sorveglianza, suggerendo strumenti giuridici per bilanciare sicurezza e protezione dei diritti individuali. ZARSKY, TAL Z., *Governmental Data Mining and Its Alternatives*, *Pennsylvania Law Review*, vol. 116, n. 3, 2014, pp. 285-320. Questo lavoro offre una panoramica sugli strumenti alternativi alle tecniche invasive di sorveglianza, fornendo spunti utili per soluzioni normative bilanciate.

[37] CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. Pen. Cont.* – Riv. Trim., n. 3-4/2014, p. 148 ss. Cfr. anche NEGRI, *Fumus commissi delicti, La prova per le fattispecie cautelari*, Torino, 2004, p. 12.

Valutare se sia corretto limitare un diritto dei "terzi non indagati", rilevante come la libertà e la riservatezza delle comunicazioni di cui all'art. 15 Cost., richiede di considerare diverse prospettive. Non solo bisogna soppesare l'importanza intrinseca del bene tutelato dalla norma, ma anche il tipo e l'impatto della restrizione: sotto quest'ultimo profilo, in particolare, bisogna domandarsi quanto detta restrizione influisca direttamente sul nucleo essenziale o su aspetti più periferici del diritto in gioco. La problematica potrebbe interessare profili inerenti alla protezione dei dati personali non strettamente sensibili, ma comunque rilevanti per la *privacy*, come, ad esempio, le informazioni di contatto o le abitudini di consumo. Sarebbero coinvolte, inoltre, situazioni in cui la violazione della *privacy* non ha conseguenze gravi o immediate sulla libertà individuale, ma comunque genera un senso di disagio o di intromissione nella vita privata.

La regolamentazione di uno strumento così invasivo richiede un approccio ampio, anche di natura tecnologica, che tenga conto non solo dei risultati di *intelligence* e giudiziari, ma anche della sua giustizia e validità.

Concludendo, a parere di chi scrive, una possibile soluzione alle delicate problematiche sopra illustrate potrebbe essere rappresentata dall'introduzione dell'obbligo di informazione dei terzi non indagati quando le loro comunicazioni vengono intercettate. Tale misura consentirebbe loro di contestare l'utilizzo dei loro dati in sede giudiziaria, fornendo così al cittadino coinvolto suo malgrado in un'indagine che non lo riguarda, un ulteriore livello di tutela della *privacy*.

Inoltre, l'introduzione di tecniche di crittografia obbligatoria e di procedure per la conservazione limitata dei dati intercettati garantirebbe che queste informazioni siano trattate in modo conforme ai principi di proporzionalità e necessità, sanciti dalla nostra Costituzione e dal GDPR.

Infine, tra le misure auspicabili, andrebbe considerata anche l'istituzione di una commissione indipendente incaricata di esercitare un controllo effettivo sull'impiego dei captatori informatici, garantendo che i dati raccolti siano utilizzati esclusivamente nei limiti strettamente necessari alle indagini e che le comunicazioni private dei soggetti estranei all'inchiesta siano adeguatamente tutelate.

Sarà, pertanto, fonte di grande responsabilità per il legislatore del futuro delineare un quadro normativo sempre più attento e completo, in conformità ai principi stabiliti dagli artt. 2 e 15 Cost., nonché dall'art. 8 CEDU e dagli artt. 7 e 52 CDFUE.

Sarà compito della dottrina e della giurisprudenza, tuttavia, supportare il legislatore in questa delicata fase di adattamento normativo rispetto ai nuovi strumenti investigativi, enucleando quanto prima i principi fondamentali e le modalità tecniche alle quali le autorità investigative dovranno conformarsi, in modo da restringere il più possibile il raggio interpretativo rispetto alle garanzie tutelate a livello costituzionale.

ABSTRACT: *Digital Surveillance, "Unsuspected Third Parties" and Sacrificable Rights: Striving for a Balance between Investigative Efficiency and Respect for Fundamental Rights*

This paper analyses the critical issues surrounding the use of electronic surveillance in criminal investigations, with particular reference to the protection of the fundamental rights of "third parties not under investigation", namely those who, whilst playing no formal role

in the proceedings, find themselves involved in environmental surveillance as interlocutors of persons under investigation.
Starting from the relevant legal framework – comprising Articles 2 and 15 of the Constitution, Article 8 of the ECHR and Articles 7, 8 and 52 of the Charter of Fundamental Rights of the European Union – and the case law of the Court of Cassation, the Constitutional Court and the Court of Justice of the European Union, the study proposes a legally grounded definition of 'uninvestigated third party' and identifies the limits within which their inviolable rights may be restricted in the name of investigative requirements, in accordance with the principle of proportionality. The analysis highlights a significant lack of scientific studies and statistical research on the subject, and draws on the resolution of the Seventh Commission of the High Council of the Judiciary (CSM) of 29 July 2016 to draw up a set of best practices already adopted by some Italian public prosecutors' offices, proposing that these be elevated to statutory safeguards. Law No. 114/2024 (the so-called Nordio Law) is also examined; whilst acknowledging its commendable aim of safeguarding rights, the analysis highlights the pitfalls of its application and potential operational challenges. *De iure condendo*, the paper advocates the introduction of an obligation to inform third parties whose communications have been intercepted, the mandatory adoption of encryption techniques, the limited retention of intercepted data, and the establishment of an independent body to oversee the use of electronic surveillance devices, in order to ensure an effective balance between investigative efficiency and respect for constitutionally guaranteed rights.