



Giunte e Commissioni

RESOCONTO STENOGRAFICO

n. 4

N.B. I resoconti stenografici delle sedute di ciascuna indagine conoscitiva seguono una numerazione indipendente.

2^a COMMISSIONE PERMANENTE (Giustizia)

**INDAGINE CONOSCITIVA SUL TEMA
DELLE INTERCETTAZIONI**

15^a seduta: giovedì 26 gennaio 2023

Presidenza del presidente BONGIORNO

INDICE

Audizione di un consulente di informatica forense

PRESIDENTE	Pag. 3, 5, 6 e <i>passim</i>	* MILANA	Pag. 3, 6, 7
CAMPIONE (<i>FdI</i>)	5		
RASTRELLI (<i>FdI</i>)	5, 7		
ZANETTIN (<i>FI-BP-PPE</i>)	5		

Audizione di un professore associato di diritto processuale penale

PRESIDENTE	Pag. 8, 10, 12 e <i>passim</i>	MORELLI	Pag. 8, 12
CUCCHI (<i>Misto-AVS</i>)	10		
POTENTI (<i>LSP-PSd'Az</i>)	11		
RASTRELLI (<i>FdI</i>)	12		
SCARPINATO (<i>M5S</i>)	10		
ZANETTIN (<i>FI-BP-PPE</i>)	11		

Audizione di un professore ordinario di diritto penale

PRESIDENTE	Pag. 14, 16, 17	* MANES	Pag. 14, 16
ZANETTIN (<i>FI-BP-PPE</i>)	16		

N.B. L'asterisco accanto al nome riportato nell'indice della seduta indica che gli interventi sono stati rivisti dagli oratori

Sigle dei Gruppi parlamentari: Azione-Italia Viva-RenewEurope: Az-IV-RE; Civici d'Italia-Noi Moderati (UDC-Coraggio Italia-Noi con l'Italia-Italia al Centro)-MAIE; Cd'I-NM (UDC-CI-Nci-IaC)-MAIE; Forza Italia-Berlusconi Presidente-PPE: FI-BP-PPE; Fratelli d'Italia: FdI; Lega Salvini Premier-Partito Sardo d'Azione: LSP-PSd'Az; Movimento 5 Stelle: M5S; Partito Democratico-Italia Democratica e Progressista: PD-IDP; Per le Autonomie (SVP-Patt, Campobase, Sud Chiama Nord): Aut (SVP-Patt, Cb, SCN); Misto: Misto; Misto-ALLEANZA VERDI E SINISTRA: Misto-AVS.

Intervengono, ai sensi dell'articolo 48 del Regolamento, il consulente di informatica forense, dottor Fabio Milana, il professor Francesco Morelli, professore associato di diritto processuale penale e, in videoconferenza, il professor Vittorio Manes, professore ordinario di diritto penale.

I lavori hanno inizio alle ore 9,15.

SULLA PUBBLICITÀ DEI LAVORI

PRESIDENTE. Comunico che, ai sensi dell'articolo 33, comma 4, del Regolamento, è stata richiesta l'attivazione dell'impianto audiovisivo a circuito chiuso, nonché la trasmissione televisiva sui canali *web* e satellitare del Senato della Repubblica, e che la Presidenza del Senato ha fatto preventivamente conoscere il proprio assenso. Poiché non vi sono osservazioni, tale forma di pubblicità è adottata per il prosieguo dei lavori.

Avverto inoltre che, previa autorizzazione del Presidente del Senato, la pubblicità della seduta odierna è assicurata anche attraverso il resoconto stenografico.

Ricordo che le audizioni si svolgono anche in videoconferenza con la partecipazione da remoto dei senatori.

PROCEDURE INFORMATIVE

Audizione di un consulente di informatica forense

PRESIDENTE. L'ordine del giorno reca il seguito dell'indagine conoscitiva sul tema delle intercettazioni, sospesa nella seduta del 24 gennaio scorso.

Sono oggi previste le audizioni di un consulente di informatica forense, di un professore associato di diritto processuale penale e di un professore ordinario di diritto penale, che si svolgeranno separatamente.

Iniziamo con l'audizione del perito informatico, dottor Fabio Milana, consulente di informatica forense.

Come lei sa, stiamo conducendo un'indagine conoscitiva sul fenomeno delle intercettazioni per cui seguirà una sua esposizione sulle materie nelle quali può fornirci un contributo, che dovrebbe essere della durata di 8-10 minuti. Seguiranno le domande dei commissari, cui lei potrà rispondere in replica. Prego, a lei la parola.

MILANA. Presidente, onorevoli senatori, buongiorno a tutti e grazie dell'invito. Cercherò di dare un contributo sulla base della mia esperienza

professionale. Una breve premessa: vengo da una preparazione informatica, sono un perito informatico e nella prima parte della mia attività lavorativa ho sviluppato *software*. Dal 2003 collaboro con procure, tribunali e studi legali; in particolare, più del 90 per cento della mia attività è relativa alle intercettazioni (sia nella fase di attuazione che nella fase dibattimentale) e ai dispositivi informatici in generale. Cercherò di dare il mio contributo in questo senso, avendo preso conoscenza anche delle vostre precedenti sedute. Cercherò di non sovrappormi ai discorsi dei colleghi che mi hanno preceduto sul *software*, sull'informatica e su eventuali garanzie, ma risponderò invece a una delle domande che ho sentito essere posta più spesso: è possibile manipolare le intercettazioni? Io porto degli esempi il cui l'esito, cioè se si sia trattato di manipolazione o altro, sta ad altre persone giudicare, non a me. Quelli che porto sono semplicemente degli elementi oggettivi. Nella mia relazione ho indicato elementi oggettivi di anomalie sia su intercettazioni classiche che su intercettazioni *trojan*. Quest'ultima materia è oggi un po' più diffusa, considerata la maggiore scaltrezza delle persone che delinquono e la facilità di accesso a un dispositivo telefonico che ha un *software* e che quindi, rispetto ai vecchi telefonini o ai telefoni fissi, è dotato di strumenti maggiori.

Tra gli esempi che ho indicato nella relazione il primo in ordine cronologico risale al 2018, quando ebbi modo di analizzare una struttura informatica e *hardware* che eseguiva già intercettazioni a mezzo *trojan* per gli inquirenti. In particolare, durante un convegno a Vasto, portai all'attenzione dei presenti, tra cui il procuratore di Vasto, l'individuazione di *server* posti all'esterno dello Stato italiano; *server* di intercettazione, non *server* di altro. Successivamente, due anni dopo, mi occupai di un caso di rilevanza nazionale, su cui, già dalla documentazione che era stata prodotta alla procura (i vari preventivi e lo studio di fattibilità), emergevano delle discrasie a mio avviso rilevanti. Queste discrasie poi furono oggetto di indagine da parte di almeno tre procure e si evidenziarono delle anomalie strutturali a livello di *hardware*, quindi di *server*, che non era corrispondente a quanto previsto dal codice o da eventuali richieste *ad hoc*, nel caso specifico poi autorizzate.

Un altro caso che posso portare alla vostra attenzione, tra i tanti di cui mi sono occupato, in cui si sono riscontrate anomalie nelle intercettazioni a mezzo *trojan*, è stato quello in cui una procura ha usufruito delle caratteristiche e delle specifiche di un *trojan* di una determinata società, che proponeva un'intercettazione passiva per comprendere quali fossero le abitudini dell'utilizzatore, il gestore telefonico, per far sì che il *trojan* attivo potesse essere inoculato grazie al consenso dell'utente che cliccava sul messaggio. Questa intercettazione, denominata « passiva » dalla società che sviluppava il *software*, fu in grado, per tutto il periodo dell'intercettazione, di acquisire l'intero contenuto del telefono, anche foto scattate dieci anni prima che erano nella memoria del telefono.

L'ultimo caso che posso portare alla vostra attenzione riguarda le anomalie che si verificano, specialmente quando si usa il *trojan*, a livello di programmazione. Il *trojan*, per passare un messaggio, deve essere visto

un po' come una sveglia che va programmata: quella sveglia suonerà alle 6 di mattina, a meno che non sia stata spenta. Il *software* è molto più complesso e non può avere dei malfunzionamenti, perché il malfunzionamento del *software* e dell'*hardware*, con cui talvolta si giustificano eventuali anomalie che poi vengono riscontrate in ambiti diversi (ad esempio, bancario o medico), creerebbe dei disastri. Quindi a volte sono giustificazioni che veramente non hanno senso.

Ritornando al caso specifico, dal momento che il *trojan* viene programmato per attivarsi a una determinata ora e terminare a una determinata ora, non avere le evidenze intercettate dal microfono significa che qualcosa non è andato bene, ma difficilmente questo corrisponde a un evento particolare che può essere scomodo aver captato casualmente.

In un ultimo caso che ho visto e analizzato, purtroppo non da meno, l'inoculazione del *trojan* è documentalmente e informaticamente risalente a una determinata ora; ma la documentazione che viene poi portata dalla polizia giudiziaria al pm sposta questa indicazione. Ora, non ipotizzo assolutamente che la polizia giudiziaria abbia prodotto un falso; però non c'è una linea di coordinamento tra le attuali società che sviluppano per la procura i *software* e gli *hardware* di intercettazione, la polizia giudiziaria operante e la procura. C'è un'interruzione del passaggio di informazioni, che in ambiti diversi dall'informatica forense viene chiamata « catena di custodia ». Nel momento in cui prendiamo un'arma che ha sparato, quell'arma va trattata in un certo modo, perché può esservi una traccia di sangue o un'impronta. Anche il dato informatico deve essere trattato in un certo modo. I miei precedenti colleghi hanno avanzato varie proposte. Tra l'altro, proprio stamattina leggevo su « Sicurezza e Giustizia » un articolo molto interessante sulla certificazione dei dati informatici tra Stati facenti parte della Comunità europea. Indubbiamente ci deve essere qualche miglioramento, laddove queste lacune sono talvolta un po' troppo evidenti. Spero di aver fornito qualche informazione in più.

PRESIDENTE. La ringrazio, dottor Milana e cedo ora la parola ai colleghi che intendono porle dei quesiti.

ZANETTIN (*FI-BP-PPE*). Dottor Milana, lei ci ha detto che, in alcuni casi che ha riscontrato, questi *trojan* non rispettavano alcuni articoli specifici della normativa vigente. Ci può dettagliare un po' meglio quali sarebbero queste anomalie di carattere normativo che ha riscontrato? È chiaro che si tratta di una materia molto tecnica; tuttavia vorrei chiederle se ce la può illustrare in modo semplice.

CAMPIONE (*FdI*). Vorrei chiedere una precisazione. Lei ha parlato di anomalie dei sistemi che vengono installati: vorrei sapere se è possibile che vi siano anche alterazioni del materiale già acquisito.

RASTRELLI (*FdI*). Vorrei chiedere alcune conferme al dottor Milana. Lei ha riscontrato, anche per esperienza professionale, che i *trojan*

di cui ha avuto contezza non rispettavano i protocolli che erano stati autorizzati. Vorrei chiederle se, dal punto di vista tecnico, un *trojan* inoculato, oltre a fare ciò che dovrebbe fare (cioè attivare e disattivare il microfono ambientale), potenzialmente può anche attivare e disattivare la telecamera, accedere alla memoria del telefonino, accedere a tutti i dati fotografici, ai video e ai *file* contenuti all'interno della memoria.

PRESIDENTE. Per concludere questo giro di domande, ricollegandomi a quelle che già sono state fatte, in particolare ci interessa l'aspetto propositivo. Ad alcuni suoi colleghi è stato chiesto se, allo stato, si può ricostruire il fatto che vi sia stata un'alterazione; ci hanno detto di no, perché servirebbe un tracciamento. Altri ci hanno parlato di certificazioni di qualità. Vorrei chiederle insomma qualcosa di propositivo.

MILANA. Rispondo alla prima domanda. Il codice prevede che i *server* siano in procura; nel momento in cui viene noleggiata l'attrezzatura da parte della procura, questo è scritto sulle carte. Chi verifica la reale architettura *hardware* di questa società sicuramente vede la presenza del *server* nella sala ascolto della procura, ma a volte capire cosa c'è tra il dispositivo inoculato e il *server* è alquanto difficile. Indubbiamente abbiamo avuto dei casi in Italia, come quelli che citavo prima, in cui si sono scoperti i *server* di un'azienda nota, a prezzi bassi, negli Stati Uniti, piuttosto che *server* che erano stati autorizzati presso altra locazione, per varie difficoltà, e poi non si trovavano neanche in quella locazione. Quindi sì, indubbiamente non sempre quello che ci viene venduto per oro è oro vero. Va eseguito a mio avviso un controllo sostanziale sia sulla parte *hardware* che sulla parte *software*.

Passo ora alla seconda domanda. Il *software* è uno strumento programmato per fare determinate cose e ha delle potenzialità enormi rispetto al programmatore, che conosce lo strumento che va a utilizzare. Ricordo le lezioni di informatica: un *software* deve essere testato prima di essere messo in commercio. Riprendo l'esempio di prima: un *software* malfunzionante venduto in ambito medico creerà sicuramente grandi difficoltà. Anche in ambito finanziario o bancario immaginiamo le falle che può creare. I *software* vanno testati; garantendo questo, garantiremo poi la certezza di inalterabilità delle evidenze intercettate. Mi è stato chiesto se è possibile alterare il materiale già acquisito. Rispondo con un esempio pratico, avendo avuto modo di analizzare delle intercettazioni postume depositate a dibattimento. In queste intercettazioni vi erano, per ogni comunicazione vocale del dispositivo, due sistemi di memorizzazione. Per fare un esempio un po' più pratico, chi ha avuto una macchina fotografica digitale Canon sa che questa crea *file* jpeg (l'immagine) e i raw. Ora, l'utente neofita non esperto lavora sul jpeg, così come l'utente neofita non esperto si accorge che un *file* mp3 è un *file* audio; ma certamente non noterà il *file* raw. Nel momento in cui io di quell'intercettazione, negli eventi telefonici e nel *server* poi riversati nei supporti che arrivano a dibattimento, trovo i *file* raw, trovo un tabulato che mi dice

che c'è stata una determinata conversazione che ha una durata, trovo sull'immagine forense del telefonino un registro con quella telefonata (a quella data ora, a quel dato minuto, con quella durata e con quell'utenza), riscontro che questi audio non sono presenti nel supporto che viene poi prodotto al pm e al dibattimento e grazie al tabulato verifico che il numero di telefono appartiene agli inquirenti; ognuno cercherà una giustificazione, ma credo che non ci siano poi tante alternative per capire cosa sia successo. Quindi sì, è possibile manipolarlo; è possibile anche tagliarlo, perché, se un *file* ha una durata (parlo di dati semplici, non di dimensioni, *tag* o altro) di dieci minuti e sul supporto me ne trovo tre, e casomai a due minuti e cinquanta si capisce che il discorso tra i due interlocutori verte su un argomento particolare che poi viene improvvisamente tagliato, la risposta è sì. Dove avviene questa ipotetica manipolazione è difficile dirlo. Certamente, se il controllore venisse controllato, sarebbe ancora meglio.

Senatore Rastrelli, il *trojan* è un *software* e il cellulare è un *hardware*. Le risorse dei cellulari sono il microfono, l'altoparlante, la videocamera, il GPS (sono tante). Se il programmatore, con poche righe di codice, ha avuto accesso al GPS, io ho modo di acquisire anche il GPS. Un esempio che feci nel convegno di Vasto è che io sono riuscito a mandare, tramite il *trojan*, degli sms, che il gestore ha registrato e il destinatario ha ricevuto; ma su quel telefono non ve n'era traccia. L'ho fatto tramite il *trojan* che avevo inoculato sul telefono bersaglio.

RASTRELLI (*FdI*). Quindi non modificato, ma proprio introdotto.

MILANA. Non l'ho introdotto sul telefono, in realtà. L'ho mandato non dal telefono, ma dal terminale che avevo davanti, che gestiva il *software* che era all'interno del telefono.

PRESIDENTE. Quindi, in sintesi, si può creare un messaggio che il mittente non ha mai scritto.

MILANA. Sì. Oggi – come diceva l'ultimo collega intervenuto – con l'intelligenza artificiale si può anche imitare la voce di un soggetto. Abbiamo l'esempio di « Striscia la notizia », con una famosa signora legata al mondo VIP che viene imitata perfettamente da un'intelligenza artificiale. Nel momento in cui ho la potenzialità del *software*, posso gestire tutte le risorse.

PRESIDENTE. Va bene. E per quanto riguarda la mia domanda?

MILANA. A livello propositivo, ci sono vari strumenti che utilizzano le società di informatica in altri ambiti per garantire la corretta funzionalità e il risultato. Uno dei più comuni nell'ambito forense è il codice ASCII, che ho visto soltanto in pochissime evidenze di alcune società di

informatica, utilizzato per garantire l'inalterabilità di quel *file* audio o sms che sia. Non è vero che deve essere per forza esterno all'azienda, perché il codice ASCII, una volta calcolato, è univoco: è un'impronta digitale del dato informatico. Una certificazione esterna certamente darebbe maggiori garanzie; l'ISO, per le varie aziende italiane, garantisce ad esempio che quell'azienda ha determinate caratteristiche. Ultimamente sto sentendo parlare di certificazioni Intrastat all'interno della Comunità europea; quindi non un controllo sul controllore, ma una garanzia che il dato ricevuto in quel determinato momento sia certo e inalterabile nel tempo.

PRESIDENTE. La ringrazio per il suo contributo, dottor Milana. Sarà messa in distribuzione la nota sottoscritta dal nostro audito.

Audizione di un professore associato di diritto processuale penale

PRESIDENTE. Passiamo ora all'audizione del professor Morelli, che ringrazio per essere qui con noi. Le faccio presente che stiamo svolgendo un'indagine conoscitiva sul tema delle intercettazioni, come ovviamente le hanno anticipato i nostri uffici. Per quanto di sua competenza, dovrebbe fare un'esposizione orale contenuta inizialmente in 8-10 minuti; seguiranno delle domande e degli interventi, ai quali a sua volta potrà replicare. Le memorie inviate dal professor Morelli sono già state stampate e sono a vostra disposizione. A lei la parola, professore.

MORELLI. Buongiorno a tutti. Nella mia memoria ho cercato di toccare un po' tutti i punti, accennando a delle argomentazioni, perché la premessa è che probabilmente questa disciplina andrebbe ritoccata oramai da capo a fondo. I legislatori nel corso degli anni hanno dimostrato di averne l'intenzione, perché effettivamente è sempre una parte del codice che viene toccata.

La direzione che una disciplina delle intercettazioni a mio parere dovrebbe prendere, per poter essere conforme all'articolo 15 della Costituzione e funzionale dal punto vista investigativo, passa ovviamente, fin dal presupposto originario, dalla proporzionalità in astratto, che è rimessa nelle mani del legislatore. Nella disciplina delle intercettazioni forse ogni tanto si perde questa dimensione, però la tutela è quella dei diritti di libertà, quindi lo schema è quello dell'articolo 13 della Costituzione, che l'articolo 15 richiama. Direi di cominciare proprio dal guardare la proporzionalità in astratto, cioè quella rimessa nelle mani del legislatore, in cui vige una riserva assoluta di legge, che è notoriamente compromessa da clausole generali passibili di un'ampia gamma di interpretazioni. L'idea del processualista è quella di aspettarsi una scelta legislativa che passi da una mera elencazione di fattispecie. Non si dovrebbe più far ricorso al limite edittale come criterio di individuazione dei reati passibili di essere oggetto di procedimenti in cui si possono usare le intercetta-

zioni, anche perché poi il legislatore sarà tentato di ritoccare le pene non in funzione delle finalità della pena, ma in funzione dell'accessibilità al mezzo, come già è successo per la custodia cautelare. Dopodiché direi che si dovrebbe anche evitare il ricorso a clausole generali, tipo reati di criminalità organizzata o reati informatici, perché sono clausole rimesse alla discrezionalità dell'interprete, che chiaramente inibiscono e depotenziano la riserva assoluta di legge. Questa è la prima cornice: una scelta legislativa precisa mi sembrerebbe conforme all'articolo 15.

Un discorso più complesso, ma forse anche più importante, è quello della proporzionalità in concreto, cioè dei presupposti dell'intercettazione, che sono esattamente i presupposti su cui mi sentirei di agire anche per giungere a una limitazione dell'uso del mezzo in senso funzionale. Se è vero che si tratta di un mezzo investigativo eccessivamente utilizzato in alcuni ambiti (forse è vero) e soprattutto di un mezzo investigativo che molto spesso tende a sopperire a tasselli di indagine che invece potrebbero essere coltivati altrimenti, in maniera più funzionale (quindi è un accomodamento investigativo, a volte l'intercettazione può diventare anche questo), passerei proprio per la definizione dei presupposti, che oggi ci sono. Sono i gravi indizi di reato e l'assoluta indispensabilità per la prosecuzione delle indagini, che rimangono clausole generali, così come le ho esposte. Direi invece che è il momento di precisare questi presupposti. Precisarli vuol dire imporre dei criteri motivazionali al pubblico ministero che chiede le intercettazioni e degli schemi argomentativi per la motivazione al giudice che le autorizza. Lo schema potrebbe essere quello dell'articolo 292 del codice di procedura penale, che abbiamo sperimentato con grandissimo successo (è forse una delle norme più belle del codice di procedura penale), perché scandisce tutti i passaggi argomentativi che il giudice deve compiere per adempiere all'onere motivazionale. Ogni volta che la giurisprudenza prende vie che non ci si aspetta, è sempre perché la norma glielo consente. Lo strumento legislativo è capacissimo di difendere sé stesso; quindi direi che la precisazione di questi presupposti potrebbe essere un'ottima via. Questo significa che, per quanto riguarda i gravi indizi di reato, bisognerebbe chiedere al pm di spiegarci quali tasselli dell'addebito ha riempito con le indagini tradizionali (chiamiamole così) e da quali atti di indagine specificamente nominati trae l'esigenza di riempire altri tasselli dell'addebito con il mezzo investigativo. La giurisprudenza oggi ci dice che ci deve essere un addebito ben configurato in chiave di ipotesi; forse è davvero poco, visto che il presupposto sono i gravi indizi di reato. Bisognerebbe invece che ci fosse una specificazione richiamata sia all'atto investigativo, che riempie l'elemento dell'addebito, sia al singolo elemento dell'addebito: questa condotta, con questo atto, si dimostra accertata con questo grado dimostrativo. Si dovrebbe adottare uno schema di questo tipo (è oneroso, lo so) e il giudice, nell'autorizzare, dovrebbe ricalcare lo stesso schema.

Analogamente, forse in maniera molto più funzionale rispetto all'*extrema ratio* in cui dovremmo intendere l'intercettazione, essendo questa legata all'articolo 15, cioè a un diritto inviolabile, che può essere com-

presso solo secondo il canone dell'*extrema ratio*, il presupposto dell'assoluta indispensabilità delle indagini dovrebbe a sua volta essere inserito in uno schema motivazionale che forse può ricalcare quello che abbiamo in mente quando parliamo di perquisizione; si tratta comunque di due mezzi di ricerca della prova. Quando il pubblico ministero dice che l'intercettazione è assolutamente indispensabile per la prosecuzione delle indagini, dovrebbe riuscire a spiegare che con indagini tradizionali ha già riempito delle caselle dell'addebito. Immaginiamo l'addebito come se fosse costituito da tante caselle, che corrispondono agli elementi del reato: ha riempito delle caselle con le indagini tradizionali, ma con le stesse indagini tradizionali non riesce a riempire altre caselle. Il pubblico ministero dovrebbe spiegare di cosa va in cerca con l'intercettazione, cioè qual è lo specifico passaggio o lo specifico segmento dell'addebito che intende riempire e colmare con l'uso delle intercettazioni, spiegando perché non è riuscito a farlo con le indagini tradizionali e perché si aspetta che l'intercettazione possa farlo. Questo è un passaggio che io preciserei.

Due ultimi accenni brevissimi. Il primo riguarda il tempo delle intercettazioni, che influisce anche sul modo di intendere i suoi presupposti. È ovvio che bisogna porre uno schema con proroghe finite e che si deve intercettare per meno tempo, anche perché, se il pm sa di cosa va in cerca, può definire bene il tempo in cui deve cercare. Un ultimo passaggio fondamentale, oggi purtroppo completamente trascurato, riguarda un problema enorme: quello della difesa che non riesce ad accedere alle copie degli audio o all'ascolto dell'audio di ciò che il pm ha captato, perché non ha il tempo necessario per farlo. Questo significa che la prova delle intercettazioni è selezionata *ab origine* secondo gli intendimenti dell'accusa e – detto molto brutalmente, anche per ragioni di tempo – è possibile che l'accusa possa decidere di occultare conversazioni che le permettono di mandare avanti l'imputazione o di occultare intercettazioni che invece le permetterebbero di chiudere quell'imputazione.

PRESIDENTE. La ringrazio, professor Morelli, per la sua relazione. Cedo ora la parola ai colleghi che intendono intervenire.

CUCCHI (*Misto-AVS*). Professore, vorrei rivolgerle una domanda secca: a suo parere l'attuale disciplina delle intercettazioni presenta profili di incostituzionalità?

SCARPINATO (*M5S*). Io ho due domande da porle. La prima si riferisce al richiamo che lei ha fatto alla riserva tassativa di legge prevista dall'articolo 15 della Costituzione, che vorrei leggere: «La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge». Noi sappiamo che tra le garanzie stabilite dalla legge c'è un elenco tassativo di fattispecie e che le intercettazioni devono essere autorizzate da un giudice. Ciò premesso, le chiedo se lei ritenga che sia conforme con questa

riserva assoluta di legge la disciplina delle intercettazioni disposta per i Servizi segreti, dove non c'è nessun controllo da parte del giudice, le intercettazioni vengono autorizzate dal procuratore generale di Roma e non c'è nessun ancoraggio a specifiche tipologie di reato. Le chiedo se si può ritenere che sia conforme alla Costituzione un'autorizzazione rilasciata da un pubblico ministero, senza nessun controllo da parte del giudice, che poi viene attuata con mezzi invasivi come il *trojan*, che sono senza dubbio, al di là della loro successiva utilizzazione processuale, comunque una violazione della libertà di comunicazione.

In secondo luogo, quando lei dice che l'utilizzazione delle intercettazioni da parte del pubblico ministero dovrebbe essere motivata con l'indicazione di tutte le indagini attraverso le quali non è possibile raggiungere i risultati, questo, secondo la mia esperienza, è quello che abbiamo sempre fatto. Le faccio un esempio, che riguarda i reati dei colletti bianchi. In un caso di corruzione moderna, che viene fatta attraverso una fatturazione per falsa consulenza, se si vanno a vedere i documenti, le carte sono a posto; se si chiamano i testimoni, è blindato; se si pedinano, siccome non fanno furti e rapine, non trova niente. Quindi, nella motivazione di intercettazioni per corruzione attraverso false consulenze, tutto questo percorso viene fatto. A lei risulta che invece nelle motivazioni dei pubblici ministeri non c'è questo itinerario?

POTENTI (*LSP-PSd'Az*). Alla prima domanda che volevo porle ha già fornito una risposta, perché volevo soffermarmi proprio sulla durata media, secondo gli ultimi dati del 2021, dell'utilizzo dello strumento di captazione informatica, che risulta essere di 73 giorni circa, rispetto ai circa 50 che afferiscono invece alla durata delle intercettazioni tradizionali (ad esempio, quelle telefoniche). Si tenga conto del fatto che, in base ai tariffari, il captatore è uno dei prodotti più costosi per la procura. Lei ha toccato inoltre il tema dei limiti temporali, anche al fine di rendere lo strumento potenzialmente utilizzabile dalla maggior parte delle procure, considerato il fatto che c'è un importo massimo che il Ministero stanziava per le spese di intercettazione e che c'è uno strumento più costoso.

Poi le garanzie vengono da sole, ma non sono scontate. La seconda domanda è infatti relativa alla maggiore pervasività e capacità di acquisizione dei dati che il captatore ha per sua natura. Vorrei chiederle se lei ritiene, sulla base della sua opinione personale, che l'attuale normativa possa in qualche modo garantire una copertura anche sull'illecito utilizzo dei dati, che sono maggiormente propalabili proprio per la loro natura immateriale, essendo di fatto documenti informatici.

ZANETTIN (*FI-BP-PPE*). Premetto che condivido profondamente le argomentazioni e i principi da lei espressi, professor Morelli, e mi complimento con lei. Le rivolgo due domande semplicissime, anche se poi la soluzione non è così semplice. La prima riguarda le intercettazioni a strascico: come le regoliamo? Sappiamo tutti che la giurisprudenza da questo punto di vista ha un po' largheggiato. Quali modifiche normative suggerisce per riportarle nell'alveo costituzionale che lei ha ben tracciato?

In secondo luogo, quando un'intercettazione diventa inutilizzabile in sede penale, perché cade il presupposto del reato penale che l'ha legittimata, come trattiamo, anche alla luce della giurisprudenza fin qui maturata, gli esiti di queste intercettazioni negli altri procedimenti? Penso al civile, all'amministrativo, al disciplinare. Il caso è tutt'altro che scolastico, perché l'abbiamo riscontrato. Io parto dal concetto che quelle intercettazioni, giustificate in sede penale sulla base di un reato che poi non ha trovato riscontro, non dovrebbero essere utilizzabili nelle diverse sedi processuali. Questa è una mia opinione; vorrei conoscere la sua.

RASTRELLI (Fdi). La mia prima domanda è sovrapponibile a quella del senatore Zanettin sull'attuale disciplina dell'utilizzo delle intercettazioni in procedimenti diversi rispetto a quelli per i quali erano state autorizzate. Vorrei comprendere la sua posizione sull'attuale disciplina degli esiti delle intercettazioni non rilevanti per l'autorità giudiziaria e sulla prospettiva della loro divulgazione.

PRESIDENTE. Può rispondere alle domande, professor Morelli, ovviamente nei limiti di tempo che ci siamo dati.

MORELLI. Partendo dall'inizio, le prime due domande riguardano la costituzionalità della disciplina. Effettivamente direi che esistono delle sacche di incostituzionalità. Alcune possono stare nell'interpretazione che si dà della norma, per esempio nei presupposti. Però c'è quella ormai palese che tocca l'articolo 3, l'articolo 25, l'articolo 27, l'articolo 111 (commi 2 e 3), l'articolo 112 e l'articolo 24; mi riferisco al momento in cui il pubblico ministero deposita i suoi risultati, con l'esclusione delle altre parti. Anche la persona offesa non può essere esclusa da questa dinamica, perché deve attrezzarsi a partecipare come parte civile. Capisco che giuridicamente non ci sia una coincidenza, ma statisticamente c'è nel 99 per cento dei casi. È chiaro che, se anche le difese devono scegliere qual è l'intercettazione rilevante nella loro prospettiva, non possono non avere il quadro di tutto il captato; ma oggi è matematicamente impossibile che ce l'abbiano. Vi faccio soltanto un esempio: due mesi di intercettazione per un'utenza significano quindici mesi di ascolto in ufficio da parte della procura. Cioè è materialmente impossibile. Questa è una sacca di incostituzionalità irrimediabile dal punto di vista interpretativo.

Per quanto riguarda invece le intercettazioni preventive, direi due cose. Ovviamente non ci può essere equivalenza tra il divieto d'uso nel procedimento penale e la legittimità dell'invasione. Sono due aspetti completamente diversi: bene il divieto d'uso per le preventive, molto male l'invasione non regolata secondo lo schema dell'articolo 15 (il controllo giurisdizionale). Quello è uno schema che l'intercettazione deve rispettare in funzione cognitiva, perché glielo chiede la Costituzione. Per quanto si voglia e si possa prevedere delle intercettazioni preventive, non può non esserci la figura del giudice che sovrintende all'operazione, a pena di incompatibilità con l'articolo 15.

È chiaro che il mio riferimento sui presupposti dello schema motivazionale del pm non si riferisce a come ogni singolo magistrato interpreta il suo ruolo e interpreta il suo onere motivazionale. Si riferisce invece a uno schema che la norma deve adottare per imporre una condotta al pubblico ministero e al giudice. Troveremo sicuramente degli esempi di un buon adempimento di quest'opera già oggi, ma troveremo parimenti delle ordinanze che invece non corrispondono a questo schema. Mi riferisco a un esempio astratto: nel 2008 Enrico Marzaduri scrive su « Cassazione penale » un articolo che parla proprio dell'interpretazione giurisprudenziale completamente « slabbrata » dei presupposti dell'intercettazione, perché uno schema molto semplificato e molto « slabbrato » arriva a essere legittimato dalla Corte di cassazione. Quindi capisco che avremo sicuramente grandi esempi di ottima azione investigativa nel concreto, ma le massime della Corte suprema invece abilitano diversamente in sede di disposizione e in sede di proroga (anzi, a maggior ragione in sede di proroga). La proroga uccide il presupposto con cui parte l'intercettazione: se l'intercettazione comincia sostenuta da buoni presupposti motivazionali, più viene prorogata e meno quel presupposto si solidifica e si consolida. Più si va avanti con il tempo e più si perde la giustificazione. Un'intercettazione partita molto bene può risultare potenzialmente priva di presupposti quando finisce.

Per quanto riguarda invece la durata media e il problema del captatore, i tempi dell'intercettazione devono essere decisamente più stretti, perché bisogna che un mezzo così invasivo sia proporzionalmente mantenuto nei limiti della compatibilità con l'articolo 15, che stabilisce un diritto inviolabile. Questo significa che il tempo deve essere contenuto e l'azione investigativa deve essere mirata; non si può intercettare per vedere che succede. Oggi l'intercettazione rischia di diventare mezzo di ricerca della notizia di reato, più che mezzo di ricerca della prova. Il captatore dà un problema diverso (questo è un discorso che mi capitò di fare qualche anno fa, nel 2015). Il captatore non dovrebbe essere disciplinato in relazione allo strumento, in quanto appunto strumento idoneo a intercettare. Il legislatore deve fare un passo indietro, sul modello tedesco, e deve capire come disciplinare il captatore inteso come strumento invasivo del dispositivo elettronico, che può intercettare, ma può anche fare moltissimo altro. Quel moltissimo altro, oggi come oggi, è scoperto da ciò che ci chiede l'articolo 8 della CEDU, che chiede appunto una disposizione di legge per un mezzo invasivo. Quando installiamo un *trojan*, anche non per intercettare, stiamo violando un diritto umano previsto dalla Costituzione senza alcuna copertura legislativa; questo è un tema che il legislatore prima o poi dovrà affrontare.

Le intercettazioni a strascico sono un problema che si può restringere e contenere agendo sui presupposti e sui tempi. Capisco che l'azione sui tempi sollevi una grande preoccupazione, però bisogna chiedere al pm di riuscire a restringere dal punto di vista temporale un'azione investigativa mirata. Così non si rinuncia a un mezzo investigativo potente, ma lo si contiene nella finestra in cui è necessario.

Per quanto riguarda invece la circolazione dei risultati, rispondo molto brevemente a tutte le domande che riguardano questo tema, da giurista schematico e da meccanico del diritto. I presupposti valutati nell'ambito di un procedimento, con un addebito preciso, con un contesto investigativo preciso e con degli elementi precisi che riempiono quel contesto, è fatto per valere esattamente in quel contesto, perché la trasmissione di quel risultato implica che nel procedimento *ad quem* quel risultato sarà utilizzato senza che si possano intravedere i presupposti che l'articolo 15 richiede. Nel procedimento *ad quem*, dove rintraccio io l'atto motivato dell'autorità giurisdizionale in riferimento al mio procedimento e non a quello *a quo*? È chiaro che questo mezzo è fatto per non girare, cioè per essere disposto in un procedimento e per restare lì, perché solo in quel procedimento si possono valutare i presupposti che lo legittimano e non in altri luoghi.

PRESIDENTE. La ringrazio, professor Morelli, è stato molto chiaro.

Audizione di un professore ordinario di diritto penale

PRESIDENTE. Passiamo ora all'audizione, da remoto, del professor Vittorio Manes, professore ordinario di diritto penale presso l'Università di Bologna, che ringraziamo per essere qui presente. Il professor Manes farà un'esposizione della durata di otto-dieci minuti, cui seguiranno delle domande alle quali il professore potrà in seguito rispondere. A lei la parola, professor Manes.

MANES. Signor Presidente, sono io a ringraziare voi per questo invito e per questa preziosa occasione di confronto con gli illustrissimi senatori della Commissione giustizia. Sarò davvero molto curioso, partendo da due premesse su questo tema così importante, che credo siano state ampiamente anticipate nelle altre audizioni che avete svolto nell'ambito di questa preziosa indagine conoscitiva. Sono due premesse generali e probabilmente scontate, ma credo che le intercettazioni telefoniche e gli strumenti intercettivi più in generale (perché oggi probabilmente i problemi maggiori si focalizzano altrove) abbiano una notevole importanza. Sono un'arma a doppio taglio, come voi ben sapete. Da un lato sono degli strumenti importanti ed estremamente utili di ricerca della prova, specie in contesti in cui la criminalità si iscrive in una penombra di omertà; penso ai contesti di criminalità organizzata di stampo mafioso, ma penso anche alla criminalità cementata da un forte collante ideologico, come il terrorismo, o anche a contesti dove la relazione cooperativa tra due autori rende più difficile l'accertamento del reato. Però, al contempo, sono strumenti e misure di una formidabile ingerenza statale nei diritti individuali di riservatezza, *privacy* e rispetto della vita privata e familiare; c'è una corona di diritti in gioco (il diritto a essere

lasciati in pace, come lo definisce la Corte suprema americana), che vengono incisi da questi strumenti.

Questo spiega – e chiudo questa premessa generale – per quale motivo ogni discorso sulle intercettazioni interpella la ricerca difficile e necessaria di un equilibrio tra sicurezza e libertà. L'individuazione di un punto di isotonia tra queste esigenze è decisivo per verificare il grado di affermazione dello Stato di diritto, perché è chiaro che, se il piatto della bilancia pende troppo dalla parte della sicurezza, ammettendo strumenti di indagine senza limite, l'equilibrio si inclina verso uno Stato di polizia, verso un sistema orwelliano dove i cittadini sono assoggettati al controllo totale del grande fratello, quindi non sono più cittadini liberi in uno Stato di diritto, ma sono sudditi di un Leviatano. Questa è anche la ragione per cui il nostro codice declina la possibilità di utilizzo, di richiesta e di attivazione di determinati strumenti di ricerca della prova (come le intercettazioni telefoniche ambientali e le intercettazioni telematiche mediante un captatore) sulla base di reati qualificati di grave o intensa gravità, cioè i reati puniti con una pena non inferiore nel massimo a cinque anni.

La seconda premessa riguarda le nuove tecnologie, che hanno aumentato straordinariamente la capacità di impatto degli strumenti captativi, come dimostra l'esperienza del *trojan horse*, ma non solo. Oggi probabilmente un discorso ancor più significativo si può fare in ordine a tutti gli strumenti di indagine che possono attingere a dati telematici conservati nel *web* o altrove. Questo ha stimolato importanti prese di posizione della Corte di giustizia dell'Unione europea sul campo analogo della cosiddetta *data retention*, proprio per cercare di rintracciare quei doverosi equilibri con i valori costituzionali, convenzionali e della carta dei diritti che entrano in gioco.

Vorrei partire da questa distinzione: un tema è discutere delle intercettazioni telefoniche, un altro tema, completamente diverso, è discutere di un *malware* che illumina a giorno l'intera vita privata e familiare di un soggetto. Questa ricerca degli equilibri costituzionali in gioco, quando parliamo per esempio del captatore informatico, deve essere assoggettata a uno scrutinio ancora più rigoroso, perché naturalmente tutti i problemi di tensione con le garanzie costituzionali si amplificano e si estremizzano. Il *trojan horse*, per esempio, segna non solo un ampliamento quantitativo del raggio di ascolto, mescolando intercettazione telefonica e intercettazione ambientale, ma segna anche un mutamento qualitativo, perché da un lato è un'intercettazione itinerante che segue la persona (*propter personam*), dall'altro di fatto realizza una perquisizione indiretta, visto che può acquisire dati informatici contenuti nell'*hardware* in cui viene inoculato. Esso quindi pone anche il problema dell'estensione delle relative garanzie previste per questi diversi strumenti di indagine, ad esempio il problema dell'acquisizione al processo degli esiti dell'esplorazione. Faccio un esempio molto concreto, per significare cosa voglio cercare di dire:

la Corte suprema americana già molti anni fa, in una pronuncia molto nota (Kyllo contro Stati Uniti, del 2001), qualificò come perquisizione l'utilizzo a scopi investigativi della cosiddetta termografia a raggi infrarossi, che era un peculiare mezzo intrusivo volto a rilevare dall'esterno il calore promanante dalle mura domestiche, così da accertare se all'interno dell'edificio fosse in atto un'attività una coltivazione illecita di marijuana.

PRESIDENTE. La devo interrompere, professor Manes, per lasciare spazio alle domande dei colleghi. Purtroppo alle 10,30 dobbiamo terminare i nostri lavori, perché iniziano i lavori dell'Assemblea.

ZANETTIN (FI-BP-PPE). Professor Manes, lei ci ha detto che dobbiamo trovare un punto di equilibrio fra i diversi diritti costituzionali in gioco e ha parlato di reati di grave allarme. Noi condividiamo questo sul piano teorico. Qual è secondo lei la distinzione nel concreto fra un reato di grave allarme, che giustifica il *trojan*, rispetto a un reato che, seppur grave e da punire (su questo siamo tutti d'accordo), non giustifica però un mezzo così intrusivo?

MANES. Grazie, senatore Zanettin. È difficile fare una gerarchizzazione in astratto, io però partirei da un criterio molto semplice: lo strumento dell'intercettazione mediante *trojan* – come stavo cercando di dire – è uno strumento che amplifica enormemente i problemi di tensione con le garanzie costituzionali, quindi andrebbe limitato in chiave di stringente eccezionalità, come ogni strumento derogatorio. Il criterio secondo me più affidabile dovrebbe essere quello di limitarne l'applicazione, del tutto eccezionale, solo a quei contesti dove vi sia una particolare presunzione di pericolosità convalidata da una base empirica. I contesti di criminalità organizzata e di terrorismo, per il particolare tessuto connettivo, per la particolare relazione omertosa, per le particolari dinamiche che si creano, forse potrebbero o possono giustificare questa straordinaria deroga e incisione dei diritti fondamentali; invece altri reati, come per esempio i reati contro la pubblica amministrazione (da questo punto di vista condivido la proposta di ritornare a un regime ordinario nell'utilizzo del captatore informatico per i reati diversi da mafia e criminalità terroristica), non giustificano questa derogatoria misura eccezionale sottesa alla captazione informatica. La Corte costituzionale ha utilizzato un'argomentazione analoga quando per esempio ha dovuto considerare, *mutatis mutandis* ovviamente, la legittimità delle presunzioni di pericolosità sottese all'utilizzo della custodia cautelare in carcere, limitandola a quei contesti dove effettivamente, dal punto di vista empirico, si avesse la dimostrazione che solo una determinata misura cautelare (quella custodiale in carcere) riuscisse a spezzare determinati legami. Quindi solo determinati fenotipi criminosi possono giustificare questa

straordinaria misura di incidenza, come appunto la criminalità organizzata di stampo mafioso e il terrorismo; altri non dovrebbero essere accostati, se non alla luce di una specifica indagine empirica che dimostri concretamente che solo questo strumento è assolutamente indispensabile per effettuare indagini efficaci.

PRESIDENTE. La ringrazio per il suo intervento e il suo contributo, professor Manes, e la saluto.

Dichiaro conclusa l'audizione in titolo e rinvio il seguito dell'indagine conoscitiva ad altra seduta.

I lavori terminano alle ore 10,30.

