

LE INDAGINI UNDERCOVER NEL MONDO DIGITALE*

Pasquale Bronzo



1. Come noto, le cd “operazioni *under cover*” rientrano tra quelle tecniche d’indagine *extra-ordinarie* utilizzate per penetrare in organizzazioni criminali che, in determinati settori (terrorismo, traffico di stupefacenti, corruzione, pedopornografia), si sono manifestate impenetrabili con gli ordinari strumenti dell’indagine penale: una persona – ufficiale di polizia o privato cittadino – celando la propria identità, si infila all’interno di tali associazioni allo scopo di scoprirne la struttura, individuare i partecipanti, procacciare prove.

Questo strumento di indagine nel tempo è assai mutato rispetto agli archetipi^[1]. Da un lato appaiono ridimensionate nelle finalità normativamente consentite: segnatamente, è recessiva oggi in tutti i sistemi

liberali la declinazione dell'“agente provocatore”, cioè di colui che non si limita ad infiltrarsi nell'associazione (cd. “agente infiltrato”), ma determina altri nella commissione di un reato; dall'altro lato, questo metodo di indagine ha visto importantissimi aggiornamenti nelle tecniche, che ne hanno notevolmente potenziato l'efficacia.

La penetrazione nelle reti criminali, infatti, avviene sempre più frequentemente in ambiente digitale: il *web* è sempre più spesso - lo sappiamo bene - teatro o strumento di condotte delittuose, e alcuni settori di attività delinquenziali si sono praticamente “trasferiti” sulle piattaforme digitali: le investigazioni penali sono dovute scendere sullo stesso terreno, trasponendo nella realtà virtuale di *internet* le tecniche dell'infiltrazione mascherata.

L'attività “sotto copertura” in genere, come attività di indagine penale, è una attività fortemente anomala: sia perché comprende condotte che, al di fuori dell'eccezionale contesto esimente, integrerebbero una responsabilità penale dell'operatore, sia perché la sua insidiosità - connessa al fatto che chi agisce non viene percepito come “autorità procedente” - implica una inevitabile compressione delle garanzie normalmente riconosciute alla persona indagata.

Inutile dire quanto siano delicate queste attività intrusive, per le quali è difficile garantire il rispetto del principio di proporzionalità, col rischio costante di legittimare abusi di potere investigativo. Delicate, eppure ormai indispensabili; lo dimostra la sua crescente diffusione in ambito sovranazionale^[2]: da ultimo la figura compare anche nella disciplina sull'ordine europeo d'indagine (d.l.gs 21 giugno 2017, n. 108^[3]).

Ha contribuito alla sua diffusione l'enorme sviluppo negli Stati Uniti, anche se la declinazione europea dell'istituto - è appena il caso di notarlo - si distacca molto dal modello americano. Negli Stati Uniti al contrario le operazioni sotto copertura sono assai poco regolamentate, soprattutto quanto ai possibili contenuti, mentre è pacificamente ammesso, e non è mai punibile, il *police incitement*; mentre è l'imputato ad esser ammesso ad eccepire la provocazione attraverso una *entrapment defense*, guadagnandosi nel caso l'assoluzione. In Italia al contrario il legislatore ha un atteggiamento «di rigore»^[4] nei confronti delle *undercover investigations*: una normazione dettagliata, specie quanto alle tipologie delle attività consentite, con la principale preoccupazione di evitare che l'attività dell'infiltrato trasmodi in quella dell'agente provocatore. Più in generale, in tutti i sistemi di *Civil law* sono dettagliatamente disciplinate dalla legge le operazioni consentite, i reati per l'accertamento dei quali possono essere impiegate (reati particolarmente allarmanti, la cui gravità rende tollerabile la flessione degli *standard* di garanzia), le procedure che devono

essere seguite, l'organo, tendenzialmente giudiziario, al quale spetta controllare il rispetto delle regole poste all'organo poliziesco. Questa differente "postura" dei diversi ordinamenti nei confronti delle operazioni sotto copertura ha a che vedere col recente passato degli Stati europei, in cui l'esperienza dei totalitarismi ha lasciato in eredità un diffuso sospetto nei confronti delle manifestazioni di potere delle forze dell'ordine, e queste attività sono associate al controllo sociale, alla repressione del dissenso politico, allo Stato di polizia.

2. Nel nostro sistema sono numerosi i problemi relativi al trattamento processuale delle operazioni *undercover*^[5]; ciò si deve anche al fatto che la disciplina italiana, a differenza di altri omologhi stranieri, è molto attenta a definire i confini della non punibilità delle condotte dell'infiltrato, mentre lo è molto meno alle implicazioni processuali di questa metodica investigativa. Un problema riguarda la loro spendibilità istruttoria: se non pongono particolari questioni la raccolta di prove reali dei reati né l'acquisizione dei relativi proventi (le "consegne controllate" e il "ritardo nei sequestri" hanno costituito la funzione principale delle attività *undercover* già nelle prime figure in materia di traffico di stupefacenti), assai problematico risulta l'apporto dichiarativo dell'agente *undercover* nel processo.

La giurisprudenza ammette la sua testimonianza indiretta sulle dichiarazioni apprese nel corso delle attività. Con lo schermo dell'anonimato (anche per il giudice), a seguito di una novella contenuta nella l. 13 agosto 2010, n. 136: ai sensi del comma 2-*bis* dell'art. 497 c.p.p., nel testo attualmente vigente, gli agenti che siano chiamati a deporre «invitati a fornire le proprie generalità, indicano quelle di copertura utilizzate nel corso delle attività medesime».

E si esclude l'applicabilità all'agente sotto copertura dell'art. 62 c.p.p. che, come noto detta un generale divieto di testimonianza de relato sulle dichiarazioni comunque rese dall'indagato o dall'imputato imputato all'interno del procedimento, perché – dice la Corte di Cassazione – gli agenti *undercover* sono soggetti partecipanti all'azione e non hanno agito nella veste di ufficiali di polizia giudiziaria con i poteri autoritativi e certificatori connessi alla qualifica^[6]. C'è chi distingue tra le dichiarazioni provocate (sulle quali non si può testimoniare) e quelle non provocate: distinzione difficile in pratica, e forse irrilevante ai fini della *ratio* di tutela della libertà di autodeterminazione processuale dell'indagato^[7].

Altro problema è quello del trattamento processuale degli esiti investigativi delle attività condotte violando le regole: fuori dai casi consentiti, senza i controlli previsti, o con modalità tali da trasmodare in vera e propria provocazione. Le norme tacciono sul punto: il legislatore non ha riprodotto una previsione sanzionatoria del tipo di quella prevista per le intercettazioni all'art. 271 c.p.p.; e anche quando la già citata

legge del 2010 ha precisato che la violazione delle regole legali preclude l'operatività dello scudo penale (cosicché l'agente risponde anche penalmente, salva l'applicabilità, in margini assai ridotti, della scriminante dell'art. 51 c.p.) quella novella ha ommesso qualsiasi specificazione in relazione alle sorti processuali del materiale raccolto.

Tutti concordano nell'escludere l'utilizzabilità delle informazioni illegittimamente acquisite, ma non essendovi una traccia espressa di un tale divieto nell'art. 9 l. n. 146 del 2006, la conclusione non è agevolmente giustificabile. Qualcuno fa leva su una nozione di «legge», ai sensi dell'art. 191 c.p.p., estesa anche alle norme penali che l'infiltrato ha violato, e tuttavia una elaborazione dottrinale ormai consolidata ci consente di escludere che le norme penali sostanziali contengano *ex se* regole di esclusione probatoria^[8].

Una diversa ricostruzione – che sottintende l'adesione alla teorica delle “prove incostituzionali” e/o “anticonvenzionali” - rinviene nella illegittimità delle operazioni una violazione del diritto all'equo processo ex art. 6 C.e.d.u. e *dunque* una inutilizzabilità dei relativi prodotti^[9]. Ma questo potrebbe dirsi, al più, per il caso in cui l'attività dell'infiltrato abbia trasmodato un vero e proprio *entrapment*, che può rendere iniquo il processo^[10]; assai più difficilmente in relazione alle operazioni *undercover* effettuate fuori dagli altri presupposti legali (per reati non consentiti, in assenza delle autorizzazioni e così via), per i quali l'eventuale violazione del diritto al rispetto della vita privata (art. 8 par. 2 C.e.d.u.) rende iniquo il processo solo all'esito di una valutazione complessiva del procedimento, che riguarda anche l'attendibilità delle prove reperite e il rispetto delle garanzie difensive^[11].

Più convincente fondare l'inutilizzabilità ex art. 191 c.p.p. delle operazioni sotto copertura eseguite in modo difforme dalle prescrizioni legali - senza scomodare categorie incerte - ravvisando nella normativa sulle operazioni *undercover* un divieto probatorio “indiretto”. All'art. 9 l. n. 146 e alle altre discipline dello strumento possiamo infatti sicuramente riconoscere natura di norme (anche) processuali: attribuiscono un potere investigativo del quale prevedono casi e modi di esercizio. Siccome le operazioni sotto copertura sono attività autoritative pubbliche che non trovano alcuno spazio di legittimazione al di fuori da questi limiti, il mancato rispetto dei presupposti sostanziali e procedurali previsti dalla disciplina di legge determina una situazione di “carenza di potere” che giustifica l'inefficacia dell'atto ossia la sua inutilizzabilità processuale^[12].

La giurisprudenza distingue, nell'ambito delle attività sotto copertura eseguite *contra legem*, tra le ipotesi di “mera” violazione procedurale e quelle in cui le operazioni abbiano costituito condotte di provocazione^[13],

ma si tratta di un distinguo opinabile: se la legittimazione a compiere le operazioni in discorso dipende dall'osservanza delle prescrizioni dettate dal legislatore, sarebbe lecito concludere che il mancato rispetto di ciascuna di esse faccia scattare la sanzione dell'inutilizzabilità^[14].

Esiste poi il problema della rilevanza probatoria delle cose sequestrate nel corso di un'azione sotto copertura illegittima; la giurisprudenza della Corte di Cassazione nega che l'illegittimità dell'operazione sotto copertura possa riverberarsi anche sull'eventuale sequestro, così da privare il relativo oggetto di valenza probatoria laddove questo consista nel corpo del reato o in cosa pertinente al reato: in simili casi vale il noto insegnamento delle Sezioni Unite secondo cui tra l'attività di ricerca della prova e la sua apprensione non intercorre un vincolo di dipendenza giuridica ma soltanto un rapporto di mera successione cronologica; ciò che è suscettibile di sequestro è tale infatti per sue caratteristiche intrinseche normativamente predeterminate – come nel caso di tutto ciò che è pertinente al reato – e non in ragione delle attività attraverso le quali si sia reso possibile il suo ritrovamento, con conseguente impossibilità di propagazione di eventuali vizi da queste a quello^[15].

Esiste infine il problema dell'utilizzabilità delle prove che siano state acquisite attraverso un'operazioni svolta sotto copertura, ma in relazione a reati diversi da quelli per i quali essa è stata disposta e autorizzata: una attività investigativa può sempre offrire modo di acquisire elementi probatori utili (anche o soltanto) per l'accertamento di un reato diverso da quello sotto indagine, non ricompreso nel catalogo dei reati per i quali l'attività è consentita. E proprio nelle operazioni *undercover* sul *web* è particolarmente facile che gli operanti si imbattano in delitti diversi ed ulteriori rispetto a quello da quello oggetto del procedimento: l'infiltrazione in un gruppo *hacker* o il semplice accesso al cd. *dark web* può mettere a contatto l'inquirente con condotte illecite inimmaginabili *a priori*, anche molto diverse da quelle in relazione alle quali l'operazione è stata disposta.

Nell'esegesi offerta dalla giurisprudenza, la legittimità dell'operazione coperta presuppone la configurabilità, in forza di una valutazione *ex ante* – nel momento in cui è adottato il provvedimento autorizzativo – di uno dei reati inclusi tra quelli legislativamente indicati, non potendo determinare l'inutilizzabilità del materiale acquisito l'accertamento, all'esito delle investigazioni, di un diverso delitto: una diversa conclusione, si osserva, sarebbe in contrasto con l'art. 55 c.p.p. e col principio di obbligatorietà dell'azione penale^[16].

In dottrina è stato segnalato, condivisibilmente, come l'inutilizzabilità dovrebbe però essere riconosciuta

almeno in due circostanze: qualora, già *ab initio*, l'ipotesi di reato originariamente formulata presentava carattere meramente strumentale; qualora l'azione *undercover* sia stata portata avanti sebbene l'originaria ipotesi di reato fosse stata ormai messa da parte per manifesta infondatezza e l'unica finalità dell'operazione fosse divenuta ormai quella di acquisire elementi di prova in relazione a reati irrilevanti per l'art. 9 l. n. 146 del 2006; con inutilizzabilità limitata però, in questa seconda ipotesi, ai soli atti acquisiti nella consapevolezza di operare violando il vincolo di scopo posto dal legislatore^[17].

3. Le attività svolte *undercover* nel mondo digitale partecipano, ovviamente, di tutti i profili di delicatezza propri di tutte le operazioni sotto copertura, ma qualche criticità, quando le infiltrazioni avvengono nel mondo digitale, risulta addirittura acuita. Nel nostro ordinamento, infatti, l'istituto è sottoposto a due limiti fondamentali, entrambi facilmente superabili quando si opera sul *web*.

Il primo limite deriva dalla configurazione normativa delle "operazioni" in parola, che sono un "mezzo di ricerca della prova" e non possono essere utilizzate per la ricerca di notizie di reato: esse cioè non possono avere funzione meramente esplorativa e devono inserirsi in un procedimento penale già instaurato, in un contesto che presuppone l'esistenza di un *fumus delicti* e dunque l'avvenuta acquisizione di una *notitia criminis*. Nel nostro sistema, infatti, non sono ricavabili spazi per un impiego di queste attività come strumenti di prevenzione: non a caso l'art. 9 della l. n. 146 del 2006, che contiene oggi lo statuto generale delle operazioni sotto copertura, sia dall'art. 97 del d.p.r. n. 309 del 1990, che in Italia rappresenta la prima configurazione normativa, le descrivono come attività compiute «al solo fine di acquisire elementi di prova» in ordine ai delitti indicati. L'obbligo di comunicare al pubblico ministero le modalità delle operazioni e i relativi risultati, la natura "eccezionale" delle operazioni in parola, le univoche indicazioni provenienti dalla giurisprudenza europea, che vincolano il compimento di tali indagini all'esistenza di una attività criminosa conclusa o in itinere, sono elementi che portano ad estromettere tali operazioni dall'area dell'attività di polizia di sicurezza diretta alla prevenzione dei reati.

E tuttavia, il confine tra prevenzione e repressione è fatalmente destinato ad assottigliarsi: ciò dipende essenzialmente da due fattori. Se uno è legato alla funzionalità dell'istituto ad indagare su crimine organizzato - l'«infiltrazione» di agenti all'interno delle organizzazioni criminali è fatalmente finalizzata (anche) alla ricerca di notizie di reato in relazione alla fisionomia dell'associazione, ai suoi membri, e ai futuri progetti criminali - l'altro è invece connesso, per l'appunto, al contesto digitale delle attività *under cover*.

Per le attività che si svolgono nella realtà digitale è infatti proprio la conformazione di quest'ultima, e il

modo in cui in essa tutti noi ci muoviamo, a favorire le distorsioni applicative: l'inserimento di agenti *undercover* in una *chat-line* mira normalmente e naturalmente a captare informazioni concernenti possibili crimini futuri, più che a reperire elementi di prova riguardo a reati già commessi. È facile allora che l'indagine diventi occasione per testare la propensione criminale delle persone-bersaglio, secondo una metodica che gli americani chiamano *mannna from heaven operations*, nelle quali la polizia lascia in custoditi oggetti di valore in pubblico per tentare i passanti.

Il secondo importantissimo limite dell'istituto delle operazioni sotto copertura riguarda il discrimine tra "agente infiltrato" e "agente provocatore": come ho già ricordato, nel nostro sistema le indagini sotto copertura non possono costituire condotte di provocazione; l'istituto presuppone contegni passivi o comunque produttivi di forme di compartecipazione materiale, mai condotte capaci di ingenerare propositi criminosi che in loro assenza non sarebbero venuti alla luce^[18].

E tuttavia, il confine tra contegno passivo e contegno proattivo, incerto sempre, lo è massimamente quando condotte criminose e atti di indagine si svolgono in uno spazio virtuale. Le metodiche tipiche delle operazioni *undercover* digitali lambiscono infatti costantemente la provocazione: l'attivazione di siti civetta, la realizzazione di aree di sharing la diffusione *on line* di materiale pedopornografico, creano artificiosamente piazze di scambio virtuali in grado di attrarre potenziali criminali conducono i frequentatori di un gruppo o di una piattaforma a scaricarlo, commettendo reato o a caricarne altro a loro volta. Si tratta di attività fatalmente propositive

In più, dobbiamo considerare che, rispetto alle tecniche di infiltrazione tradizionali, l'ambiente digitale potenzia l'efficacia degli adescamenti, perché nel web la percezione dell'illegalità si attenua. I criminologi hanno notato che il cyberspazio influisce sulle modalità percettive e cognitive delle persone, riduce gli ordinari freni inibitori presenti che si attivano nelle relazioni fisiche, contribuendo a sfumare i confini già labili tra conformità, devianza e criminalità; né vale granché adoperare "maschere di deterrenza", che avvisano i navigatori del web che il contenuto del sito è vietato dalla legge.

4. Rispetto a questi profili di delicatezza l'antidoto principale è certamente nella costante controllabilità dell'attività da parte dell'autorità giudiziaria. Va rilevato, a proposito, che il potere di iniziativa spetti normalmente agli organi di vertice delle forze di polizia, ancorché sia necessaria l'autorizzazione del p.m. Fondamentale anche il controllo *a posteriori*, visto che l'agente provocatore si muove fatalmente ai confini della legalità, confini netti in sede di pianificare l'operazione, assai meno nella fase esecutiva. Ma come e

quando è verificabile il rispetto delle indicazioni normative in materia di azioni coperte? Secondo la giurisprudenza se il pubblico ministero ritenga *nelle regole* l'operato dell'agente sotto copertura, non vi è alcuna notizia di reato da iscrivere ex art. 335 c.p.p., in quanto condotta carente di antigiuridicità (si tratta di una esimente, non di una causa di non punibilità). Il pubblico ministero valuta, perciò, autonomamente il comportamento tenuto dall'agente che godrebbe, nei fatti, di una sorta di «immunità procedimentale»^[19]. Con importanti ricadute sul processo: una volta ritenuti superflui gli adempimenti di cui all'art. 335 c.p.p., nel procedimento a carico dei responsabili dei reati «sollecitati», l'agente può essere sentito in veste di persona informata sui fatti, sia, in seguito, in qualità di testimone, e non già quale imputato in procedimento connesso, e alle dichiarazioni vanno applicate le regole di valutazione di cui agli artt. 210 e 192 c.p.p.

Ci sarebbe un'altra soluzione, più complicata ma forse più armoniosa rispetto ai principi del sistema: ritenere ineludibile il vaglio del giudice, già nelle indagini, sulla condotta dell'agente coperto. Il sindacato sull'antigiuridicità della condotta andrebbe sottratto al p.m., che sarebbe in ogni caso tenuto a procedere agli adempimenti di cui all'art. 335 c.p.p. ed alla successiva presentazione di una richiesta di archiviazione. Spetterebbe al giudice investito dell'istanza valutare la posizione dell'agente e, segnatamente, la sussistenza del requisito dell'antigiuridicità delle attività: sarebbe un assetto coerente col ruolo di garanzia del giudice per le indagini preliminari, organo di controllo degli atti di parte^[20].

Un altro correttivo al rischio dell'abuso investigativo è nella descrizione legale, la più accurata possibile, delle attività che è consentito compiere in modo "coperto", che non serve solo a definire l'area dello scudo penale che protegge l'agente infiltrato, ma vale anche a ridurre il rischio di violazioni del principio di proporzionalità. Qui pesa il *deficit* di tipizzazione legale - e prima ancora l'estrema difficoltà di tipizzare - le attività di indagine mascherata consentite nel *web*; difficile trarre un catalogo di attività, ad esempio, dalle previsioni dell'art. 14 comma 2 l. 269/1998 in tema di contrasto alla pedopornografia. Il rischio - è chiaro - è che nel mondo digitale l'istituto delle indagini undercover renda possibili poco controllabili "scorrerie investigative"^[21].

Considerando la decisa espansione dell'ambito applicativo delle operazioni *undercover* anche digitali - si noti che gli ampliamenti dipendono a volte più dalla spiccata utilità dello strumento che dalla gravità del reato^[22] - i profili di criticità fin qui descritti appaiono tutt'altro che trascurabili.

* Contributo tratto dalla relazione svolta nell'ambito del convegno "Per uno statuto dei nuovi mezzi di ricerca della prova di fronte alla società digitale", tenutosi in Roma in data 22.9.2023.

[1] Risale almeno ai *delatori privati* usati dalla monarchia francese per contrastare il dissenso politico (De Maglie, *L'agente provocatore. Un'indagine dommatica e politico-criminale*, Giuffrè, 1991, p. 3 ss)

[2] V. Fanchiotti, voce *Agente sotto copertura*, in *Enc. dir.*, Annali VIII, Giuffrè, Milano, 2015, p. 1 ss. nota come l'istituto abbia subito una sorta di "europeizzazione" in seguito alla sottoscrizione degli accordi di Schengen in tema di consegne controllate e di osservazione transfrontaliera

[3] P. Paulesu, *Operazioni sotto copertura e ordine europeo d'indagine penale*, in *Archivio pen.*, 2018, f. 1, 25

[4] D. Curtotti, *Operazioni sotto copertura*, in *Le associazioni di tipo mafioso*, a cura di B. Romano, Utet, 2015, 431.

[5] Per una accurata ricostruzione anche dell'evoluzione normativa dell'istituto, cfr. L. Ludovici, *L'agente sotto copertura*, in G. Colaiacovo (a cura di) *Sicurezza, informazioni e giustizia penale*, Pacini, 2023, p. 685 ss.

[6] Cass. pen., Sez. II, 22 dicembre 2016 n. 14714, rv. 269670.

[7] L. Ludovici, *L'agente sotto copertura*, cit.. p. 706.

[8] F. Cordero, *Prove illecite nel processo penale*, in *Jus*, 1961, p. 68 ss., ed in *Riv. it. dir. e proc. pen.*, 1961, p. 32 ss., nonché in Id., *Tre studi sulle prove penali*, Giuffrè, 1963, p. 147 ss. Id, *Procedura penale*, IX ed., Giuffrè, 2012, p. 613 ss.

[9] Cass. pen., Sez. VI del 9 febbraio 2022, n. 27160, rv. 283467.

[10] L. Ludovici, *L'agente sotto copertura*, cit.. p. 801.

[11] M. Daniele, *Indagini informatiche lesive della riservatezza. verso un'inutilizzabilità convenzionale?*, in *Cass. pen.* 2013, p. 367 ss.

[12] C. Bortolin, *Operazioni sotto copertura e 'giusto processo'*, in AA.VV., *Giurisprudenza europea e processo penale italiano*, a cura di Balsamo-Kostoris, Giappichelli, Torino, 2008, p. 416.

[13] L'inosservanza degli obblighi comunicativi nei confronti del pubblico ministero e la mancanza delle specifiche autorizzazioni previste dalla legge dall'art. 9 della legge 16 marzo 2006, n. 146 non determinano l'inutilizzabilità in giudizio dei risultati dell'attività investigativa svolta dall'agente infiltrato, «non potendosi ipotizzare patologie invalidanti degli atti processuali non previste dalla legge e non concretando lo svolgimento di attività di indagine prima che ne sia data notizia al pubblico ministero alcuna lesione di diritti fondamentali traduentesi nella violazione dell'art. 6 Conv. EDU» (Cass. pen., Sez. VI del 9 febbraio 2022, n. 27160, cit.) mentre sarebbe inutilizzabile la prova acquisita dall'agente infiltrato che abbia determinato l'indagato alla commissione di un reato (Cass. pen., Sez. 6 f febbraio 2020, n. 12204, rv. 278730).

[14] C. Bortolin, *Operazioni sotto copertura e 'giusto processo'*, cit., p. 416.

[15] Cass. pen., Sez. un., 27 marzo 1996, Sala, in *Cass. pen.*, 1996, p. 3272.

[16] La fattispecie potrà verificarsi con qualche complicazione in più nell'ordine europeo di indagine: cosa accade se l'infiltrazione realizzata per eseguire un ordine emesso dall'autorità italiana per un certo reato conduca alla scoperta di altre fattispecie delittuose non contemplate nell'istanza di collaborazione investigativa? In quel caso potrebbe trovare applicazione l'art. 34 del d.lgs. n. 108 del 2017, che prevede, nell'ambito dello stesso o di altro procedimento, la possibilità di emettere un ordine d'indagine integrativo (P. Paulesu, *Operazioni sotto copertura e ordine europeo d'indagine penale*, in *Archivio pen.*, 2018, p. 3)

[17] L. Ludovici, *L'agente sotto copertura*, cit., p. 759.

[18] Chiara sul punto anche la giurisprudenza della Corte europea: v. per tutti Corte e.d.u., 9 giugno 1998, Teixeira de Castro c. Portogallo, §§ 35-36 e 39, nonché Corte e.d.u., Sez. I, 21 marzo 2002, Calabrò c. Italia e Germania.

[19] P. Paulesu, *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni «sotto copertura», captazione di dati digitali*, in *Riv. dir. proc.* 2010, p. 791

[20] P. Paulesu, *Notizia di reato, cit.*, p. 791.

[21] P. Troisi, *Operazioni digitali sotto copertura*, in A. Scalfati (a cura di) *Le indagini atipiche*, Giappichelli, 2019, p. 634.

[22] Si pensi all'estensione dello strumento, ad opera della l. 9 marzo 2022, n. 22, ai reati di traffico di beni culturali.