INTERCETTAZIONI ED ACQUISIZIONI DI DATI IN SISTEMI INFORMATICI

Roma, Martedì 27 ottobre 2020, Aula Virtuale Teams

REPORT

a cura della Dott.ssa Anna Mauro, Magistrato addetto all'Ufficio del Massimario della Corte

In data 27 ottobre 2020, presso l'Aula Virtuale Teams, ha avuto luogo l'incontro di studio organizzato dalla Struttura della formazione decentrata della Corte di cassazione dal titolo "Intercettazioni ed acquisizioni di dati in sistemi informatici"

Ha introdotto i lavori **il Consigliere della Corte di cassazione Alessandra Bassi, componente della Struttura di formazione decentrata della Corte di cassazione**, la quale ha evidenziato che l'incontro di studio trae origine dall'esigenza di riflettere, sotto prospettive diverse, sugli aspetti maggiormente problematici dell'attuale disciplina delle intercettazioni delle comunicazioni interpersonali che, a seguito dei numerosi interventi normativi in materia, da ultimo la legge 28 febbraio 2020, n. 7 che ha convertito, con modificazioni, il d.l. 30 dicembre 2019, n. 161, costituisce uno dei temi più delicati e controversi del diritto processuale penale contemporaneo. La materia delle intercettazioni richiede un costante aggiornamento e adattamento della disciplina processualistica alla veloce evoluzione degli strumenti tecnologici di investigazione al fine di cercare un punto di equilibrio ragionevole tra l'esigenza di tutelare i diritti fondamentali dell'intercettato, presidiati dalle disposizioni di cui agli artt. 2, 15 e 24 della Costituzione, e le esigenze di carattere generale quali quelle di contrasto alla repressione di reati, alla difesa sociale e al diritto all'informazione dell'opinione pubblica. Il seminario, quindi, si pone l'arduo compito di ricostruire l'intelaiatura normativa di riferimento e di fare il punto sullo stato dell'arte della dottrina e della giurisprudenza in materia all'esito dei plurimi interventi normativi che i sono succeduti nel tempo.

Dopo tale breve intervento introduttivo ha preso la parola **Margherita Cassano, Presidente Aggiunto della Corte di cassazione**, che, da subito, ha messo a fuoco i punti più importati dell'argomento oggetto del convegno sottolineando, innanzitutto, che discutere di intercettazioni significa più in generale interrogarsi sulla professionalità del pubblico ministero e su quella del giudice che è chiamato ad autorizzare, ove ne sussistano i presupposti, il ricorso ad uno strumento di indagine particolarmente invasivo; significa domandarsi quali siano i possibili confini dei rapporti tra pubblico ministero e polizia giudiziaria; significa anche

verificare, alla luce dell'evoluzione del diritto vivente del processo penale, quali siano le cause che hanno reso così centrale e addirittura, a volte, unico il ricorso allo strumento dell'intercettazione; significa poi domandarsi quali siano i margini di effettività nella direzione delle indagini e nell'assunzione di tale attività da parte del pubblico ministero che potrebbe astrattamente svolgerla in prima persona anche se, nella prassi, nella maggior parte dei casi, essa viene delegata alla polizia giudiziaria.

Le recenti modifiche normative della materia - che trovano la loro *ratio* giustificatrice nell'esigenza, fortemente avvertita dal legislatore, di intervenire a causa della divulgazione sempre più accentuata da parte degli organi di informazione del contenuto delle intercettazioni telefoniche e di brani di intercettazioni avulsi dal contesto che possono essere astrattamente lesivi dell'altrui reputazione o contenere la diffusione di dati sensibili - hanno aperto un fronte di riflessione molto più ampio rispetto al passato sia sulle verifiche da parte del giudice e sulla motivazione dei provvedimenti che autorizzano le intercettazioni, sia sulle tecniche di motivazione delle ordinanze del tribunale del riesame e dell'appello delle sentenze dei giudici di primo e secondo grado, sia sull'individuazione degli ambiti del controllo riservato alla Corte di cassazione, sotto il profilo dell'art. 606, lett c) e lett e), cod. proc. pen.

La Presidente Cassano, quindi, ha sottolineato che, nonostante gli intenti perseguiti dal legislatore, molte sono ancora le questioni che rimangono aperte e che costituiscono delle criticità rilevanti. Ed invero, è appena abbozzato e non completamente percorso tutto il profilo che attiene al rispetto pieno dei diritti della difesa e alle possibilità e al ruolo dei difensori fino al momento di selezione da parte del giudice per le indagini preliminari delle conversazioni rilevanti da inserire nel fascicolo delle indagini in quanto il difensore, fino a tale momento, ha solo la facoltà di esaminare e prendere visione degli atti e di ascoltare le registrazioni e prendere cognizione dei flussi delle comunicazioni informatiche o telematiche, ma non può estrarre copia e ottenere una trasposizione su supporto informatico. Tale regime mal si attaglia alle disposizioni di cui all'art. 111 Cost. che assicurano la pienezza del contraddittorio da attuarsi, da subito, nella fase delle indagini. Per tale motivo, ha sottolineato la Presidente, si pone l'esigenza di lettura e coordinamento sistematico, ove possibile, di tale previsione normativa come contenuta nella riforma. Ma non è solo questo l'argomento che merita un approfondimento scientifico apparendo anche di grande interesse e problematicità, e non pienamente preso in carico dal legislatore, tutto il regime contenuto nella riforma in relazione alla gestione dell'archivio riservato delle intercettazioni, che non è più indicato come coperto da segreto con riferimento ai verbali e alle registrazioni, nonché il raccordo che deve porsi tra le disposizioni di cui all' art. 267, 5 co., cod. proc. pen., come modificato, e quelle di cui agli artt. 329 e 114 cod. proc. pen. in tema obbligo di segreto degli atti di indagine e di divieto di pubblicazione e divulgazione, la cui interpretazione strettamente letterale potrebbe portare a ritenere non intensamente tutelata la sfera della riservatezza delle persone e dei dati sensibili che la riforma avrebbe inteso perseguire.

.....

Terzo tema affrontato dalla Presidente è quello che riguarda le intercettazioni non acquisite a seguito della procedura di selezione: la norma, sul punto, non chiarisce nemmeno il luogo in cui tali intercettazioni stralciate dovranno essere custodite e non appare chiaro se debba o meno applicarsi il disposto del decreto ministeriale 20 aprile 2018, emanato in esecuzione della riforma del 2017.

Da ultimo, ma non per interesse, si pone tutta la problematica concernente il captatore informatico. Un primo problema riguarda la collocazione sistematica dell'intervento riformatore: si allude, in particolare, agli art. 266, comma 2-*bis*, 267, co. 1, cod. proc. pen. e 89 disp. att. cod. proc. pen.; nello stesso tempo, a fronte dell'estrema invasività e complessità dell'attività di indagine che il captatore consente, occorre evidenziare che attualmente è regolamentato solo uno dei suoi possibili usi, quale mera modalità di esecuzione delle intercettazioni tra presenti attraverso l'attivazione del microfono dei dispositivi mobili portatili, dando così continuità ideale a quel mezzo di intercettazione ambientale, definito dalle Sez. un. Scurato, "itinerante". L'esperienza, però, insegna che le potenzialità del captatore informatico sono molto più ampie e allora non può che chiedersi in quali rapporti si porrà la nuova disciplina con i principi che sono stati enunciati, in tema di video ripresa di comportamenti comunicativi e non, dalle Sez. un. Prisco e dalla Corte costituzionale con le sentenze n. 135 del 2002 e n. 149 del 2008 e come si potrà garantire una motivazione rafforzata di un provvedimento autorizzativo di questa forma così invasiva di captazione a fronte di presupposti indicati in termini di necessità e non di indispensabilità; in terzo luogo, non può non chiedersi come si porrà questa norma rispetto alle disposizioni di cui all'art. 266, comma 2., cod. proc. pen. in tema di intercettazioni ambientali; ed, infine, rispetto ad un decreto del giudice per le indagini preliminari che indichi il luogo e il tempo in relazione ai quali viene autorizzata l'attivazione di un microfono, occorre chiedersi quali dovranno essere gli elementi forniti affinché il decreto non si risolva in uno stereotipo di provvedimento e quali saranno le conseguenze in caso di discostamento dal paradigma normativo e, infine, se sia applicabile o meno il disposto di cui all'art. 271 cod. proc. pen. in tema di inutilizzabilità.

Altra questione meramente tecnica segnalata dalla Presidente Cassano riguarda l'impossibilità di installare il captatore informatico continuativamente nell'arco delle 24 ore a causa dell'esaurimento delle batterie del dispositivo mobile all'interno del quale il virus è installato: ciò comporta la scelta di un arco temporale all'interno del quale deve avvenire la captazione, scelta che riguarda non soltanto il pubblico ministero che dovrà ricorrere a tale metodo, ma anche il giudice che dovrà autorizzare e, nei successivi gradi, operare un controllo non essendo chiaro quale sarà l'ambito del controllo sulla scelta dell'arco temporale di captazione dei colloqui. Questo è un tema che ha diretto riguardo alla professionalità e soprattutto all'onestà intellettuale del magistrato nello svolgimento delle indagini posto che l'individuazione di un arco temporale più o meno lungo può incidere sulla completezza della ricostruzione di un quadro probatorio e, più ancora, sulla genuinità della ricostruzione di determinati accadimenti.

La Presidente, quindi, ha concluso sottolineando che ciascuna delle questioni evidenziate ha immediato riflesso sulla professionalità di tutti coloro che hanno a

che fare con tale materia poiché essa si intreccia con la tutela di valori costituzionali, quali riservatezza e diritto di difesa, ed è per tale motivo che si gioca la credibilità complessiva della magistratura e della sua professionalità in un momento che richiede più che mai, in ciascun magistrato, la dimostrazione della legittimazione tecnico-professionale affermata solennemente dalla Costituzione.

Terminato l'intervento, ha preso brevemente la parola il **Consigliere Antonio Corbo, componente della Struttura di formazione decentrata della Corte di Cassazione** che, nel ringraziare la Presidente Cassano per il suo intervento, ha sottolineato come esso abbia messo in luce i problemi fondamentali che gli operatori del diritto devono affrontare con la nuova disciplina, che si presenta particolarmente minuziosa e analitica e, per molti aspetti, assai problematica e che richiede una particolare attenzione per la ricostruzione sistematica i cui principi di riferimento sono, essenzialmente, la tutela di diritto di difesa e l'obbligatorietà dell'esercizio dell'azione penale e dell'accertamento dei fatti. In questa prospettiva, nell'organizzare il seminario, è stato ritenuto opportuno partire dall'analisi dei principi fondanti e degli interessi fondamentali che possono essere composti dal legislatore con una certa discrezionalità e, per tale motivo, è stato chiesto al prossimo relatore, Prof.ssa Novella Galantini, di individuare il perimetro fondamentale nel quale si muove l'attività dell'interprete al fine di individuare le soluzioni più corrette da dare alle nuove disposizioni normative verificando, al contempo, gli spazi che restano alla materia delle invalidità e dell'inutilizzabilità, onde individuare ciò che resta fermo, alla luce della rivisitazione di tale complessa disciplina, della giurisprudenza che si è consolidata in materia e cosa invece, oggi, appare superato.

Ha quindi preso la parola la **Prof. Novella Galantini** che ha ricordato innanzitutto quanto sia oggi sempre più importante mettere a fuoco la contrapposizione esistente tra esigenze di accertamento della responsabilità e di efficienza investigativa, da un lato, e di tutela dei diritti fondamentali dall'altro; contrapposizione che esige un bilanciamento attraverso il ricorso a quei principi fondamentali di fonte costituzionale e convenzionale che hanno fissato le linee precise sul piano della legalità e della proporzionalità: il principio di proporzionalità, scritto nella Carta dei diritti fondamentali dell'Unione europea, ma che già con molta lungimiranza la Corte costituzionale aveva individuato in una storica sentenza degli anni 70, quando ebbe a costruire la categoria, ancora non conosciuta, della prova incostituzionale, a cui fece eco, solo nel 1988, il legislatore con l'introduzione della figura dell'inutilizzabilità della prova illegittimamente acquisita; il principio di legalità, sottostante a qualsiasi disciplina che tocchi i diritti fondamentali; il principio di proporzionalità che, nelle sue varie espressioni (adeguatezza, idoneità, stretta necessità), potrebbe oggi valere anche sul piano interpretativo e applicativo tanto da poter parlare di "di proporzionalità giudiziale". Occorre allora chiedersi se, alla luce di tale premessa, l'attuale disciplina normativa, con riferimento anche allo specifico problema del trattamento dei dati, sia o meno adeguata a far fronte alla nuova dimensione tecnologica degli strumenti di accertamento, capace di determinare uno squilibrio

nell'assetto dei rapporti tra i cd. poteri autoritativi e libertà fondamentali che ha indotto parte della dottrina a parlare di "capitalismo della sorveglianza".

La relatrice, quindi, con riferimento all'aspetto delle invalidità degli esiti delle intercettazioni, ha individuato tre fronti su cui ragionare concernenti l'ammissibilità nell'*an* (requisiti di ammissibilità), nel *quomodo* (corretta esecuzione dell'atto) e sotto il profilo del metodo.

Con riferimento al primo punto (inutilizzabilità dell'atto ove eseguito al di fuori dei casi consentiti), la prof. Galantini, pur evidenziando che in merito non sussistono particolari criticità, ha ricordato che una questione di non poco momento è quella collegata alla qualificazione giuridica del fatto, atto riservato al pubblico ministero allorché chiede l'autorizzazione all'intercettazione, posto che, per parte della giurisprudenza, se un'intercettazione è stata chiesta con riferimento ad un'imputazione e non è stata autorizzata, è sufficiente, per ottenere l'autorizzazione, che il p.m. modifichi la qualificazione giuridica, così come è possibile, in sede di riesame, la riqualificazione successiva che consente la conversione dell'inutilizzabilità originaria in utilizzabilità.

Altra questione di grande rilievo attiene all'utilizzabilità delle intercettazioni nei procedimenti diversi. La relatrice, dopo avere ricordato che il tema sarà specificatamente affrontato da altro relatore, ha sottolineato, in ogni caso, che i differenti approcci giurisprudenziali, precedenti alla recente riforma, erano stati ricondotti ad unità dalle Sez. un. Cavallo, secondo cui il procedimento non è diverso quando i reati risultano connessi per un legame di tipo sostanziale e non meramente occasionale o probatorio. La riforma intervenuta successivamente non ha dato una risposta chiara sul punto perché, se dagli atti preparatori emerge la volontà del legislatore di seguire la strada tracciata dalle Sez. un. Cavallo, in realtà non sembra che ciò sia accaduto, tant'è che commentatori hanno ritenuto che "l'uso obliquo delle intercettazioni" sia stato addirittura dilatato attraverso la nuova previsione di cui all'art. 270 cod. proc. pen., nonostante essa abbia introdotto oltre al requisito dell'indispensabilità anche quello della rilevanza.

Altro problema sottolineato è quello che attiene alle norme che hanno riguardo al captatore informatico, posto che l'art. 270 cod. proc. pen., al comma 1-*bis*, fa riferimento all' "utilizzabilità anche per reati diversi", nonostante la rubrica abbia riguardo all' "utilizzazione in altri procedimenti". La relatrice, quindi, ha proposto, al fine di fornire un'interpretazione di siffatte disposizioni, l'applicazione dei principi elaborati dalla Corte costituzionale che, con due sentenze degli anni '90, ha ritenuto possibile l'utilizzabilità *aliunde* purché vi siano i presupposti, ma ha anche stabilito che, in ogni caso, non possono essere ammesse le autorizzazioni in bianco. Tale tema è stato poi ripreso anche dalle Sez. un. Cavallo là dove affermano che il provvedimento autorizzativo del giudice circoscrive l'utilizzazione degli esiti dell'intercettazione ai fatti di reato riconducibili all'autorizzazione medesima che delimita, dunque, l'intervento giudiziale abilitativo, impedendo che esso si trasformi in un'autorizzazione in bianco.

Collegato a siffatto tema è poi quello concernente la legalizzazione successiva dell'intercettazione originariamente non utilizzabile, ossia l'uso postumo della stessa, consentito dalla giurisprudenza della Corte di cassazione quando sia possibile effettuare da parte del giudice un efficace controllo di legittimità.

Sempre con riferimento all'ammissibilità, deve rilevarsi che l'art. 271, co. 1, cod. proc. pen. richiama integralmente le disposizioni di cui all'art. 267 cod. proc. pen. la cui inosservanza comporta l'inutilizzabilità dei risultati delle intercettazioni per cui il provvedimento autorizzativo deve motivare in ordine alla gravità indiziaria da intendersi, in taluni casi, soltanto quale "sufficienza indiziaria" perché essa basta per generare l'ammissibilità delle intercettazioni sul fronte di particolari reati (criminalità organizzata; reati contro la p.a.). Con riferimento alla motivazione del provvedimento autorizzativo, per taluni è sufficiente il richiamo alla richiesta del pubblico ministero, per altri occorre una motivazione *per relationem*, ossia che faccia riferimento alle richieste del p.m. o anche alle relazioni di servizio della polizia giudiziaria, purché il suo *iter* cognitivo e valutativo sia autonomo. Occorre, in ogni caso, che il provvedimento autorizzativo non si esaurisca in una mera formula di stile.

Anche sul piano dell'eseguibilità delle intercettazioni vi sono dei vuoti normativi dal punto di vista sanzionatorio non apparendo chiaro in che termini l'assoluta indispensabilità richiesta dall'art. 267 cod. proc. pen. debba essere resa sul piano della motivazione. Parimenti manca ogni raccordo, sul piano sanzionatorio, con le disposizioni di attuazione (artt. 89 e 89-bis disp. att. cod. proc. pen.) in assenza di qualsivoglia rinvio dell'art. 271 cod. proc. pen. nonostante siffatte disposizioni, oggi, a seguito dei recenti interventi normativi, abbiano un rilievo maggiore rispetto al passato comportando l'osservanza di precisi adempimenti: in particolare, l'art. 89, co. 3 fa riferimento, in relazione alle intercettazioni attraverso captatore informatico, alla "catena di custodia", ma non è prevista alcuna sanzione collegata al mancato controllo e alla mancata attuazione del procedimento di passaggio di dati da una sede all'altra.

Con riferimento al terzo profilo sopra evidenziato, concernente i requisiti di corretta adozione delle metodologie, la relatrice ha specificato che essi non devono intendersi riduttivamente con riferimento alle semplici modalità esecutive, che sono altra cosa rispetto alle metodologie.

Ulteriore questione messa in luce riguarda l'effettiva vigenza delle norme in tema di captatore informatico in quanto la data indicata nel d.lgs n. 216 del 2017 per l'applicazione della riforma, è stata più volte differita.

La fonte normativa espressa del captatore informatico è, per la prof. Galantini, da rinvenirsi nell'art. 4 della Riforma Orlando, entrato in vigore effettivamente dal 1 settembre 2020. Tale affermazione non è pacifica e l'equivoco sull'effettiva vigenza è sorto poiché parte della giurisprudenza ha ritenuto nella specie applicabile l'art. 6 della Riforma Orlando, la cui entrata in vigore (26 gennaio 2018) non è stata rinviata e che ha introdotto delle varianti sul piano dei requisiti di ammissibilità delle intercettazioni con riferimento a particolari gravi reati, attenuando il rigore dei requisiti. A ben vedere, il presupposto per l'operatività del captatore informatico è stato rinvenuto, di fatto, in via giurisprudenziale: ed invero, con la sentenza delle Sez. un. Scurato del 2016, è stata ritenuta possibile, sulla base della caratteristica tipica del captatore informatico individuata nella natura itinerante di tale mezzo di ricerca della prova, l'intercettazione ambientale per reati di criminalità organizzata e, quindi, tale decisione ha dato il via alla possibilità di utilizzo di questo metodo intercettativo tant'è che, successivamente,

la Corte di cassazione, con una sentenza del 2017, ha utilizzato l'art. 266-*bis* cod. proc. pen. quasi che si trattasse di un'intercettazione informatica. Anche prima, però, nel 2009, con la sentenza Virruso (dep. nel 2010), già si era affermato che con tale strumento era possibile captare i dati presenti su un *computer* fisso e non su un portatile e, nel 2016 (sentenza Grassi), è stato ritenuto utilizzabile il captatore per l'acquisizione di altro, ad esempio, dati visibili attraverso la digitazione sulla tastiera, bozze di *mail*, dati presenti nel *computer*. Si è avuta, dunque, un'applicazione inedita del captatore anche prima della vigenza dell'art. 266, commi 2 e 2 bis, cod. proc. pen.

Anche le Sez. un. civili, in sede disciplinare, facendo capo alla sentenza Scurato, hanno ritenuto utilizzabili le intercettazioni con captatore informatico applicando le disposizioni di cui all'art. 6 della Riforma Orlando; a tal proposito ci si è chiesti se tale *dictum* possa avere un riscontro in ambito penalistico e se la giurisprudenza possa essere "creativa" sulla base dei principi generali o se debba attenersi scrupolosamente alla riserva di legge.

Ad oggi, l'impiego del captatore informatico è limitato solo, a norma dell'art. 266, comma 2, cod. proc. pen., alle intercettazioni di comunicazioni tra presenti eseguita su un dispositivo elettronico portatile, ossia ad un'intercettazione vecchio stile effettuata, però, con un metodo diverso e più avanzato e non pare possibile il conseguimento di altre utilità, quali l'acquisizione del traffico di dati, l'attivazione di un microfono, la captazione di immagini, la registrazione di attività. Parimenti non pare possibile l'intercettazione su *computer* fisso e ciò, secondo taluni, in applicazione del principio di proporzionalità, così come non è consentita la video registrazione atteso il dato letterale di cui all'art. 266 co. 2, cod. proc. pen. Le disposizioni normative che si sono succedute in materia, dunque, sembrerebbero non aver apportato nulla di nuovo rispetto a quanto già affermato nel 2006 dalle Sez. U. Prisco e dalla Corte costituzionale nel 2002 e nel 2008 e lasciano ampio spazio a numerose criticità interpretative essendo ancora rimasta in una sorta di limbo la nozione di comportamento comunicativo.

Rimangono, infine, aperte due questioni su cui la giurisprudenza appare divisa.

La prima questione riguarda l'ammissibilità o meno della testimonianza sul contenuto dell'intercettazione. Per la relatrice, in forza del principio di legalità probatoria, non dovrebbe ritenersi consentito che un mezzo di prova possa essere sostituito da un mezzo di ricerca prova.

Altra questione concerne la possibilità di applicare estensivamente la nozione di invalidità derivata, di cui all'art. 185 cod. proc. pen., all'inutilizzabilità. Sul punto, nel 2019, si è pronunciata la Corte costituzionale che ha dichiarato infondata la questione di illegittimità costituzionale dell'art. 191 cod. proc. pen. là dove non prevede l'inutilizzabilità derivata. Per la relatrice non si tratta di applicare estensivamente i principi di cui all'art. 185 cod. proc. pen. sulle nullità ad una diversa figura di invalidità, qual è quella dell'inutilizzabilità, ma piuttosto bisognerebbe guardare alla causa scatenante dell'inutilizzabilità costituita dalla violazione di un diritto probatorio occorrendo che, in un tema così importante, qual è quello delle intercettazioni dove vengono alla ribalta diritti fondamentali della persona, si fornisca un'interpretazione attenta e consona alla delicatezza

della materia rimodulando estensivamente i principi costituzionali in tema di libertà della persona.

Terminato l'intervento della prof. Galantini, ha preso la parola il **Consigliere Cesare Parodi, Procuratore aggiunto presso il Tribunale di Torino** che, chiamato ad illustrare, "**le recenti novità normative in tema di intercettazioni**" ha proposto una lettura di tali disposizioni dall'angolo prospettico dell'inquirente che si appresti ad utilizzare le nuove metodologie per lo svolgimento delle indagini.

Il relatore, dopo aver sottolineato che la riforma non ha risolto tutti i problemi che si ponevano sotto il vigore della vecchia disciplina, ma che ne ha anche aggiunto qualcun altro, ha rilevato che il testo della cd. Riforma Orlando e successive modifiche e quello di cui alla legge n. 7 del 2020 anche se apparentemente simili, sono in realtà profondamente diversi soprattutto perché gli interessi, comunque sempre tutelati, quali tutela della riservatezza, dei diritti della difesa, del diritto di cronaca e dell'efficacia delle indagini, hanno rivestito via via importanza diversa: mentre, infatti, era la riservatezza ad occupare un ruolo di primo piano con la riforma Orlando, nel 2020 sono state meglio calibrate le esigenze di efficacia delle indagini a scapito, in un certo qual modo, della riservatezza e del diritto di difesa che è stato, per alcuni aspetti, concretamente pregiudicato.

Il relatore, quindi, ha messo in luce alcuni problemi pratici, analizzando, in particolare, le circolari operative della Procura generale presso la Corte di cassazione, nonché delle Procure di Milano, Roma e Torino con riferimento, innanzitutto, al ruolo del pubblico ministero e ai suoi rapporti con la polizia giudiziaria.

La riforma ha previsto una specifica funzione di vigilanza in capo al pubblico ministero il quale è tenuto ad assicurare non soltanto la rigorosa selezione delle intercettazioni rilevanti ed utilizzabili, ma anche ad evitare, ex art. 268 co. 2 cod. proc. pen., che siano riportate nei verbali espressioni lesive della reputazione delle persone o loro dati sensibili, salvo che non siano rilevanti per le indagini.

Le intercettazioni rilevanti, poi, devono essere limitate con riferimento alla parte di effettivo interesse della conversazione e ciò perché il legislatore ha voluto evitare l'eccessiva trasposizione su carta delle conversazioni e, quindi, la circolazione delle dichiarazioni non rilevanti. Per tale motivo, come indicato nella circolare della Procura generale, il pubblico ministero è chiamato a fornire alla polizia giudiziaria indicazioni generali calate, però, nelle singole realtà operative e, nei casi dubbi, al fine di garantire l'effettività della vigilanza, la polizia giudiziaria ha l'obbligo di consultare il magistrato anche informalmente al fine di evitare che nei cd. "brogliacci di ascolto" venga documentato il contenuto di conversazioni manifestamente irrilevanti o inutilizzabili. Secondo le indicazioni fornite dalla Procura di Torino, al fine di individuare in che misura debbano essere riportate le conversazioni nelle annotazioni di p.g., è utile il richiamo alla disciplina di cui all'art. 291, co.1-ter cod. proc. pen. che prevede che nelle richieste di misure cautelari "siano riprodotti solo i brani essenziali delle comunicazioni e conversazioni intercettate" e ciò perché, in assenza di una norma specifica che abbia riguardo alle intercettazioni in generale, potrebbe applicarsi il medesimo

principio alle annotazioni. Occorre allora chiedersi cosa debba intendersi per "essenziale"; trattasi, invero, di un concetto che, anche in presenza di assoluta buona fede, appare pur sempre assai opinabile: si pensi, ad esempio, al caso in cui, nel corso dell'indagine e in un momento in cui l'individuazione dei fatti, potenzialmente utili ai fini di prova, è ancora in divenire, si aderisca ad una linea interpretativa che non corrisponde alla realtà dei fatti e che porta a selezionare brani delle intercettazioni che non erano così indispensabili o, invece, ad escludere cose importanti. Sino all'implementazione dei nuovi programmi informatici, la procedura per il rilascio del Registro delle Intercettazioni Telefoniche (RIT) e per tutte le relative annotazioni resta identica a quella in vigore. Il passaggio da un binario essenzialmente cartaceo ad uno essenzialmente telematico non è cosa facile. Le segreterie dei pubblici ministeri, con la collaborazione della polizia giudiziaria assegnata all'ufficio, sino all'elaborazione di uno specifico protocollo con il tribunale, invieranno la "cartellina dedicata" cartacea a mezzo cancelleria centrale e formeranno anche delle cartelline telematiche che verranno quindi inviate al giudice per le indagini preliminari; nel caso di un'annotazione mirata ad una richiesta di proroga che fa riferimento a documentazione anche molto corposa, occorre caricare tutto nelle cartelline telematiche, ma non è chiaro, come sottolineato dal relatore, che tipo di lesione si ponga in essere nel caso in cui ciò non avvenga. La questione che, *prima facie*, potrebbe apparire di scarsa importanza, ha, invece, una rilevanza enorme dal punto di vista operativo perché in alcuni fascicoli non vi sono limiti dimensionali agli atti richiamati. A fronte di tale quesito non risulta fornita una risposta precisa che, però, come auspicato dal Procuratore Parodi, spetterà necessariamente agli studiosi e agli operatori del diritto.

La circolare della Procura Generale presso la Corte di cassazione che, come già sottolineato dal relatore, ha messo a disposizione degli operatori del settore alcune indicazioni di grande importanza, ha affrontato, tra gli altri, il problema di fornire una definizione alla nozione di "bersaglio delle intercettazioni", atteso il silenzio del legislatore. Per taluni, "il bersaglio" è il soggetto intercettato a prescindere dal numero dei dispositivi elettronici oggetto di captazione, mentre è preferibile ritenere, conformemente alle indicazioni offerte dalla Procura generale, che per "bersaglio" si intenda il singolo apparato. Tale opzione interpretativa, che è sicuramente quella più garantista, comporta, però, una serie di ricadute pratiche gestionali di non poco momento. Essa trova il suo fondamento normativo nelle disposizioni di cui all'art. 267, co. 5, cod. proc. pen. là dove si fa riferimento a "ciascuna intercettazione". Ne consegue che nel registro riservato dovrà essere annotato cronologicamente il decreto di autorizzazione, contraddistinto da un numero di R.I.T. per ogni dispositivo o numero di telefono su cui transitano le conversazioni intercettate. In tal modo si garantisce una corretta, univoca e legittima gestione del dato sensibile e operativamente, un immediato riscontro dello stato dell'attività, ai fini del suo trattamento.

Le recenti riforme normative hanno introdotto l'obbligo di "conferimento" immediato, nell'archivio di cui all'art. 269, comma 1, cod. proc. pen., dei verbali e delle registrazioni trasmesse dalla polizia giudiziaria al pubblico ministero al termine dell'attività di intercettazione, comprensiva di ascolto, trascrizione e

redazione dei verbali inerenti alle comunicazioni rilevanti. Il "conferimento" non era previsto prima della riforma e comporta lo spossessamento, da parte della polizia giudiziaria e dei gestori che collaborano con essa, degli esiti delle intercettazioni e la p.g. operante dovrà dare atto di non aver trattenuto copia delle intercettazioni non rilevanti o inutilizzabili e di ogni bozza o minuta di lavoro eventualmente formata. L'immediata trasmissione dei verbali e delle registrazioni priva di fatto la polizia giudiziaria della materiale disponibilità della documentazione per la redazione dell'informativa di reato e, quindi, per garantirle il tempo necessario per tali incombenze e per rielaborare e rivedere gli esiti delle captazioni, il pubblico ministero, come previsto dall'art. 268, co. 5, cod. proc. pen., ove la p.g. chieda di essere autorizzata a conservare l'accesso alle tracce foniche ed ai relativi verbali, potrà chiedere al giudice per le indagini preliminari l'autorizzazione al ritardato deposito delle intercettazioni non oltre la conclusione delle indagini preliminari. Rimane aperto il problema se siffatta autorizzazione debba essere richiesta per i singoli RIT o globalmente al termine delle operazioni. Secondo il relatore, la richiesta andrebbe formulata all'esito delle singole operazioni, ma occorre anche comprendere che cosa debba intendersi per deposito immediato attesa l'astrattezza del concetto di immediatezza ed essendo venuta meno la previgente formulazione del comma 4 dell'art. 268 cod. proc. pen. che prevedeva la possibilità per il pubblico ministero di disporre con proprio decreto il differimento della trasmissione dei verbali e delle registrazioni, stabilendo le prescrizioni utili ad assicurare la tutela del segreto.

Sono tre le opzioni ermeneutiche: secondo una prima interpretazione, la polizia giudiziaria sarebbe onerata ad una sorta di conferimento "globale", all'esito della chiusura di tutte le attività di intercettazione, previa richiesta di ritardato deposito, e ciò proprio al fine di consentirle un'analisi dettagliata di tutto il materiale derivante dall'attività di captazione; secondo altra lettura, al fine di ridurre il tempo nel quale viene concesso alla polizia giudiziaria il possesso esclusivo delle intercettazioni, questa sarebbe tenuta all'immediato conferimento all'atto della trasmissione al p.m. dell'ultimo verbale di chiusura delle intercettazioni nell'ambito del singolo procedimento; per una terza opzione interpretativa, l'immediato conferimento è da intendersi riferito alla chiusura dei singoli bersagli. In questo caso, come nel primo, il p.m. dovrebbe procedere alla richiesta di ritardato deposito e la p.g. dovrebbe essere immediatamente "spossessata" degli esiti delle captazioni. La Procura generale presso la Corte di cassazione, ha ricordato il relatore, propende per la prima interpretazione a favore della quale depone sia il dato letterale - e ciò in quanto l'art. 268, comma 4 richiede l'immediata trasmissione dei "verbali e intercettazioni", così considerando queste ultime, a differenza dell'art. 267, comma 5, cod. proc. pen., unitariamente - sia il dato sistematico in quanto se la normativa persegue lo scopo, in un'ottica di garanzia, di documentare le sole conversazioni utilizzabili e rilevanti, l'oculata selezione delle stesse presuppone necessariamente l'ultimazione degli ascolti. Deve in ogni caso sottolinearsi che non sono previste sanzioni nel caso di ritardato conferimento della polizia giudiziaria e, pertanto, siffatto ritardo potrà rilevare semmai sotto il profilo disciplinare, ma non influirà sulla valenza probatoria degli esiti delle captazioni. E' questo, come osservato dal

relatore, un problema aperto su cui dovranno confrontarsi giurisprudenza e dottrina.

Il procuratore Parodi, quindi, è passato ad esaminare il rapporto tra misure cautelari e intercettazioni. La cd. riforma "Orlando", che aveva apportato modifiche anche alla disciplina del procedimento cautelare, non è stata radicalmente mutata anche se sono stati apportati dei correttivi importanti dal punto di vista operativo.

La legge n. 7 del 2020 ha modificato l'art. 291 cod. proc. pen. precisando che le intercettazioni richiamate in una richiesta di misura cautelare devono essere "comunque conferite nell'archivio digitale di cui all'art. 269" previa precisa indicazione dei RIT e dei progressivi utilizzati. Secondo tale disposizione, quindi, il pubblico ministero, nel formulare al giudice per le indagini preliminari la richiesta di misura cautelare, deve selezionare, tra gli esiti delle intercettazioni confluite nell'archivio, quelli che ritiene rilevanti ai fini della richiesta, trasmettendo i verbali delle operazioni contenenti le trascrizioni sommarie, ma non anche le tracce foniche delle captazioni che potranno, eventualmente, essere ascoltate dallo stesso giudice, al fine di valutare la richiesta, accedendo presso le apposite sale d'ascolto. Ovviamente tale procedimento implica la predisposizione di un elenco preciso al fine di meglio comprendere cosa sia utile, ai fini della richiesta, trasmettere al giudice. L'art. 291, co. 1-ter, cod. proc. pen. dispone che nella richiesta di misura cautelare il p.m. riproduca solo i brani delle comunicazioni e conversazioni intercettate ritenute rilevanti e utilizzabili. La scelta del legislatore è quella di ridurre l'indicazione del minimo indispensabile. Ciò comporta dei rischi non solo per la difesa, che avrà a disposizione il materiale indicato nella richiesta al momento dell'esecuzione della misura, ma anche per il p.m. perché la difesa potrebbe fornire elementi utili per meglio dare una lettura globale alla vicenda.

Il d.l. n. 161 del 2019 ha abrogato i periodi terzo e quarto dell'art. 293 cod. proc. pen. eliminando così la disciplina del rilascio di copia del materiale intercettativo utilizzato per la misura cautelare. Si è venuto quindi a creare un vuoto normativo che comporta non pochi problemi, che si sarebbero potuti evitare, apparendo siffatte disposizioni in contrasto con quanto stabilito dalla Corte costituzionale che, con la sentenza n. 336 del 2008, riconosce al difensore il diritto di ottenere copia delle registrazioni delle conversazioni poste a base della misura cautelare, indicazioni queste che, nonostante il silenzio della legge, debbono essere eseguite. Il difensore potrà ottenere la trasposizione delle fonie su idoneo supporto, previa specifica autorizzazione del P.M. procedente.

Come si è detto, dopo il deposito, sia esso ritardato o meno, ai difensori delle parti, a norma dell'art. 286, comma 6, cod. proc. pen. è immediatamente dato avviso che entro il termine fissato hanno la facoltà di esaminare gli atti e ascoltare le intercettazioni, per via telematica, ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche. Scaduto il termine per esame, il giudice dispone l'acquisizione delle conversazioni e dei flussi di comunicazioni indicati dalle parti che non appaiono irrilevanti, disponendo contestualmente lo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione e di quelle che riguardano categorie particolari di dati personali, sempre che non ne sia dimostrata la rilevanza. La procedura di selezione in passato non era un sistema

praticato ed efficace e, in assenza di sanzioni, era evitabile. Il ruolo primario della tutela della riservatezza dovrebbe far assurgere la procedura di selezione ad un livello primario. La nuova procedura di selezione ipotizzata dal legislatore - che comporta la scomparsa delle intercettazioni non utilizzabili, che devono essere conferite definitivamente all'archivio delle intercettazioni, e l'acquisizione al fascicolo del p.m. della intercettazioni utilizzabili per le determinazioni inerenti l'esercizio dell'azione penale - nella pratica, per il relatore, poco ha modificato rispetto alla previgente disciplina in quanto i pubblici ministeri continueranno ad operare la loro selezione prevalentemente al momento della chiusura delle indagini preliminari (art. 415-*bis* cod. proc. pen.). Di ciò è consapevole, in certo qual modo, anche la Procura generale che, nell'indicare, nella propria circolare, i vari momenti di selezione, li pone tutti sul medesimo piano. Se nella pratica, dunque, la procedura di cui all'art. 415-*bis* cod. proc. pen. e quella per il giudizio immediato sono quelle prevalenti, diviene molto importante seguire le prescrizioni della Procura generale che richiedono, pertanto, per la predisposizione degli elenchi delle intercettazioni - che non potranno essere più omessi - la maggiore completezza ed esaustività possibile al fine di consentire una precisa individuazione delle conversazioni rilevanti. Tali elenchi, quindi, dovranno essere completati prima della notifica degli avvisi ex art. 415-*bis* cod. proc. pen. perché solo in tal modo si ha la garanzia che esclusivamente quanto indicato come rilevante sarà utilizzato in una precisa direzione.

In ultimo il relatore, omettendo per questioni di tempo la trattazione di tutte le altre questioni trattate nelle *slide* da lui predisposte e a cui ha fatto rinvio, ha ritenuto di dover soffermare l'attenzione solo su altre due questioni.

La prima concerne un profilo organizzativo di grande rilievo: il cd. *back up* dei dati. Dopo il conferimento all'Archivio digitale delle intercettazioni e verificata da parte del personale preposto la corretta esportazione e la funzionalità degli ascolti, il gestore, su disposizione del pubblico ministero, procederà alla cancellazione definitiva dai propri *server* delle registrazioni e dei verbali, interrompendo il collegamento alla postazione di ascolto da remoto; si pone, quindi, il problema di evitare il rischio di un'irreversibile cancellazione e perdita dei dati essendo esigenza prioritaria, come indicato nella circolare della Procura Generale che richiama a tal proposito il dettato dell'art. 89, co. 4, disp. att. cod. proc. pen., quella di garantire la corretta conservazione della fonte di prova.

Altra questione su cui il relatore ha richiamato l'attenzione e più ampiamente esaminata nelle *slide*, è quella che riguarda le disposizioni in tema di captatore informatico che tradiscono una certa ritrosia del legislatore il quale, non potendosi esimere dal disciplinare tale mezzo di ricerca della prova, ha comunque voluto differenziarne l'uso a seconda che si abbia riguardo ai reati di criminalità organizzata (in relazione ai quali è sempre consentito) o a quelli contro la pubblica amministrazione, per i quali è richiesta la preventiva indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'art. 614 cod. pen. Si avverte, da tali previsioni normative, il timore del legislatore che possano essere utilizzate formule di stile, rischio che certamente sussiste in quanto le motivazioni per l'utilizzo del captatore, che facilita enormemente le indagini, sono, per tale ragione, quasi *in re ipsa*.

Ha preso quindi la parola il **Consigliere Corbo** che, dopo aver ringraziato il relatore per la panoramica generale della nuova disciplina e della sua operatività complessiva, ha introdotto il successivo relatore, **Giuseppe Santalucia, Consigliere della Corte di cassazione**, chiamato ad intervenire sull'“**Utilizzabilità dei risultati delle intercettazioni in altri procedimenti**”, argomento su cui, come ricordato dal Consigliere Corbo, sono intervenute prima le Sez. U. Cavallo, che hanno risolto il contrasto tra le decisioni delle Sezioni semplici in modo abbastanza rigoroso, e successivamente la legge n. 7 del 2020 che sembrerebbe consentire un più ampio recupero delle attività delle intercettazioni, lasciando comunque spazio a numerosi dubbi interpretativi.

IL contributo del **Consigliere Santalucia** ha avuto ad oggetto essenzialmente le disposizioni di cui all'art. 270 cod. proc. pen. il cui testo originario è stato riformato dal d.l. n. 161 del 2019 convertito, con modificazioni, dalla legge n. 7 del 2020. Tale decreto legge aveva lo scopo dichiarato di risolvere alcuni nodi che la cd. riforma Orlando aveva posto, nella pratica, benché tale riforma si fosse occupata dell'art. 270 cod. proc. pen. - che disciplina l'uso degli esiti delle intercettazioni “in altri procedimenti” - solo inserendo il comma 1-*bis* con riferimento ai risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile, nell'ottica di restringere, quanto più possibile, i risultati delle intercettazioni da “trojan” in ragione della particolare invasività di tale strumento. La riforma Orlando ha stabilito che gli esiti di tali captazioni non possono essere utilizzati per la prova di reati, anche connessi, diversi da quelli per i quali è stato emesso il decreto di autorizzazione, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza e ha utilizzato un criterio di restrizione di utilizzabilità probatoria facendo riferimento alla nozione di diverso reato, così validando il criterio selettivo che l'art. 270, comma 1, cod. proc. pen. contiene invece per tutta la trasmigrazione dei risultati intercettativi in altro procedimento per le intercettazioni non derivanti da captatore informatico. Tale riforma ha quindi imposto, con riferimento alle intercettazioni con captatore informatico, il criterio selettivo del “diverso reato”, così estendendo, dai “procedimenti diversi” ai “diversi reati”, l'operatività della clausola di esclusione dell'utilizzabilità del materiale raccolto a mezzo intercettazioni. Nelle more della maturazione del termine per l'efficacia del citato comma 1-*bis*, si sono occupate della questione, con la sentenza n. 51 del 28/11/2019, (dep. 2020), Cavallo, le Sez. un. il cui intervento, reso necessario, ad avviso di parte della dottrina, per la vaghezza del termine “procedimento”, sarebbe da considerare espressione non tanto di un'attività interpretativa del diritto, quanto piuttosto di un'attività creativa. Per il consigliere Santalucia, il termine procedimento non è poi così vago in quanto le nozioni di “diverso reato” e di “diverso procedimento” scontano una caratura processuale: quando si parla di reato non ci si riferisce a qualcosa di molto diverso dalla nozione processuale di procedimento perché il reato non va inteso nel suo accadimento storico, non è la condotta nel tempo e nello spazio, ma è da

considerarsi quale proiezione ipotetica, sul piano processuale, di quel tipo di condotta. In tal modo, le differenze dal punto di vista qualitativo tra reato e procedimento si assottigliano: la nozione di "diverso reato" ha una dimensione processuale pari a quella di "diverso procedimento".

Il relatore ha quindi proseguito nell'analisi dell'art. 270, come consegnato dalla legge del 2020 che non ha modificato il testo di cui al comma 1-bis, su cui era intervenuto il d.l. n. 161 del 2019, ma ha operato sul comma 1.

Il comma 1-*bis*, già contenuto nella legge 23 giugno 2017, n. 103 (cd. riforma Orlando che aveva un campo di operatività molto limitato dalla legge di delega e che era stata criticata per non avere preso posizione sulla nozione di diverso procedimento), ha poi patito numerosi interventi normativi e da ultimo la decretazione di urgenza del 2019. Quest'ultimo decreto, innanzitutto, ha ribaltato la struttura dell'art. 270, comma 1-*bis* utilizzando una formula che, al contrario della precedente, più attenta al divieto ("i risultati delle intercettazioni tra presenti operato con captatore informatico ... non possono essere utilizzati ..."), sembra aprire alla possibile utilizzazione del *trojan* anche per la prova di reati diversi da quelli per vi è stata autorizzazione purché risultino indispensabili per l'accertamento dei reati indicati nella norma. Tale comma inizia con "fermo restando quanto previsto dal comma 1 ..." e, ad una prima lettura, sembrerebbe che il legislatore abbia inteso considerare la disposizione in esso contenuta, che si riferisce all'intercettazioni a mezzo *trojan*, quale norma di completamento rispetto alla disciplina del comma 1. Per il Consigliere Santalucia, però, siffatta interpretazione non appare condivisibile in quanto l'utilizzo della prova per reato diverso è una formula di restrizione che sostituisce quella di procedimento diverso utilizzata al primo comma e, quindi, appare difficile ritenere che una norma di completamento possa introdurre un divieto di maggiore selezione ed avere, al medesimo tempo, siffatta natura. Essa è, invece, una norma meramente sostitutiva, da leggere senza l'inciso iniziale e da interpretarsi, nonostante la modifica del testo da divieto a formula permissiva, come espressione della volontà del legislatore di restringere l'utilizzo dei risultati da intercettazione da *trojan* in considerazione della portata particolarmente intrusiva di tale mezzo tecnologico nella libertà di comunicazione.

Almeno fino all'ultimo intervento della legge di conversione, "l'indispensabilità", a cui fa riferimento il primo comma dell'articolo in commento, era limitata ai delitti con arresto obbligatorio; con l'intervento della legge di conversione, invece, si ha riguardo a tutti i reati indicati nell'art. 266, comma 2-*bis*, cod. proc. pen. ossia a tutti quei reati che, pur compresi nelle disposizioni di cui all'art. 266, comma 1, cod. proc. pen., giustificano un uso meno limitato da intercettazione con *trojan* in ambiente domiciliare senza la restrizione dell'attualità della condotta criminosa e che, con riferimento ai delitti dei pubblici ufficiali e agli incaricati di pubblico servizio, richiedono anche, per giustificare l'uso del captatore informatico, "la necessità".

Sul comma 1 dell'art. 270 cod. proc. pen., secondo il relatore, il legislatore è intervenuto non già per rimediare ad un'asserita insufficienza della riforma Orlando, che mai, sostanzialmente, è entrata in vigore viste tutte le proroghe, ma al fine di reagire ad una presa di posizione della giurisprudenza delle Sez. un. con

la sentenza Cavallo. Ed invero, un intervento normativo così celere induce inevitabilmente a pensare ad una legislazione di reazione perché altrimenti sarebbe stato più ovvio non modificare una norma non interessata dalla riforma Orlando. Dopo alcuni emendamenti che avevano sostituito la nozione di diverso procedimento con quella di diverso reato, si è poi ritornati al criterio selettivo di diverso procedimento: il risultato che ci consegna il legislatore è, dunque, quello di un incremento del criterio qualitativo del dato intercettativo per poter trasmigrare, nel senso che esso non deve essere solo indispensabile, come richiesto in precedenza, ma anche rilevante. Inoltre, si guarda all'accertamento nel diverso procedimento dei delitti per i quali è obbligatorio l'arresto in flagranza e dei reati di cui all'art. 266, comma 1, cod. proc. pen.

Soffermando l'attenzione poi sulle nozioni di "rilevante" e "indispensabile", il relatore ha osservato, innanzitutto, che è indispensabile solo ciò che è rilevante, ma non sempre ciò che è rilevante e anche necessariamente indispensabile e, pertanto, qualora tali termini dovessero essere letti come un'endiadi, l'intervento di interpolazione del legislatore dovrebbe ritenersi inutile poiché l'indispensabilità non è altro che una rilevanza rafforzata. Rilevante è il dato probatorio che serve a provare il reato, ma non è così necessario perché la prova di quel reato può essere formata anche altrimenti.

I delitti per i quali è consentita la trasmigrazione probatoria, a seguito degli ultimi intervenuti normativi, sono quelli per i quali è obbligatorio l'arresto in flagranza, (già contemplati) e i reati elencati nell'art. 266, comma 1, cod. proc. pen. per i quali, dunque, la legge consente l'intercettazione. Come già ricordato dalle Sez. U. Cavallo, l'utilizzazione per i reati diversi da quello oggetto di decreto di autorizzazione, presuppone che il reato diverso sia un reato per il quale la legge consente l'ammissibilità dello strumento intercettativo. Non si può, secondo le Sez. U, pensare alla possibilità di utilizzare diversamente il dato intercettativo, non tanto per il divieto di cui all'art. 270 cod. proc. pen., ma perché l'intercettazione è utilizzata fuori da un caso previsto dalla legge e la sanzione di inutilizzabilità sembra, quindi, derivare piuttosto dalla previsione di cui all'art. 271 cod. proc. pen. Orbene, il legislatore della legge di conversione estende questo pronunciamento delle Sez. un. espressamente all'art. 270 cod. proc. pen. e stabilisce che i reati che beneficiano della trasmigrazione probatoria sono quelli di cui all'art. 266, comma 1, cod. proc. pen. facendo così saltare quel criterio di cauta restrizione dei commi 1 e 2 dell'art. 270 cod. proc. pen. che, nell'originaria versione di cui alla riforma Orlando, si riferivano ai reati di maggior allarme sociale quelli, cioè, di cui all'art. 380 cod. proc. pen. (per i quali è previsto l'arresto obbligatorio in flagranza) e apre a tutti i reati intercettabili. Per il relatore occorre allora, al fine di dare un senso alle modifiche intervenute con la legge del 2020, effettuare un'operazione di ortopedia normativa e ritenere che il criterio della rilevanza sia riferito ai delitti per i quali è obbligatorio l'arresto in flagranza, mentre quello dell'indispensabilità ai delitti di cui all'art. 266, comma 1, cod. proc. pen: poiché la trasmigrazione del dato intercettativo è un evento eccezionale, il risultato delle intercettazioni "rilevante" può trasmigrare nel procedimento *ad quem* se si tratta di provare un reato di grande allarme sociale; se, invece, si tratta di provare un reato a minor tasso di gravità occorrerà che l'esito delle

intercettazioni sia indispensabile al suddetto fine, ossia, che abbia una maggiore intensità probatoria.

Si potrebbe, quindi, giungere alla conclusione che, nel medesimo procedimento, il legislatore, *a contrario*, consenta l'utilizzabilità del dato intercettativo legittimamente acquisito, perché fondato su decreto del giudice adeguatamente motivato, anche per la prova di reati non contemplati nel catalogo di cui all'art. 266, comma 1, cod. proc. pen. L'art. 270 cod. proc. pen., in altri termini, andrebbe letto quale disposizione normativa che introduce un criterio limitato al campo operativo a cui essa ha diretto riguardo (ossia ai diversi procedimenti).

Seguendo l'impostazione interpretativa delle Sez. un., che fanno un uso massiccio del principio di proporzionalità in materia di prova occorre, quindi, avere riguardo all'adeguatezza motivazionale del decreto su cui non solo si fonda la legittimità dell'operazione di intercettazione, ma che circoscrive anche l'area di utilizzabilità futura degli esiti delle intercettazioni. Conclusione questa che, al relatore, non pare così scontata poiché il decreto motivato di autorizzazione, che è sicuramente strumentale alla legittimità dell'operazione intercettativa, non necessariamente deve ipotecare il futuro momento dell'utilizzabilità probatoria che non deve essere, quindi, valutata attraverso le disposizioni di cui all'art. 266 cod. proc. pen. Si potrebbe allora pensare che il legislatore del 2020 abbia voluto aprire all'utilizzazione degli esiti intercettativi nel medesimo procedimento, affrancata dalla necessità del rispetto delle disposizioni di cui all'art. 266, comma 1, cod. proc. pen. Questa operazione, però, non sarebbe accoglibile senza critiche poiché, per il principio di proporzionalità, l'imposizione di un sacrificio ai diritti fondamentali della persona si può giustificare solo alla luce dell'importanza dell'acquisizione. Se il reato non è di tale gravità, allora potrebbe venire meno il principio di proporzionalità in senso stretto.

Si tratta allora di capire cosa deve intendersi per medesimo o diverso procedimento. Per le Sez. un. Cavallo non vertiamo in tema di diverso procedimento se i reati sono connessi e guarda alla connessione come ad un legame sostanziale tra reati che consente di affermare che il reato connesso a quello direttamente oggetto del provvedimento autorizzativo è in qualche modo interessato da quest'ultimo proprio per il legame sostanziale che lo lega al reato oggetto del provvedimento. Fa anche riferimento ad una sorta di vaghezza della nozione di procedimento che, però, come si è detto, non trova pienamente d'accordo il relatore il quale, dopo avere evidenziato che indubbiamente il legislatore distingue reato da procedimento, ha notato che è dalla legge stessa che possono ricavarsi le differenze: ed invero, se si guarda alla nozione di procedimento che ci consegnano gli artt. 17 e 18 cod. proc. pen. alcune incertezze su tale nozione verrebbero meno in quanto l'art. 18 fa riferimento ai processi legittimamente riuniti e allora sarebbe possibile ritenere che si ha medesimo procedimento nei casi indicati dall'art. 17 il quale fissa dei paletti ben precisi perché si possa avere un processo cumulativo ed essi sono costituiti dalla connessione e dai casi previsti dall'art. 371, comma 2, lett. b) cod. proc. pen.

Le Sez. un. Cavallo valorizzano il legame sostanziale ma, per il relatore, la connessione va riguardata con riferimento al dato processuale e, quindi, le differenze fra gli artt. 12 e 371, co 2, lett. b), cod. proc. pen., pur non venendo

annullate, si riducono perché il legame forte di cui all'art. 12 è sempre un legame di accertamento perché si ha riguardo ad esigenze di tipo probatorio, identiche a quelle sottese alle disposizioni di cui alla riunione dei processi ex art. 371, comma 2, lett. b) cod. proc. pen. Il relatore ha, infine, sottolineato che anche se il sistema consentirebbe una risposta, la prassi processuale ha modellato il sistema in quanto non è difficile verificare che il pubblico ministero ha spesso gioco facile nel creare procedimenti cumulativi superando il dato normativo. In tale situazione, ha quindi concluso, la soluzione delle Sez. U. e, cioè, la limitazione al vincolo della connessione, anche se potrebbe apparire non la più corretta dal punto di vista teorico, è sicuramente quella più utile e opportuna.

Terminato l'intervento del Consigliere Santalucia, ha preso la parola il **Consigliere Bassi** che, nel ringraziare il relatore per la lettura analitica e problematica dell'argomento trattato, si è chiesta fino a che punto le affermazioni di principio delle Sez. un. possano ritenersi ancora valide dopo l'intervento del legislatore del 2020 in quanto il richiamo operato dall'art. 270 cod. proc. pen. all'art. 266, comma 2, lett b), cod. proc. pen., potrebbe essere considerato assorbente rispetto ad ogni altro criterio selettivo e consentire il superamento del concetto di connessione sì da poter postulare l'intercettabilità autonoma prescindendo dalla connessione tra reati e, quindi, dal concetto di procedimento più o meno coincidente con quello di reato, a condizione che sussista l'autonoma intercettabilità del reato in relazione al quale il dato probatorio acquisito con l'intercettazione si intende utilizzare. Questa impostazione del legislatore consente, per certi aspetti, anche un'applicazione più facile della regola processuale e permette la trasmigrazione o meno del dato probatorio nel diverso procedimento o anche nel medesimo procedimento a condizione che sussista l'autonoma intercettabilità. Tale soluzione normativa tranquillizza anche sotto il profilo di possibili scelte strategiche dell'accusa, scongiurando che attraverso il "gioco delle iscrizioni", si possa condizionare l'utilizzabilità di un mezzo di ricerca di prova assai invasivo come quello intercettativo.

Seguendo l'ordine dei lavori, è quindi seguito l'intervento del **Sostituto Procuratore generale presso la Corte di cassazione Luigi Cuomo** dal titolo "**Acquisizione dei dati in sistemi informatici e telematici tra intercettazioni, perquisizioni e sequestri**". Il relatore ha esordito affermando che ogni indagine penale viene compiuta o con l'esecuzione di intercettazioni o con l'acquisizione di dati informatici e che, pertanto, il *computer* è soggetto o oggetto del reato o testimone dello stesso in quanto conserva la prova dei dati ricevuti o trasmessi.

Ogni conversazione è cifrata e digitalizzata; il flusso delle comunicazioni viene captato con linguaggio binario e, quindi, non si tratta di informazioni vocali immediatamente comprensibili.

Tutto ciò nasce nell'epoca moderna con la crittografia di massa ossia la scienza che si occupa dell'elaborazione di sistemi di scrittura segreti o, in generale, di comunicazioni progettate per essere intelleggibili solo per chi ne possiede il codice. Essa, quindi, assicura con certezza l'autenticità della comunicazione, impedisce

che terzi si sostituiscano al mittente o si impadroniscano di informazioni riservate e garantisce l'epoca delle trasmissioni telematiche. Una prima questione da esaminare concerne la sussistenza o meno del diritto di accesso agli algoritmi di cifratura da parte della difesa o comunque dei soggetti interessati al processo.

I vari sistemi informatici utilizzano differenti algoritmi (ad esempio, *Whatsapp* usa un determinato sistema di cifratura, *Telegram* ne usa un altro, *Messenger* e *Facebook* altri ancora) e, pertanto, non esistendo una chiave di lettura uguale per tutti i sistemi, ossia un algoritmo crittografico univoco, anche il possesso di un algoritmo non consente comunque di captare altri *social*. Esistono poi ulteriori strumenti che rafforzano la tutela della *privacy*: ad esempio, l'aggiunta di una *password* in più o di funzionalità che comportano l'autodistruzione delle *mail* dopo pochi secondi; l'utilizzo di *mail* criptate che sono mandate e rimandate a *server* che si trovano nei paradisi fiscali e che, in quanto cifrate e come se fossero dei messaggi in busta chiusa; ancora, tutte le conversazioni su *Skype* che non si riescono ad intercettare se non si ha la disponibilità di un captatore molto complicato; la navigazione anonima (*rectius* privata), molto facile da impostare, che non permette di andare a investigare su cosa accade nel cd. *deep web* (ossia il web sommerso non indicizzato dai normali motori di ricerca) o che consente di nascondersi, senza lasciare tracce della navigazione, mentre si utilizzano alcuni siti, ad esempio, pedo-pornografici.

Ulteriori difficoltà sono da ricondursi al fatto che a volte il captatore non è utilizzabile poiché non sempre si ha a che fare con delitti che consentono l'uso di un mezzo di ricerca della prova avente tale forza invasiva; in altri casi, più semplicemente, il captatore o non è disponibile o è eccessivamente oneroso (si pensi, ad esempio, che per ogni aggiornamento del sistema operativo, serve un nuovo captatore). La polizia giudiziaria, inoltre, solo nel caso in cui il gestore del servizio fornisca assistenza, può accedere a *cloud* e fare copia delle informazioni contenute in un telefonino. Altra difficoltà che si incontra è quella che attiene alla captazione di informazioni che si trovano su un *server* all'estero poiché in tal caso non sempre è facile individuare la legge applicabile se, cioè, essa sia quella nazionale della società che gestisce il servizio oppure quella del luogo dove è allocato il *server* e se serva in ogni caso una rogatoria. Numerosi sono poi i profili di criticità nell'acquisizione dei dati. L'algoritmo è spesso oggetto di privativa industriale e la politica aziendale di tutela della sicurezza dei dati spesso non consente la collaborazione.

L'algoritmo di decifratura, inoltre, non va a modificare il contenuto dei dati (è come se fosse una formula matematica), e la giurisprudenza, a partire dalla sentenza n. 5818/2015, Rv. 266267 della Sezione Terza della Corte di cassazione, in materia di *blackberry*, ha elaborato un insieme di regole in materia di cifratura e decifratura dei dati, affermando che legittimamente la polizia giudiziaria può avvalersi delle società che gestiscono questi servizi da considerarsi alla stregua di ausiliari tecnici la cui attività di "messa in chiaro" dei dialoghi captati rientra nei comportamenti di quotidiana cooperazione con l'autorità giudiziaria che risulta perfettamente coerente con la disciplina processuale di acquisizione dei documenti e dei dati (come, ad esempio, avviene per l'acquisizione dei tabulati telefonici).

Guardando la tematica in esame dall'angolo prospettico del difensore, ci si è chiesti come possano fare i difensori per controllare che le procedure di decriptazione delle conversazioni siano corrette. Sul punto, una sentenza della Corte di cassazione (Sez. 6, n. 14395/2018, Rv. 275534) ha affermato che, in tema di intercettazioni di flussi comunicativi, l'indisponibilità dell'algoritmo utilizzabile per la decriptazione dei dati informatici non determina alcuna lesione del diritto di difesa, atteso che l'interessato può avvalersi della procedura prevista dall'art. 268, commi 6 e 7, cod. proc. pen. per verificare il contenuto delle captazioni, ma non può anche pretendere un controllo diretto mediante l'utilizzo esclusivo e non mediato del programma di decriptazione. In altri termini, ci sarà un momento necessario nel processo in cui la difesa e, in particolare, l'imputato (che è l'autore dei messaggi) potranno mostrare che c'è discrasia tra quanto è stato decrittato e quanto ha effettivamente scritto o detto. I difensori, quindi, potranno ottenere il dato criptato a monte (ossia la sequenza numerica) e la comunicazione decifrata, ma non l'algoritmo, ossia la modalità con cui si è pervenuti al dato criptato. Sul punto, però, ha ricordato il relatore, è dato registrare una recente sentenza della Corte di cassazione di segno contrario (Sez. 4, n.49896/2019, rv. 277949-03) che ha ritenuto nulla, ex art. 178, lett. c), cod. proc. pen., la procedura di decifrazione svolta dal fornitore del servizio fuori dal contraddittorio, ove non si metta a disposizione della difesa l'algoritmo. Tale decisione, che non ha avuto ricadute concrete in quanto il processo si è svolto con il rito abbreviato, pur da apprezzare per il suo sforzo garantistico, non viene condivisa dal relatore in quanto, qualora si dovesse consegnare l'algoritmo alla difesa, questo diventerebbe pubblico e, pertanto, si rischierebbe di non avere più alcuna collaborazione del gestore del servizio. Si rileva, inoltre, che l'utilizzo del sistema di cifratura non determina alcuna modifica del contenuto dei messaggi, neanche nell'ipotesi di errore nell'operazione di messa in chiaro del flusso comunicativo.

Il Procuratore Cuomo, quindi, ha proseguito fornendo alcune specificazioni sulle più comuni modalità di criptazione, esponendo che la tutela della riservatezza dell'utente può essere garantita nelle conversazioni in *chat* mediante l'inviolabilità del *server* (crittografia *Pin to Pin*) o l'inviolabilità del dispositivo (crittografia *end to end*). Quando è adoperata la modalità di criptazione *pin to pin* (piattaforma *Blackberry*), gli utenti utilizzano un *software* di messaggistica che cifra la comunicazione dello *smartphone* e il messaggio criptato viene spedito al gestore del servizio (la RIM) che ha sede in Canada che lo smista al dispositivo destinatario, all'interno del quale il messaggio viene decodificato e reso intellegibile. L'intermediario conserva le comunicazioni e può decodificare il traffico dati attraverso l'algoritmo del *server* (che si trova in Canada), ma per ottenere gli esiti delle intercettazioni non occorre far ricorso alla rogatoria essendo sufficiente che il gestore o l'utente siano italiani o il contratto di utenza sia intestato ad un italiano.

Per quanto riguarda la modalità di criptazione *end to end* (che è un sistema di comunicazione cifrata nel quale solo le persone che stanno comunicando possono leggere i messaggi), non c'è un intermediario che conserva le comunicazioni in quanto il messaggio (ad esempio, *whatsapp*) viene inviato all'altro telefonino

criptato e decriptato direttamente da questo senza che ci sia un server o un intermediario. In tal caso, la polizia giudiziaria o riesce a captare il telefono da cui parte il messaggio prima che questo venga criptato per essere inviato al destinatario, oppure può captare il dispositivo di destinazione quando il messaggio è arrivato e messo in chiaro.

Il relatore, quindi, avvalendosi di *slide* da lui predisposte, ha illustrato lo stato della giurisprudenza in tema di utilizzabilità delle cartelle bozze, dei dati *whatsapp* o dei flussi comunicativi. In tema di cartella bozze, la giurisprudenza di legittimità si è sostanzialmente attestata su un indirizzo pressoché consolidato (da ultimo, *ex multis*, Sez. 6, n. 12975/2020, Rv. 278808-02), secondo cui i messaggi di posta elettronica memorizzati nell'*account* o nel *computer* del mittente ovvero del destinatario hanno natura di documenti informatici, sicché la loro acquisizione processuale non soggiace alla disciplina delle intercettazioni, che postula la captazione di un flusso di comunicazioni in atto, ma si si attua tramite sequestro. A fronte di tale orientamento, si rinviene un'isolata sentenza della Sezione quarta della Corte di cassazione secondo cui l'acquisizione di messaggi di posta elettronica, già ricevuti o spediti e conservati nelle rispettive caselle di posta in entrata e in uscita, costituisce attività di intercettazione, sottoposta alla disciplina di cui agli artt. 266 e 266-*bis* cod. proc. pen. indipendentemente dal sistema intrusivo adottato dagli inquirenti (tramite accesso diretto al *computer* o inserimento di un programma spia).

Il relatore ha quindi affrontato la questione attinente all'utilizzazione probatoria dei dati comunicativi tramite *wathsapp*, *telegram*, *sms*, ecc. precisando che tale flusso comunicativo si documenta o con la trascrizione della comunicazione o con gli *screen-shot* del video del dispositivo (riproduzione fotografica) ad opera della persona offesa o della polizia giudiziaria o con la collaborazione del gestore oppure con il sequestro e l'acquisizione del sistema informatico.

Nulla quaestio se le prime due attività siano riconducibili alla polizia giudiziaria trattandosi di un'attività di ispezione del dispositivo che ha piena valenza probatoria. Nel caso in cui, invece, siffatte attività di trascrizione, registrazione o riproduzione fotografica vengano effettuate dalla persona offesa, occorre, come affermato di recente dalla Corte di cassazione (Sez. 5, n. 49016/2017, rv. 271856-01), al fine di corroborare il risultato probatorio e di verificare l'affidabilità, la provenienza e l'attendibilità del contenuto di dette operazioni, anche l'esibizione del dispositivo.

Con riferimento al sequestro, il relatore ha fornito delle indicazioni su come motivare il decreto: occorre cristallizzare la condotta, preservare l'organizzazione logica dei dati, prevenire la loro dispersione logica, disporre una consulenza tecnica, estrarre copia dell'*hard disk* per la prosecuzione delle indagini, fornire una descrizione tecnica.

Una volta sequestrato il dispositivo, le indagini sono sicuramente più agevoli perché tutto il contenuto del dispositivo è utilizzabile e a tutto è attribuita la valenza di documento ex art. 234 cod. proc. pen. (così, *ex multis*, Sez. 5, n. 1822/2017, Rv. 272319). In tema, si è pronunziata anche Sez. 3 n. 38681/2017, Rv. 2709502 che, in un certo qual modo, ha un po' modificato alcuni principi consolidati in materia di documenti costituenti corpo di reato, ritenendo corretta

l'acquisizione, quale documento proveniente dall'imputato, ai sensi dell'art. 237 cod. proc. pen., non solo di quanto trovato nella sfera fisica di quest'ultimo, ma anche dei messaggi inviati attraverso i *social networks Whatsapp* e *Facebook* dall'imputato alla persona offesa e da questa messi a disposizione della polizia giudiziaria.

Altra questione su cui il relatore ha richiamato l'attenzione è quella che attiene alla distinzione nella pratica tra intercettazione e sequestro, dovendosi ritenere che se l'acquisizione dei dati avviene contestualmente alla trasmissione, in modo occulto, con l'intervento del gestore o con captatore informatico, allora si tratta di intercettazione, mentre se l'acquisizione dei dati è compiuta direttamente sul dispositivo a sorpresa, ma in modo palese, allora si tratta di sequestro.

Il relatore ha quindi fatto un'ultima notazione in tema di *Digital Forensic* che è quella scienza che si occupa di garantire l'integrità dei dati e consentire alla Polizia giudiziaria e al Pubblico Ministero di lavorare non sull'*hard disk*, ma sulla copia del disco. In una sentenza della Corte di cassazione (Sez. 3, n. 43304/2014), a fronte dell'eccezione della difesa che contestava il fatto che i dati fossero stati acquisiti a *computer* spento e che, quindi, ci fosse stata una manipolazione del sistema volta a introdurre artatamente o a modificare la sequenza logica dei dati, si è affermato che tutte le modifiche dei *file* che possono essere state causate involontariamente ed automaticamente dalle normali manovre di accensione, spegnimento ed esame del *computer*, non sono idonee a inserire in esso dei dati nuovi che possano costituire prove nuove a carico dell'imputato.

Infine, il relatore ha richiamato due importanti sentenze della Corte di cassazione: la prima, in tema di efficacia probatoria della copia (Sez. 6, n.12975/2020, Rv. 278808), in cui la Corte ha affermato che "la copia estratta di un documento informatico ha la stessa valenza probatoria del dato originariamente acquisito, salvo che se ne deduca e dimostri la manipolazione" e ciò in quanto nel mondo digitale non esiste la copia, ma il duplicato digitale, poiché la copia è quella che proviene dal mondo analogico ed è la trascrizione fedele di un documento originale, mentre il duplicato è la riproduzione identica di un oggetto mediante procedimento elettronico (nel mondo digitale ogni documento è uguale a se stesso); la seconda (Sez. 3, n. 37644/2015, Rv. 265180), pronunciata in tema di perquisizione di sistema informatico o telematico, in cui la Corte ha affermato che sia l'art. 247, comma 1-bis, sia l'art. 260, comma 2, cod. proc. pen., si limitano a richiedere l'adozione di misure tecniche e di procedure idonee a garantire la conservazione dei dati informatici originali e la conformità ed immodificabilità delle copie estratte per evitare il rischio di alterazioni, senza imporre misure e procedure tipizzate e, quindi, ha rigettato il motivo di ricorso che faceva leva sulla mancata indicazione, da parte del consulente tecnico del PM, del cd. valore *hash* dei *files* ottenuti dai supporti informatici.

Nel concludere il proprio intervento il Procuratore Cuomo ha affermato che, a suo avviso, anche se il captatore informatico è stato regolamentato soltanto con riguardo alle intercettazioni, tale mezzo di ricerca della prova può essere utilizzato anche in tutti gli ambiti che offrono nuovi spazi investigativi, a condizione, ovviamente, che la sua attività sia riferibile a una figura processuale e a un mezzo

di ricerca della prova regolamentato, e ciò perché non può sostenersi che l'omissione di regolamentazione da parte del legislatore di tali aspetti, ne comporti conseguentemente il divieto di utilizzo.

.....
Ha fatto seguito l'intervento del **Prof. Giuseppe Della Monica**, intitolato « **Intercettazioni e acquisizioni di dati informatici nella prospettiva del difensore** ».

Il relatore ha esordito segnalando di avere focalizzato l'attenzione, anche al fine di dar voce alla prospettiva della difesa, su ciò che il legislatore non ha espresso, piuttosto che sulle titubanti e nebulose modifiche della disciplina delle intercettazioni. Muovendo da tale premessa, il contributo del Prof. Della Monica ha, quindi, preso avvio dalla constatazione delle straordinarie potenzialità del captatore informatico, che consente lo svolgimento di una congerie di attività investigative, tipiche ed atipiche, tutte fortemente invasive della libertà del soggetto attinto dall'azione investigativa. Il captatore non permette, infatti, solo l'intercettazione di comunicazioni, ma anche di attivare, da remoto, il microfono dell'apparecchio elettronico, di estrarre copia dell'*hard disk*, di intercettare tutto quanto digitato sulla tastiera, nonché di fotografare documenti ed immagini visualizzati all'interno del *computer*, del *tablet* o dello *smartphone*.

Occorre, quindi, operare una *summa divisio*, classificando tali plurime attività investigative in due macro aree: da un lato, le intercettazioni in senso proprio, allorché il captatore informatico consente di acquisire conversazioni o comunicazioni in qualunque forma esse si esplicano; dall'altro, l'attività di ricerca o di osservazione *on line*, attuata attraverso l'acquisizione da remoto e in forma occulta di dati di natura non comunicativa, interni o esterni al sistema informatico in cui viene inserito l'apparecchio telematico.

Le differenze tra queste due macro categorie di attività investigativa risultano evidenti perché, per un verso, si ha un mezzo di ricerca della prova tipico — l'intercettazione — che rinvia esplicita disciplina normativa nel codice di rito; per altro verso, pone in essere un'attività d'indagine — quale l'acquisizione da remoto e in forma occulta di dati privi di natura comunicativa — che resta, allo stato, sfornita di regolamentazione.

Il primo problema evidenziato dal relatore concerne, quindi, la possibilità di ricondurre tale ultima attività alle perquisizioni *on line*, ex art. 247, comma 1-bis, c.p.p., norma che legittima l'acquisizione di dati non comunicativi attraverso l'uso da remoto del captatore informatico. Nella prospettiva del relatore, deve escludersi tale assimilazione, in quanto si tratta di un'attività che non appartiene al *genus* delle perquisizioni, da qualificarsi, invece, — come affermato anche dalla Corte di cassazione (Sez. V, n. 16556/2009, Virruso) — quale attività di indagine atipica. La perquisizione, infatti, pur essendo atto a sorpresa, è, comunque, un atto garantito, che consente la presenza del difensore nel momento in cui la perquisizione viene effettuata. Non costituisce attività di ricerca occulta, ma palese, come si evince chiaramente dalle disposizioni di cui agli artt. 249, 250 e 365 c.p.p., tant'è che, anche quando non viene rinvenuto, *in loco*, il soggetto che

ha la disponibilità del sito da perquisire, deve lasciarsi l'avviso a chi, anche provvisoriamente, ne abbia la disponibilità e ciò proprio al fine di garantire la partecipazione alla perquisizione. Del resto, l'eventuale collaborazione alla perquisizione da parte dell'indagato — che potrebbe anche esibire spontaneamente quanto ricercato gli inquirenti — è una collaborazione sempre consapevole. Viceversa, la collaborazione che presta il soggetto attinto dall'azione investigativa, nel caso di utilizzo occulto da remoto del captatore informatico, risulta del tutto inconsapevole (l'indagato accede al *link* contenuto nella *mail*, determinando l'inserimento del *trojan* all'interno dell'apparecchio elettronico, oppure scarica un'applicazione e, sempre senza consapevolezza, attiva l'introduzione del captatore informatico all'interno dell'apparecchio elettronico). Non è, quindi, corretto equiparare, ai fini della tipicità normativa, la perquisizione *on line* all'acquisizione di dati non comunicativi in forma occulta e da remoto con captatore informatico che — in quanto attività di indagine atipica — dovrebbe ricondursi al disposto di cui all'art. 189 c.p.p., sottoposta, di conseguenza, ai limiti di ammissibilità fissati dalle Sez. Un. Prisco, ricondotti al profilo in disamina. Il relatore ha, dunque, ripercorso, a tale fine, i passaggi più significativi delle Sez. Un. Prisco: 1) la video ripresa (che costituisce l'oggetto del *decisum* delle Sez. Un.), se effettuata dalla polizia giudiziaria è mezzo di ricerca della prova atipico; 2) se la video ripresa è svolta all'interno di un domicilio, si tratta di un'attività atipica inammissibile, perché attuata in violazione dell'art. 14 Cost., che impone, a garanzia della persona, la doppia riserva di legge e la riserva di giurisdizione occorrendo, quindi, che il legislatore individui casi e modi di intrusione domiciliare. In altri termini, se difetta la disciplina, l'attività, pur se finalizzata all'acquisizione di dati probatori, deve reputarsi non consentita e, quindi, inammissibile; 3) la lacuna normativa non può essere colmata dall'art. 189 c.p.p., posto che, nel caso specifico, la prova atipica prima di essere tale — vale a dire non disciplinata dalla legge — deve comunque qualificarsi come prova e, per essere tale, il suo fondamento, ossia l'attività di ricerca, deve essere consentito dalla legge o quantomeno non vietato. Ricorda il relatore che, nel caso esaminato dalle Sez. Un. Prisco, l'acquisizione della prova comportava l'intrusione nel domicilio e che, pertanto, non soccorrendo la garanzia della riserva di legge di cui al 14 Cost., la Corte l'ha ritenuta inammissibile. Il *discrimen* decisivo — per il relatore del tutto condivisibile — utilizzato dal Supremo consesso va sì individuato nel seguente profilo: se le videoriprese catturano atti di natura comunicativa all'interno del domicilio e manca il decreto autorizzativo, i risultati sono inutilizzabili, poichè in contrasto con la garanzia di riserva di giurisdizione imposta dall'art. 14 Cost. Le Sez. Un. si interrogano, poi, sul concetto di domicilio e forniscono indicazioni che saranno riprese, dopo un decennio, dalle Sez. Un. D'Amico, secondo cui rientrano nella nozione di privata dimora esclusivamente i luoghi nei quali si svolgono, non occasionalmente, atti della vita privata, non aperti al pubblico né accessibili a terzi senza il consenso del titolare, compresi quelli destinati ad attività lavorativa o professionale. Domicilio, dunque, è un luogo dove si svolgono momenti di vita privata, di vita intima. È un luogo connotato dallo *ius excludendi alios*, che si caratterizza per il rapporto stabile con la persona e, quindi, proprio per tale motivo, occorre che esso debba godere di

una protezione anche in assenza della persona, a differenza di ciò che avviene nei luoghi pubblici o aperti al pubblico o nei luoghi riservati, nei quali il soggetto non può nutrire un'aspettativa di tutela della propria riservatezza equiparabile a quella all'interno del domicilio. Tale argomentazione — nella prospettiva del relatore — può essere utilizzata anche con riferimento al captatore informatico adoperato, in forma occulta da remoto, per l'acquisizione di dati non comunicativi (se l'acquisizione è svolta in maniera palese, deve essere ricondotta al *genus* della perquisizione). L'apparecchio di captazione consente sia di acquisire immagini esterne al sistema informatico — in quanto è possibile, da remoto, attivare la telecamera del *tablet* o del portatile (nel qual caso devono ritenersi validi gli enunciati delle Sez. Un. Prisco perché si tratta di dati non comunicativi esterni al sistema) — sia di acquisire in forma occulta dati non comunicativi interni al sistema informatico. Occorre allora interrogarsi su qual è, in tal caso, il livello di tutela alla riservatezza a cui può aspirare il titolare o l'utilizzatore esclusivo dell'apparecchio elettronico. Per il relatore occorre assicurare la massima tutela possibile, vale a dire quella prevista dall'art. 14 Cost., giacché il sistema informatico ha tutti i requisiti per poter essere assimilato al domicilio, risultando sicuramente un luogo, sia pure virtuale e non fisico, in cui l'individuo esplica momenti anche intimi della propria vita privata e in relazione al quale — quando è scollegato dal sistema — fruisce dello *ius excludendi alios*. Il sistema è, infatti, protetto da *password*, da chiavi di accesso, cautele volte ad evitare l'intrusione altrui in assenza dell'utilizzatore esclusivo dell'apparecchio elettronico. Se l'assunto è corretto, ossia se è possibile tale equiparazione al domicilio, è da reputarsi inammissibile l'attività di acquisizione, da remoto in forma occulta, quando si tratti di dati non comunicativi.

Quand'anche non si intendesse recepire la tesi dell'equiparazione al domicilio, occorre comunque considerare che si tratta pur sempre di uno spazio riservato, anche se virtuale, rispetto al quale deve garantirsi l'aspettativa di riservatezza dell'utilizzatore, riconosciuta non solo dall'art. 2 Cost., ma anche dall'art. 8, comma 2, CEDU, secondo cui non può esservi ingerenza di un'autorità pubblica nel diritto alla vita privata di un individuo, a meno che tale intrusione non sia prevista *ex lege*. La riserva di legge, quindi — pur non figurando nell'art. 2 Cost. — può essere così recuperata, attraverso la tutela del diritto alla riservatezza, garantito sia nel sistema interno dall'art. 2 Cost., sia dall'art. 8 della CEDU, attraverso il parametro dell'art. 117 Cost.

In definitiva, domicilio o luogo riservato che sia, la tutela della riservatezza, cui legittimamente può aspirare chi ha la disponibilità del sistema informatico, deve essere protetta dalla riserva di legge. Le attività atipiche — non assimilabili alle perquisizioni per la loro natura occulta, che consentono la devastante e incontrollata acquisizione di dati non comunicativi — vanno, dunque, considerate attività atipica di indagine non ammissibile, con la conseguente inutilizzabilità dei relativi risultati. Sempre considerando l'argomento affrontato dall'angolo visuale del difensore, occorre indubbiamente sollecitare una pronuncia della Corte di cassazione che rappresenti il *sequel* o, per rimanere in metafora, la versione 2.0 della sentenza Prisco, non risultando ammissibile che un'attività così fortemente invasiva possa essere svolta, senza preventiva regolamentazione, in aperto

contrasto con l'art. 14 della Cost. e con l'art. 8 CEDU, per il tramite dell'art. 117 Cost.

Ma anche qualora non si intendesse seguire tale prospettazione, il difensore dovrebbe quantomeno esigere l'osservanza delle disposizioni di cui all'art. 189 c.p.p.: se l'attività investigativa atipica occulta, realizzata mediante captatore informatico, è da valutarsi quale attività lecita, occorrerà applicare — tranne che non si opti per il giudizio abbreviato — il disposto di cui all'art. 189 c.p.p., che, nel caso in cui la scelta sia indirizzata verso il rito ordinario, richiede l'instaurazione del contraddittorio sulle modalità acquisitive, contraddittorio volto a verificare sia l'operatività del *software* utilizzato — per poter controllare l'eventuale alterazione dei dati — sia le modalità di installazione del *trojan*, se attuate da remoto o attraverso un accesso all'apparecchio elettronico.

Prima di accingersi a concludere il proprio contributo argomentativo, il relatore si è soffermato sulle novità normative in materia, rimarcando che il difensore verifica *ex post* e seleziona il materiale rilevante, controllando altresì, la motivazione rafforzata. Con specifico riferimento a tale profilo, è stata segnalata una discrasia di sistema: quando il captatore viene utilizzato nell'ambito di procedimenti relativi a reati contro la p.a., l'intercettazione è consentita, previa indicazione delle ragioni che ne giustificano l'utilizzo, anche nei luoghi di cui all'art. 614 c.p. Tale condizione di ammissibilità dell'azione captativa rintraccia il proprio fondamento normativo nelle disposizioni di cui all'art. 266, comma 2-*bis*, c.p.p. e non in quelle di cui all'art. 267 c.p.p. Poiché il perimetro dell'inutilizzabilità, *ex art.* 271 c.p.p., è da individuarsi nella normativa di cui agli artt. 267 e 268, commi 1 e 3, c.p.p. — la cui violazione determina l'inutilizzabilità dei risultati delle intercettazioni — l'interpretazione formale di dette disposizioni dovrebbe comportare l'inutilizzabilità del dato intercettato, in assenza di motivazione sul punto sopra richiamato o di motivazione apparente. Se, al contrario, si dovesse propendere per un'interpretazione di natura sostanziale — reputando la mancanza di motivazione requisito di ammissibilità — l'inutilizzabilità del dato intercettato potrebbe essere recuperata anche attraverso la previsione generale di cui all'art. 191 c.p.p.

Al termine dell'intervento, il Prof. Della Monica ha tenuto ad affermare con forza che al difensore non spetta il subdolo compito di ostacolare l'accertamento penale, ma quello, di certo più edificante, di stimolare costantemente la verifica di legittimità di tale accertamento, in modo da non esaurire il proprio ruolo in una marginale, quasi solo scenica, assistenza all'attività investigativa e processuale, monopolizzata dall'autorità giudiziaria.

.....

Ha concluso i lavori il **consigliere Antonio Corbo** il quale, nel ringraziare i relatori, ha sottolineato che la complessità delle questioni oggetto del convegno e la ricchezza dei contributi forniti dai relatori mal si prestano ad una sintesi; la tematica delle intercettazioni è, invero, molto complessa, sia per profili di natura tecnica, sia per profili disciplinari da interpretarsi, anche alla luce di quanto è emerso dall'incontro di studio, elaborando la materia facendo riferimento essenziale ai principi costituzionali e convenzionali.

.....

.....