Senato della Repubblica XIX LEGISLATURA

Giunte e Commissioni

RESOCONTO STENOGRAFICO n. 3

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

2ª COMMISSIONE PERMANENTE (Giustizia)

INDAGINE CONOSCITIVA SUL TEMA
DELLE INTERCETTAZIONI

14ª seduta: martedì 24 gennaio 2023

Presidenza del presidente BONGIORNO

INDICE

Audizione del Presidente del Garante per la protezione dei dati personali

Audizione del Presidente dell'Associazione *Lawful Interception*

Audizione dell'ingegner Lelio della Pietra

Audizione del professor Gianluigi Gatta

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 Presidente del Garante per la protezione dei dati personali, professor Pasquale Stanzione, il Presidente dell'Associazione Lawful Interception, dottor Elio Cattaneo, l'ingegner Lelio Della Pietra, consulente di informatica forense, e il professor Gianluigi Gatta, professore ordinario di diritto penale.

I lavori hanno inizio alle ore 14.

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 del Presidente del Garante per la protezione dei dati personali

PRESIDENTE. L'ordine del giorno reca il seguito dell'indagine conoscitiva sul tema delle intercettazioni, sospesa nella seduta del 17 gennaio scorso.

Oggi saranno svolte, separatamente, le audizioni del Presidente del Garante per la protezione dei dati personali, professor Pasquale Stanzione, del Presidente dell'Associazione *Lawful Interception*, dottor Elio Cattaneo, dell'ingegner Lelio Della Pietra, consulente di informatica forense e del professor Gian Luigi Gatta, professore ordinario di diritto penale.

Procediamo dunque con la prima audizione. Cedo la parola al professor Stanzione.

STANZIONE. Signor Presidente, onorevoli senatrici e senatori, il Garante è onorato di poter fornire il proprio contributo ai lavori della Commissione.

Nel riformare la disciplina delle intercettazioni, il legislatore ha il delicatissimo compito di coniugare il diritto alla riservatezza con le esigenze investigative, il diritto di difesa e, con riferimento alla circolazione extraprocessuale, il diritto di e all'informazione. Questo bilanciamento va condotto naturalmente nella consapevolezza delle implicazioni profonde sulla riservatezza del ricorso alla tecnologia, tanto in fase investigativa – si pensi ai *trojan* – quanto in sede di circolazione extraprocessuale dei contenuti captati con l'amplificazione che il *web* assicura a ogni tipo di pubblicazione.

In questo senso, è necessario ben distinguere presupposti e limiti dell'utilizzo processuale delle conversazioni intercettate da presupposti e limiti della loro divulgazione a fini informativi, garantendo ai due aspetti della disciplina l'autonomia derivante dalla differenza di finalità ed esigenze che vi sono sottese.

Il diritto alla riservatezza rileva in maniera particolare nell'ambito della disciplina delle intercettazioni sotto un duplice profilo rispetto alle operazioni captative in sé e alla circolazione endo ed extraprocessuale dei contenuti captati, ricordando comunque che la disciplina di protezione dei dati si applica anche al trattamento di dati personali in sede giudiziaria penale.

Rispetto al primo profilo è certo rilevante la definizione del perimetro di ammissibilità delle intercettazioni variamente modulata dai progetti di legge proposti nelle scorse legislature non solo rispetto alla categoria dei reati individualizzanti e intercettabili, ma anche in ordine ai presupposti che sono relativi alle singole captazioni. Queste scelte – vorrei fortemente ribadirlo – sono rimesse naturalmente alla discrezionalità politica, pur con il limite però del rispetto del principio di proporzionalità tra esigenze investigative e *privacy*.

In questo bilanciamento avrà naturalmente un peso importante il grado di invasività del mezzo investigativo, certamente maggiore per strumenti potenzialmente onnivori e ubiquitari come sono i *trojan*. Allora, particolarmente importante è il regime circolatorio endoprocessuale dei contenuti captati. Sul punto, la disciplina vigente dal 2020 contiene misure importanti volte a limitare la circolazione endoprocessuale delle intercettazioni eccedenti le esigenze investigative, pur nel rispetto del contraddittorio per e sulla prova. Esse recepiscono una esigenza di garanzia condivisa anche dalla stessa magistratura, come dimostrano le direttive emanate da alcune procure nel 2016 – lo ricorderete – nonché le buone prassi indicate dall'organo di governo autonomo nel luglio del 2020. Particolarmente rilevanti sono la prevista esclusione, rimessa al dovere di vigilanza del pubblico ministero, della trascrivibilità di dati sensibili irrilevanti e di contenuti lesivi della reputazione nonché la devoluzione di tali dati e delle conversazioni inutilizzabili all'archivio digitale, con conseguente loro assoggettamento al regime del segreto d'ufficio.

Se attuata con rigore, la nuova disciplina può effettivamente contribuire a ridurre e limitare la circolazione endoprocessuale di dati personali eccedenti. Naturalmente ciò presuppone, soprattutto per la fase della con-

servazione in archivio dei contenuti stralciati, l'adozione di regole di sicurezza adeguate e conformi a quelle indicate dal Garante, che ha avuto modo di esprimersi fin dal 2013 su questi argomenti. Ebbene, la vera scommessa della riforma dipende infatti molto da come verrà garantita l'effettiva impermeabilità dell'archivio.

Inoltre, laddove non abbiano sortito effetti i criteri di sobrietà contenutistica e minimizzazione selettiva, un'importante tutela rimediale per le parti deriva dall'innovativa procedura introdotta dall'articolo 14 del decreto legislativo n. 51 del 2018. Tale norma, come sapete, legittima chiunque vi abbia interesse a richiedere al giudice, sussistendone i presupposti, la rettifica, la cancellazione o la limitazione dei dati che lo riguardano, anche durante il procedimento penale. Si tratta di una norma dalle notevoli potenzialità che, combinandosi con la procedura di distruzione di cui all'articolo 269 del codice di procedura penale, potrebbe contribuire a rafforzare sensibilmente le garanzie di riservatezza soprattutto dei terzi le cui conversazioni siano state indirettamente captate.

Naturalmente, l'effettività della norma sarebbe rafforzata, auspicabilmente, con la previsione di un onere informativo a carico del pubblico ministero per evitare che il soggetto apprenda dell'esistenza in atti processuali di proprie conversazioni direttamente dalla stampa, quando ormai l'intervento ablativo sarebbe tardivo.

Più complesso è il tema della pubblicazione in violazione del segreto veramente esterno, *ex* articolo 114, comma 2, del codice di procedura penale, di stralci, spesso ampi, di conversazioni captate. Benché questo divieto sia posto a tutela non tanto della *privacy* quanto della neutralità conoscitiva del giudice, la sua violazione, che ben può ledere la riservatezza, integra comunque un trattamento illegittimo di dati personali, punito dal 2018 – che, come è noto, è l'anno dell'entrata in vigore del regolamento generale sulla protezione dei dati (GDPR) – con sanzioni amministrative pecuniarie sino a 20 milioni di euro e al 4 per cento del fatturato.

Tali sanzioni possono svolgere una rilevante funzione deterrente rispetto alla divulgazione acritica e indiscriminata delle conversazioni captate ben oltre le reali esigenze di cronaca. Naturalmente si può anche ipotizzare, come nelle scorse legislature, di modulare diversamente il regime di pubblicità degli atti d'indagine.

Tuttavia, prima di mutare un bilanciamento tra *privacy* e informazione, in fondo ragionevole, è forse preferibile verificare tenute ed effetti delle riforme recenti, ivi inclusa quella di cui al decreto legislativo n. 188 del 2021 sulla presunzione di innocenza, che conosciamo tutti.

Per quanto riguarda invece le intercettazioni mediante captatori, le potenzialità intrusive di tali strumenti impongono garanzie adeguate. La necessità di tali garanzie sembra peraltro asseverata da vicende recenti (penso soltanto al cosiddetto caso Exodus del 2019) relative alle particolari modalità di realizzazione delle captazioni mediante *malware*; esse evidenziano i rischi connessi all'utilizzo di captatori informatici, con il ricorso da parte delle società incaricate a tecniche di infiltrazione prive

della necessaria selettività. Ci si riferisce, in particolare, all'utilizzo a fini intercettativi di *software* connessi ad *app*, quindi non direttamente inoculati nel solo dispositivo dell'indagato – e andrebbe bene, allorché sia autorizzato dal giudice ovviamente – ma posti su piattaforme (come ad esempio Google Play Store) accessibili a tutti. Ove rese disponibili sul mercato, anche solo per errore, in assenza dei filtri necessari a limitarne l'acquisizione da parte dei terzi, queste *app*-spia rischierebbero infatti di trasformarsi in pericolosi strumenti di sorveglianza massiva.

È inoltre pericoloso l'utilizzo di sistemi *cloud* per l'archiviazione addirittura in Stati extraeuropei dei dati captati. La delocalizzazione dei *server* in territori non soggetti alla giurisdizione nazionale costituisce, infatti, un evidente *vulnus*, non soltanto per la tutela dei diritti degli interessati, ma anche per la stessa efficacia e segretezza dell'azione investigativa.

In ogni caso, anche in ragione della rapida evoluzione delle caratteristiche e delle funzionalità dei *software* disponibili a fini intercettativi, come già abbiamo rilevato in talune segnalazioni al Parlamento e al Governo nel 2019, sarebbe opportuno vietare il ricorso a captatori idonei a modificare il contenuto del dispositivo ospite e a cancellare le tracce delle operazioni svolte.

Ai fini, dunque, della corretta ricostruzione probatoria della garanzia del diritto di difesa come anche della *privacy*, è indispensabile disporre di *software* idonei a ricostruire nel dettaglio ogni attività svolta nel sistema ospite e sui dati ivi presenti senza alterarne il contenuto, corrispondentemente valorizzando l'esigenza di una verbalizzazione analitica delle operazioni compiute.

Ferma dunque restando – e mi avvio a concludere – l'opportunità della introduzione delle su descritte cautele, la particolare invasività dei *software* spia merita certamente una riflessione da parte del Parlamento in ordine al reale ambito applicativo di questo mezzo di ricerca della prova.

Certamente positiva è la previsione della necessità di indicazione nel decreto autorizzativo delle ragioni di indispensabilità dell'utilizzo del *trojan* (secondo quanto introdotto dal decreto-legge n. 132 del 2021) e, per i delitti diversi dai distrettuali o dai più gravi contro la pubblica amministrazione, dei luoghi e dei tempi di attivazione del microfono; in tal modo si può almeno in parte circoscrivere la potenziale ubiquitarietà del mezzo e la difficile predeterminazione dello sviluppo delle captazioni.

Tuttavia, laddove il Parlamento ritenesse di ripensare il perimetro di ammissibilità di questo tipo di captazione, utili spunti possono derivare dalla lettura forte dello scrutinio di proporzionalità tra esigenze investigative e riservatezza, offerta a proposito anche dei *trojan* da una bella esperienza che è stata svolta dalla Corte costituzionale tedesca. È infatti particolarmente rilevante – e chiudo veramente – la considerazione di come il canone di proporzionalità imponga una modulazione delle garanzie, che tenga conto delle potenzialità del mezzo investigativo concretamente utilizzato e della sua capacità di incidenza sul nucleo intangibile della vita privata del soggetto.

Sono considerazioni a me pare utili per un legislatore che ha il difficile compito di bilanciare beni giuridici fondamentali come la riservatezza, il diritto di difesa e le esigenze della giustizia.

PRESIDENTE. Ringrazio il professor Stanzione per la sua relazione. Lascio ora la parola ai colleghi che desiderano intervenire.

SCARPINATO *(M5S).* Professor Stanzione, ho tre domande da porle.

Come lei sa, e come ha detto, dal 1° settembre 2020 è entrata in vigore una nuova disciplina in materia di intercettazioni.

La mia prima domanda è la seguente. Tenuto conto che il Garante della *privacy* può intervenire, non solo su richiesta, su esposto, ma anche d'iniziativa, vorrei sapere quanti casi di violazione della *privacy* si sono verificati dopo il 1° settembre 2020.

La seconda domanda riguarda invece il numero di casi di violazione della *privacy* accertati negli ultimi vent'anni, dal 1° gennaio 2000 al 1° settembre 2022. Le pongo tale quesito perché oggi ho letto sulla stampa un articolo in cui si parlava di una ventina di casi: non sapendo se questo dato sia esatto oppure no, le chiedo di darci il dato ufficiale.

Infine, professor Stanzione, lei ha fatto riferimento nella parte conclusiva della sua relazione all'esperienza della Corte costituzionale tedesca a proposito del forte scrutinio di proporzionalità tra le esigenze investigative e la riservatezza e ha detto che se ne possono trarre spunti.

Siccome sono stato sentito dal Parlamento tedesco e ho avuto degli incontri seminariali con il Ministro della giustizia, mi risulta che in Germania abbiano un grandissimo problema legato al fatto che il Paese è diventato l'Eldorado di tutti gli investimenti mafiosi (dalla mafia russa a quella italiana) perché, come dice lo stesso Ministro della giustizia, i limiti posti alle intercettazioni dalla legislazione impediscono alla magistratura e alla polizia di fare indagini serie sul riciclaggio e sulla mafia: per questo siamo stati noi italiani, secondo la nostra legislazione, a scoprire i beni dei mafiosi in Germania. Vorrei sapere se questo le risulta, visto che lei ha citato la Corte costituzionale tedesca.

BAZOLI *(PD-IDP)*. Professor Stanzione, la ringrazio anch'io molto per la sua relazione, che mi pare ci aiuti a sgomberare un po' il campo da tante argomentazioni molto superficiali che stanno emergendo oggi nel dibattito politico italiano a proposito di questo argomento. La ringrazio anche per aver fatto la distinzione – che io credo sia necessaria quando si ragiona di questi temi – tra i limiti di divulgazione endoprocessuali (e quindi i limiti ai presupposti per le intercettazioni che attengono alla fase processuale) e quello che invece attiene alla pubblicazione delle intercettazioni sulla stampa e sugli organi di informazione, che mi sembra un aspetto altrettanto importante.

Sulla prima questione, cioè sui limiti di divulgazione endoprocessuali, lei ha detto una cosa che a me pare importante: la nuova disciplina

introdotta nel 2020 ha trovato un assetto tutto sommato ragionevole, un buon assetto per garantire che si eviti una circolazione di dati che rischi poi la divulgazione, però tutto dipende – semplifico molto – sostanzialmente dalle regole con le quali si garantirà la sicurezza degli archivi digitali nei quali vengono riversati i dati irrilevanti. Da quanto lei ha detto, mi pare di aver capito che queste regole ancora non ci sono e devono ancora essere elaborate: sono regole che deve redigere il Ministero o si tratta di altro? Mi interesserebbe capire se su questo occorre fare qualche passo in avanti per fare in modo che quella disciplina, che secondo lei è una buona disciplina, venga attuata concretamente e in modo efficace.

SCALFAROTTO *(Az-IV-RE)*. Signor Presidente, anch'io ringrazio il Garante per la disponibilità.

Professor Stanzione, lei ha concluso la sua relazione indicando i beni giuridici che vanno contemperati in questa situazione e ha detto giustamente che la contemperazione di questi beni giuridici è complessa.

La mia domanda è molto semplice: dal punto di vista del Garante della *privacy* esiste una gerarchia tra questi beni giuridici? Nell'impossibilità di rispettarli entrambi, dal vostro punto di vista esiste teoricamente, ossia sulla base della norma costituzionale, la possibilità di derogare a uno di questi beni a favore dell'altro? Sarebbe sostanzialmente come dire: dato che noi dobbiamo mantenere l'ordine pubblico e reprimere il crimine, possiamo derogare al diritto alla riservatezza. Oppure, viceversa, poiché c'è il diritto alla riservatezza dobbiamo affievolire la lotta al crimine?

STEFANI *(LSP-PSd'Az)*. Signor Presidente, ringrazio il Garante per le informazioni che ci ha riferito; spero che ci lascerà un documento, poiché la relazione è stata molto dettagliata.

Una domanda del collega Scarpinato verteva sui casi in cui sia stata comminata una sanzione da parte del Garante. Tuttavia, le sanzioni – anche se dovremmo saperlo, le chiedo una conferma in modo che resti agli atti – sono ovviamente irrogate una volta che si sia realizzata la violazione.

Come valuta la normativa attuale? Più che chiedere se essa sia un valido deterrente perché prevede la sanzione, vorrei capire se il sistema che abbiamo sia in grado di prevenire la pubblicazione delle informazioni, soprattutto in quei meccanismi molto complessi che sono all'interno del processo. Vi può essere qualche nuova iniziativa che possa dare una migliore determinazione, proprio con riferimento alla normativa sulla *privacy*, sul tema delle intercettazioni? Oppure è solo una questione di impermeabilità degli archivi? Ad ogni buon conto, penso che le sanzioni vengano irrogate quando c'è una denuncia, ma non sempre si denuncia una violazione della *privacy* perché probabilmente molti non conoscono nemmeno quali siano i confini del diritto alla *privacy*.

PRESIDENTE. Concludo io gli interventi chiedendole di poter sapere qualcosa di più sul *trojan*, che lei ha definito onnivoro. Credo che

sul *trojan* lei abbia sottolineato la necessità di integrare la normativa: anche su questo profilo le chiederei di essere propositivo. A noi infatti piace quando gli auditi ci lasciano anche qualche spunto di riflessione, a prescindere se possa poi incontrare la condivisione o meno.

STANZIONE. Vorrei rispondere succintamente, secondo le indicazioni della Presidente, anche perché molte sono domande di senso, e spiegherò subito il perché.

Per quanto riguarda il senatore Scarpinato, dal 2020, dopo la nuova legislazione, noi non registriamo nell'*Authority* alcun caso al riguardo. Su questi numeri (la nostra consiliatura è attiva da due anni), non posso essere preciso perché non ho il punto della situazione dal 2000 al 2020. Posso tranquillizzare questa Commissione: non sono moltissime le ipotesi esaminate al riguardo.

Senatrice Stefani, consideri che l'Autorità interviene indubbiamente *ex post*, quando il fatto si è verificato, dopo il reclamo o la notizia *aliunde* appresa dai giornali e così via. È vero che preventivamente abbiamo un obbligo di cooperazione nell'accompagnare nella fase ascendente anche le proposte di legge, i disegni di legge e così via, ma il discorso preventivo probabilmente dovrebbe essere spostato su ben altri parametri, vale a dire quello di una diffusa educazione – oserei dire *paideia* integrale relativamente a queste tematiche – e quello della sensibilizzazione nei confronti dei diritti fondamentali della persona.

Sono state citate la Germania e le note sentenze del tribunale federale tedesco costituzionale del 2016 e del 2018. Al riguardo, come *Authority*, non abbiamo alcuna possibilità di intervenire, nemmeno come suggerimento, sul perimetro dell'ammissibilità dei mezzi captatori o delle intercettazioni. Questa – mi pare evidente – è una prerogativa esclusiva del Parlamento. Possiamo intervenire esclusivamente in una fase successiva.

Senatore Bazoli, quello che possiamo verificare è che mancano ancora le sale *server* interdipartimentali previste da decreti recanti specifiche tecniche, che tuttavia non risultano adottati. Anzi, relativamente a queste misure di sicurezza, è compito istituzionale del Garante offrire una collaborazione in una prospettiva di valutazione, rispetto alle iniziative assunte dalle autorità competenti.

Senatore Scalfarotto, lei ha posto la domanda delle domande. Non c'è una tirannia dei valori, se vogliamo esprimerci in questi termini. Probabilmente una gerarchia potremmo individuarla nell'ambito della nostra Carta costituzionale ed è quella rappresentata dalla centralità della persona umana: ci muoviamo in un sistema ordinamentale che è costruito intorno al valore fondante della persona umana. Tutto ciò che viola, tocca, vulnera la persona umana, quello è da delimitare, comprimere, possibilmente eliminare. Ma è chiaro che, relativamente a questi profili che abbiamo visto e che concernono il diritto di difesa, la riservatezza, le esigenze della giustizia, la soluzione è quella del bilanciamento; non c'è

altra strada al riguardo. Però il faro, la linea, la via principale è rappresentata dalla tutela della persona umana.

Badate che questo non lo dice soltanto la nostra Costituzione, poiché ci muoviamo in un sistema europeo che del personalismo ha fatto la centralità della propria normativa. Saranno il GDPR, il *Digital service act*, l'*Artificial intelligence act* a muoversi in questa prospettiva. Anzi, mi permetto di dire, se la Presidente lo consente, che l'Europa ha una via mediana proprio nei confronti dell'intelligenza artificiale, che tocca questi profili enormi di invasione della sfera intima della persona. La via mediana consiste in una strada che non è né il liberismo sfrenato dell'esperienza anche statunitense né quella articolata viceversa sullo statalismo più accentuato, ossia la cinese-coreana, che non lascia spazio all'espletamento e al libero sviluppo della personalità, a cui il nostro articolo 2, tante volte citato, dà garanzia e solida conformazione.

Quanto al *trojan*, mi è sembrato di essere stato abbastanza netto al riguardo nel dire che esso va utilizzato se così desidera l'autorità politica competente, che è in primo luogo il Parlamento. Tuttavia, bisogna stare attenti alle modalità di utilizzazione dello stesso, perché il modo con cui si potrebbe interferire con l'utilizzo del *trojan* da parte di tutti (ad esempio, attraverso *app*-spie e quant'altro) non va proprio bene. Limitato al destinatario, se così si decide, e con l'autorizzazione motivata da parte dell'autorità giudiziaria, perché no?

PRESIDENTE. Ringrazio a nome della Commissione il Garante della *privacy*, anche per la nota scritta che ci ha lasciato e che è già in distribuzione, vista l'importanza del suo contributo.

Audizione del Presidente dell'Associazione *Lawful Interception*

PRESIDENTE. I nostri lavori proseguono ora con l'audizione del Presidente dell'associazione *Lawful Interception*, dottor Elio Cattaneo, al quale do il benvenuto, ringraziandolo per aver accettato il nostro invito ad offrire alla Commissione un approfondimento sul tema delle intercettazioni.

Dopo la relazione, ci sarà spazio per eventuali quesiti da parte dei colleghi.

Prego, dottor Cattaneo, a lei la parola.

CATTANEO. Buonasera a tutti, sono Elio Cattaneo, amministratore delegato di SIO Spa e presidente di ASLI.

Ringrazio la Commissione per l'invito ad intervenire in questa prestigiosa sede e porgo il mio deferente saluto a lei, signora Presidente, e agli onorevoli senatori presenti.

ASLI (Associazione *Lawful Interception*) è l'associazione di categoria affiliata ad Aiad (Federazione italiana per l'aerospazio e la difesa e la sicurezza) che raggruppa le sei principali aziende del settore: Area Spa, Innova Spa, IPS Spa, Lutech Spa, RCS Spa e SIO Spa.

Le nostre aziende, ciascuna con almeno venticinque anni di esperienza nel campo delle intercettazioni, rappresentano per volume il 75 per cento dal comparto e occupano complessivamente oltre 1.500 addetti impiegati su tutto il territorio nazionale. Sono imprese *hi-tech* che investono circa il 18 per cento del proprio fatturato tra ricerca e sviluppo ed infrastrutture.

PRESIDENTE. La inviterei a passare subito al tema, dottor Cattaneo.

CATTANEO. Certamente. Ci tengo a dire, però, che siamo proprietari della parte *hardware* e *software* delle tecnologie che vengono fornite alle Forze di polizia e alla magistratura per l'esercizio delle loro funzioni. In Italia infatti sono gli organi di Stato, e soltanto loro, i nostri clienti. Per quanto riguarda l'estero, pur essendo complesso raffrontare sistemi istituzionali dissimili con differenti *budget*, voglio accennare al fatto che Paesi come il Regno Unito, la Francia e altri, spendono centinaia di milioni di euro l'anno, e non solo per l'aggiornamento delle tecnologie legate alle intercettazioni legali, che acquistano da aziende simili alle nostre.

Venendo all'ambito dell'indagine conoscitiva e ai temi emersi nel corso del dibattito in questa sede, vorrei soffermarmi sui seguenti aspetti: il recente decreto ministeriale per la determinazione delle tariffe delle intercettazioni e la certificazione dei procedimenti per il trattamento dei dati.

Con riferimento all'ampio quadro normativo e regolamentare in cui le imprese erogano le prestazioni funzionali sul tema della spesa per le intercettazioni, vale la pena citare il decreto ministeriale del 6 ottobre 2022, entrato in vigore il 15 dicembre scorso, con la pubblicazione sul bollettino ufficiale del Ministero la giustizia. Si tratta di un provvedimento lungamente atteso e condivisibile, con un impianto volto ad introdurre uniformità di gestione e parità di trattamento tra le aziende fornitrici.

Il decreto ministeriale introduce un listino unico nazionale caratterizzato da tariffe e importi fissi associati a ciascuna prestazione, ad eccezione di quelle a carattere speciale da determinarsi in seguito. Il listino unico sostituisce il precedente regime in cui vi erano più listini adottati localmente dalle singole procure. Il percorso di razionalizzazione delle tariffe individuato dal decreto ministeriale si pone, quindi, come primo tassello per affrontare seriamente il tema della sostenibilità del comparto e conseguentemente la qualità del servizio strategico fornito alla magistratura.

Va tuttavia sottolineato che il nuovo tariffario comporta un complessivo calo di prezzi in un settore che ha già visto, negli ultimi dieci anni, una progressiva riduzione del 30 per cento della spesa e presenta tempi di incasso dei pagamenti dei servizi erogati che ormai sono arrivati a superare l'anno. È di tutta evidenza che l'efficacia dello strumento delle

intercettazioni passi attraverso la sostenibilità della remunerazione delle imprese che forniscono tale servizio, le quali devono essere in grado di mantenere quegli elevati *standard* tecnologici richiesti dalle Forze di polizia per il contrasto al crimine e il conseguente recupero allo Stato dei patrimoni illeciti.

Eventuali e ulteriori riduzioni dei prezzi comporterebbero minori investimenti e una perdita di competitività rispetto ai Paesi esteri e, soprattutto, alla stessa criminalità, che sempre più investe per porre in essere misure di inibizione dei sistemi di intercettazione.

Il settore delle intercettazioni, eccellenza del comparto *hi-tech* del nostro Paese, fonda infatti la propria attività su ricerca e sviluppo, che richiedono ingenti risorse e una programmazione a lungo termine. Per questo riveste particolare importanza il fatto che le tariffe del nuovo listino siano applicate in maniera fissa ed uniforme su tutto il territorio, realizzando un quadro sufficientemente stabile per permettere alle imprese di pianificare la propria attività, perseguendo il fine dell'eccellenza del servizio.

Per un confronto sui temi menzionati, ASLI si associa all'auspicio espresso, anche in questa sede, affinché il tavolo tecnico permanente di monitoraggio del sistema delle prestazioni funzionali, previsto dall'articolo 8 del medesimo decreto, sia costituito prima possibile così da potervi dare il proprio contributo in qualità di *stakeholder* qualificato.

Infine, sulle certificazioni. Fermi restando gli adempimenti di legge previsti a partire dal decreto legislativo n. 216 del 2017, nel provvedimento ministeriale (articoli 3 e 4) sono introdotti specifici obblighi per i fornitori delle prestazioni e sono individuate quali debbano essere le garanzie di sicurezza nella conservazione e nella gestione dei dati, stabilendo (articolo 7) che l'autorità giudiziaria possa procedere a verifiche e controlli in merito alla funzionalità e alla sicurezza delle attrezzature impiegate e dell'organizzazione complessiva.

Si tratta di un regime di disposizioni particolarmente articolato e oneroso, calibrato sulla delicatezza dei dati trattati e delle operazioni svolte.

Sul punto per ASLI non vi sono motivi che ostino alla previsione, ove richieste, di ulteriori verifiche. Si condivide, quindi, l'opportunità che le imprese possono essere sottoposte ad un obbligo di certificazione per i requisiti di sicurezza delle informazioni e dei modelli organizzativi da parte di enti terzi, qualificati ed accreditati.

Conseguentemente nella nostra prospettiva di assicurare il massimo livello di *compliance* alle norme e alle pratiche in termini di riservatezza e operatività, il punto di arrivo virtuoso sarebbe allora la creazione di un albo ministeriale per i fornitori autorizzati.

PRESIDENTE. La ringrazio, dottor Cattaneo.

La parola va ora ai colleghi che hanno chiesto di intervenire.

SCARPINATO *(M5S)*. Dottor Cattaneo, se ho ben capito, lei rappresenta le principali aziende che in campo nazionale forniscono strumenta-

zione, *server* e *software* per le intercettazioni. Nella sua relazione ha fatto riferimento sostanzialmente alle spese per le intercettazioni giudiziarie.

Lei certamente sa che le intercettazioni, però, non sono disposte soltanto dalla magistratura, ma anche dai Servizi segreti, senza nessun ancoraggio a specifiche ipotesi di reato e senza nessun controllo da parte dei giudici. Vorrei sapere, dunque, se le aziende che lei rappresenta forniscono la stessa tecnologia anche ai Servizi segreti oppure se questi usano *server*, *software* e strumentazione propri.

In secondo luogo, i *software* usati dai Servizi segreti sono uguali a quelli utilizzati dalla magistratura o sono diversi, come nel caso di quelli utilizzati in Stati esteri che non si utilizzano in Italia?

STEFANI *(LSP-PSd'Az)*. Stando a quanto appreso dalla sua esposizione, siete voi stessi ad elaborare le tecnologie dei singoli *software*? Avete detto che vi basate su un tariffario, quindi la tecnologia è quella che riuscite ad elaborare sulla base delle risorse disponibili derivanti dalla corresponsione del pagamento dei vostri servizi? Un'altra domanda: quali sono i vostri meccanismi all'interno per garantire la genuinità dei *file* che vengono estratti?

Un esperto che abbiamo ascoltato riferiva che vi è la possibilità di manipolare questi dati, soprattutto con il *trojan*, ossia il captatore inoculato che aveva delle caratteristiche ed era talmente invasivo che poteva anche alterare i dati stessi. Non penso che lei me lo direbbe, ma lo chiedo lo stesso: ci sono state delle fughe di notizie dalle vostre società sui dati che sono stati da voi rilevati?

PRESIDENTE. Mi ricollego alla domanda della senatrice Stefani. Con riferimento al *trojan*, ci è stato rappresentato che, con questo tipo di captazione e i dati raccolti, il soggetto che li raccoglie è come se diventasse il gestore di fatto e che addirittura può anche agire, ad esempio, sulla delocalizzazione. Volevamo sapere – se questo è vero, se diventa gestore e mi sembra evidente che sia vero – come si può evitare che questo avvenga. Con la disponibilità economica si riesce anche a creare un meccanismo di tracciamento e ad avere la possibilità di precludere queste manipolazioni? Magari non ce ne sono state, ma capisce bene che sarebbe abbastanza pericoloso se ci fossero.

Vorrei inoltre sapere quali requisiti dovrebbero avere queste certificazioni di qualità di cui ormai ci hanno parlato vari nostri auditi.

CATTANEO. Signora Presidente, inizio a rispondere partendo dal senatore Scarpinato. Se non sbaglio, lei mi ha chiesto se le nostre aziende forniscano anche le istituzioni di Intelligence in Italia. La risposta è sì: le nostre aziende riforniscono anche le istituzioni di Intelligence con gli apparati più diversi, nel senso che magari la mia azienda fornisce alcuni prodotti, un'altra azienda ne fornisce altri e così via. Sono esattamente gli stessi prodotti che vengono forniti anche alle Forze di polizia.

PRESIDENTE. Lei ha detto che sono uguali. Il senatore Scarpinato le chiedeva se esistono dei *software* israeliani, o di altre Nazioni, che voi

fornite ai Servizi diversi da quelli che fornite alla polizia giudiziaria e quindi all'autorità giudiziaria.

CATTANEO. Penso di poterle rispondere di no, nel senso che non ne sono a conoscenza ma, per quanto riguarda la mia azienda, le posso garantire di no. Non so se altre aziende forniscano *software* israeliani o di altri Paesi ai Servizi segreti. Noi forniamo solo prodotti che produciamo noi, sia nella parte *hardware* che *software*.

La senatrice Stefani mi chiedeva se i *file* estratti possono essere manipolati. Assolutamente no. I *file* che vengono presi dal captatore (*trojan* o virus) vanno direttamente nel *server* della procura della Repubblica che ha autorizzato, attraverso il decreto del magistrato, la captazione di un determinato *smartphone*. Per cui non può essere modificato. Tutte le operazioni che la polizia giudiziaria fa verso il captatore sono tutte tracciate.

STEFANI *(LSP-PSd'Az)*. Chiedevo anche se le tecnologie le elaborate *in house* e se quindi vi finanziate con quel che vi pagano.

CATTANEO. Assolutamente sì. Sostanzialmente, noi abbiamo solo un cliente, che è la magistratura. Anche i Servizi, però rappresentano una piccola parte percentualmente. Abbiamo solo un cliente e qualcosa all'estero, quindi ci finanziamo con quello che ci viene erogato.

PRESIDENTE. Le ricordo le mie domande. Rispetto ai *trojan*, ci hanno detto che il materiale captato non va direttamente al *server*, ma va in « nuvole » di cui il captatore diventa gestore.

A integrazione della risposta che stava dando alla senatrice Stefani, lei diceva che il vostro cliente principale è la magistratura e solo in parte i Servizi. Ci può fornire il dato percentuale?

CATTANEO. Una volta che il telefono viene intercettato, i dati vanno direttamente al *server* della procura della Repubblica. È ovvio che non passano attraverso una bacchetta magica, ma attraverso una rete che è la rete cellulare dello stesso telefono. In poche parole, se il suo *smartphone* è dotato di un captatore, sarà il suo stesso telefono che invia, attraverso un *software* che iniettiamo, direttamente alla procura della Repubblica, nel suo *server*, tutte le informazioni.

PRESIDENTE. Non ci sono quindi delle « nuvole » in cui sosta il materiale.

CATTANEO. Assolutamente non c'è nulla dove questi *file* si fermano, che siano *file* audio, fotografie, la rubrica telefonica o quant'altro. È tutto tracciato e non si ferma da nessuna parte. Per definizione, per spostare un *file*, o mi metto vicino al suo telefono, a trenta centimetri, a un metro di distanza, e le catturo i dati, oppure per forza di cose...

Quanto al dato percentuale, dico una cosa che può essere tutto e il contrario di tutto: sarà forse il 5 per cento.

PRESIDENTE. Il 5 per cento?

CATTANEO. La percentuale tra procura e Servizi: il 5 per cento sarà dei Servizi; ma forse neanche arriviamo al 5 per cento.

PRESIDENTE. La ringraziamo ancora per la sua disponibilità. Mi pare che al momento non abbia lasciato agli atti una relazione.

CATTANEO. Provvedo subito.

PRESIDENTE. Benissimo. Grazie ancora per il suo contributo.

Audizione dell'ingegner Lelio della Pietra

PRESIDENTE. I nostri lavori proseguono ora con l'audizione dell'ingegnere Lelio della Pietra, consulente di informatica forense, che saluto e ringrazio.

L'audizione si inserisce nell'ambito dell'indagine conoscitiva sul tema delle intercettazioni che sta svolgendo la Commissione.

Dopo la relazione introduttiva che dovrà essere contenuta in pochi minuti, ci sarà spazio per eventuali richieste di approfondimento da parte dei commissari a cui poi lei, ingegnere, potrà replicare.

Cedo dunque la parola all'ingegnere Della Pietra.

DELLA PIETRA. Un saluto a tutti voi, senatrici e senatori.

Come ha detto la Presidente, sono un consulente di informatica forense. Dopo aver seguito le precedenti audizioni in cui sono stati ascoltati i colleghi ingegneri Reale e Dal Checco, ho scelto per il mio intervento un approccio completamente diverso, per cui, anziché parlare genericamente dei *trojan*, vorrei portare alla vostra attenzione ciò che è avvenuto in un caso particolare, in occasione del quale si sono evidenziate delle manifeste patologie nel procedimento di acquisizione e detenzione delle tracce foniche provenienti dal captatore. Tali patologie, infatti, possono essere curate e, secondo me, è strategico che vengano curate al più presto, perché ne va della credibilità dello strumento e di tutte le indagini ad esso collegate.

Intervengo fondamentalmente come consulente nello stesso caso cui ha accennato l'ingegner Reale, vale a dire quello del *server* rinvenuto a Napoli. In qualità di consulente di parte mi è stata fornita tutta la documentazione estratta da tutti i *server* analizzati, la copia forense del cellulare su cui era stato inoculato il captatore e tutta la documentazione dei procedimenti disciplinari e penali collegati; mi è stato chiesto di incrociare il tutto al fine di evidenziare incongruenze e manomissioni.

Faccio un attimo un salto indietro dal punto di vista tecnico. Un captatore informatico, nel caso di specie era uno di quelli che registrava le conversazioni fra presenti, non è una microspia, nel senso che non registra ventiquattro ore su ventiquattro, ha dei limiti, perché il suo primo obiettivo è quello di non essere scoperto. Ove infatti il captatore venisse scoperto e segnalato alla casa madre del dispositivo (quindi Apple o Google), ciò significherebbe bloccare tutti i captatori prodotti da quell'azienda, per cui sarebbe un disastro. Per questo il captatore deve cercare assolutamente di mascherarsi, non deve scaldare il dispositivo, non deve consumare troppa batteria o troppa banda.

Nel caso di specie l'azienda suggeriva alla polizia giudiziaria di non utilizzarlo per più di otto ore: ciò vuol dire che di fatto parliamo di un dispositivo a pilotaggio attivo, nel senso che la polizia giudiziaria definisce i segmenti temporali nelle varie giornate in cui quel captatore deve captare e può farlo attraverso un'interfaccia, con la possibilità di creare un comando di captazione (registrando, ad esempio, un certo giorno dalle ore 10 alle 11), di modificare una captazione (portando, ad esempio, l'orario in avanti) o di cancellarla. Questo perché, nelle more di indagini diverse – magari ci sono anche pedinamenti o intercettazioni tradizionali – possono cambiare le esigenze e quindi può cambiare la scelta dei periodi di captazione.

Nel caso di specie a un certo punto si è reso necessario o opportuno analizzare i tracciati informatici (i cosiddetti *log*), sia dell'accesso alle tracce foniche per la redazione dei brogliacci, sia dei comandi inviati al captatore (il *log* delle captazioni). Qui c'è la prima sorpresa: l'informazione non viene estratta direttamente dalla polizia giudiziaria, ma viene fornita dall'azienda, segno evidente che la polizia non aveva modo di accedere direttamente a questo tipo di informazione. In effetti il *log* delle programmazioni, che è stato il cuore dell'analisi che ho effettuato, è stato fornito su carta intestata dell'azienda.

Guardando il *log* delle programmazioni appare immediatamente evidente che c'è qualcosa che non va: l'elenco dei comandi è fornito in ordine non cronologico e questo è un assurdo perché, ove ci sono dei comandi di modifica, ad esempio, è chiaro che l'ultimo prevale sugli altri, per cui i comandi vanno analizzati in ordine cronologico, altrimenti si rischia di non ricostruire la realtà delle cose.

Ma vi è di più: l'ordine in cui sono inseriti i comandi non è cronologico, ma alfabetico. Non entro nei dettagli, ma i due ordini coincidono, ove nella stampa della coppia data-ora l'ora sia scritta sempre a due cifre, per cui, ad esempio, invece di scrivere 9:30 venga scritto 09:30. Abbiamo 180 righe di *log* in cui ci sono date, sia nella colonna di invio del comando, sia nella colonna dei comandi stessi, quindi, ad esempio « capta in un determinato giorno ». Le date sono sempre scritte senza lo zero davanti (9:30), ma in sette righe che si riferiscono ai tre giorni *clou* dell'indagine compaiono misteriosamente degli zeri. Questo vuol dire che il *log* è ordinato alfabeticamente, ma in quei giorni, grazie agli zeri comparsi, è ordinato anche cronologicamente: in quei tre giorni, dun-

que, non si vede l'alterazione dell'ordinamento, che si vede invece negli altri giorni, nei quali, ad esempio, capita che un comando di modifica preceda il comando che sta modificando.

Sempre a guardare il *log*, poi, sembrerebbe che la polizia giudiziaria abbia compiuto delle operazioni...

PRESIDENTE. Ingegnere, mi scusi, ma affinché il linguaggio da lei usato sia accessibile a tutti, prima di parlarci del *log*, potrebbe spiegarci che cos'è il *log*?

DELLA PIETRA. Certamente. Il *log* – in realtà lo avevo detto prima – è il tracciato, l'elenco pedissequo delle operazioni che sono state fatte; è una tabella in cui sono indicati l'ora del comando, chi lo ha impartito e il dettaglio del comando.

Come dicevo, stando al documento che ci è stato fornito, in quattro casi la polizia giudiziaria avrebbe fatto un'operazione stranissima: invece di creare una nuova captazione, avrebbe modificato una captazione già conclusa, quindi retroattivamente, portandone in avanti la data di fine; la cosa non ha senso, perché la polizia ha un pulsante per creare una nuova captazione. In ben undici casi sono state effettuate operazioni di programmazione su programmazioni già cancellate: ovviamente questo è un assurdo logico.

Non solo; vi è anche il *login*, cioè il codice utilizzato per l'accesso dall'operatore che compie l'operazione. Sono tutti *login* costituiti dall'iniziale del nome più cognome, quindi, ad esempio, L.Della Pietra o G.Bongiorno. Tuttavia, una domenica, in una sola giornata, un non meglio identificato – quanto meno sulla base dei documenti in mio possesso – operatore Maurizio invia una bordata di comandi al captatore in quantità enormemente superiore a quelli inviati negli altri giorni. Questo Maurizio, per quanto di mia conoscenza, non si sa chi sia. Infine, e questa è una cosa di cui ha parlato anche la stampa, vi sono tredici casi di comandi di modifica o cancellazione di una captazione che non è nel *log*: di nuovo un assurdo.

Sono state chieste all'azienda spiegazioni in merito a questo comportamento. L'azienda ne ha fornite, anche se, osservando una peculiarità del *log* sulla quale non voglio scendere in dettaglio, riferisco che la spiegazione fornita è in realtà in contraddizione con lo stesso *log* in dieci casi su tredici; fondamentalmente la spiegazione non è coerente con i dati che sono nel *log*, cioè non regge.

A questo punto ho calcolato i periodi di programmazione sulla base di questo documento e ho visto in quali periodi sono arrivate le captazioni, che è la prova del nove. Premetto che per me quello non è l'esatto elenco dei comandi inviati al *trojan*. Sulla base di questa analisi, in cinque casi il captatore avrebbe registrato laddove non programmato per farlo, un po' come quando nelle cause esce fuori che il fucile ha sparato da solo: in questo caso il *trojan* avrebbe registrato da solo. In 22 casi vi sono stati poi lunghissimi periodi (nottate intere) in cui il *trojan* era pro-

grammato per captare e non è arrivato assolutamente nulla; peraltro uno di questi periodi è proprio la notte *clou* delle indagini, in cui il captatore alle ore 2 della notte smette di ricevere, laddove programmato per tutto il giorno successivo.

Infine, è stato analizzato il tracciato degli elementi pervenuti sul *server* che ha ricevuto le captazioni dal *trojan* e incrociato di nuovo con il DVD, con le captazioni, che è quello che viene normalmente fornito alle difese. Vi sono quattro audio che sul *server* risultano regolarmente ricevuti: se ne conosce l'ora di captazione, la durata fino al millesimo di secondo e l'ora di ricezione sul *server*. Inoltre, c'è una traccia che dice che questi audio sono stati trasmessi al *server* « archivio » che è a valle. Sul DVD questi quattro audio non ci sono, il che vuol dire che sostanzialmente sono spariti e non vi è modo di sapere cosa vi fosse in quelle quattro captazioni.

Si è poi verificato diciassette volte che un audio pervenisse sul primo *server* e rimanesse bloccato lì senza andare sul *server* archivio. Queste sono le evidenze in questo stranissimo caso.

Premetto che con la legge Orlando sono cambiate alcune cose. Innanzitutto è stato introdotto l'archivio digitale delle intercettazioni. Fondamentalmente, partendo dal presupposto che sia fatto a regola d'arte, è chiaro che nel momento in cui un elemento captato finisce in quell'archivio è sigillato per sempre. Però, rispetto al caso di specie c'è una differenza: per quanto mi risulta, i dati confluiscono nell'archivio digitale al termine del processo di intercettazione. Quindi, se l'intercettazione dura trenta giorni, vuol dire che quei dati restano trenta giorni nella pancia del *server* gestito dall'azienda, mentre nel caso di specie il dato arrivava subito al *server* di deposito, tant'è vero che si parlò di *server* di transito.

Segnalo una cosa per aggiungere una chicca: attenzione, perché con l'intelligenza artificiale sta diventando molto semplice contraffare le voci e anche i volti, quindi è fondamentale e strategico che un sistema del genere sia assolutamente blindato; nessuno si deve mai più permettere di mettere in dubbio la validità dei dati acquisiti da un captatore informatico. Si tratta di una questione veramente strategica importantissima.

Vengo quindi alla fase propositiva del mio intervento. È evidente che va tracciato tutto: ogni accesso alle macchine, ogni accesso all'interfaccia di programmazione, ogni accesso alle tracce foniche; la polizia giudiziaria deve poter estrarre ogni tipo di traccia senza chiedere l'intervento dell'azienda. In particolare, si tenga conto del fatto che le aziende possono intervenire sui sistemi per manutenzione e che questo può avvenire anche durante la notte. Sono infatti capitati casi di problemi notturni, per cui l'azienda remotamente è entrata nel *server*. Attenzione, non c'è un problema di fisicità, cioè non c'è qualcuno che entra nel *data center* della procura, poiché si interviene da fuori. È pertanto fondamentale che questi interventi siano videoregistrati. Non è che questo non si faccia: oggi ci sono dei casi in cui si fa, ma questo strumento non è della procura, bensì dell'azienda. Questo sistema di videoregistrazione deve entrare nell'artiglieria di sicurezza informatica del perimetro delle procure: queste ultime

non devono fare entrare un *server* nei propri *data center* senza avere un sistema per videoregistrare qualsiasi intervento venga fatto su questi *server*.

Aggiungo una procedura in uso ai protocolli informatici che potrebbe essere usata nei casi di specie e che in realtà in alcuni casi è già usata. I protocolli informatici, alla mezzanotte di ogni giorno, trasmettono in conservazione sostitutiva – è una specie di archivio digitale tipo le intercettazioni – le firme dei documenti ricevuti. Questo vuol dire che, una volta che la firma del documento è pervenuta in quell'archivio, la sequenza di protocollo non è più alterabile. Bene, bisognerebbe fare in modo che anche questi *server* che registrano le tracce foniche, o comunque quanto captato, trasmettano a *server* esterni delle procure qualsiasi evento di accesso e i dettagli delle tracce foniche. Questo potrebbe essere poi parte del controllo di integrità che viene effettuato quando le tracce vengono importate nell'archivio digitale delle intercettazioni, perché si potrebbe verificare che ogni elemento importato corrisponda a quella firma che è stata inviata da quel *server*. Quanto più frequente è l'invio (ad esempio, ogni ora), meno tempo si avrebbe per intervenire sugli elementi: vuol dire che si avrebbe al massimo un'ora per poter alterare l'elemento su quel *server*.

Dopodiché, come già è stato detto da tanti interlocutori prima di me, è opportuno che tutti questi sistemi siano certificati, sia i *software* sia le procedure.

Torno su un discorso che è stato fatto in alcune sedute precedenti, perché si è parlato di *trojan* onnipotenti che possono modificare il contenuto dei dispositivi. Un *trojan* è un *software*, pertanto se ad esempio voglio che un *trojan* modifichi gli SMS di un cellulare, devo inserire in quel *software* un pezzo di codice che modifichi gli SMS del cellulare; cioè, per poter fare una cosa, il *trojan* deve essere programmato per farla. È chiaro che un prodotto acquistato « a listino » dalle procure non dovrebbe poter fare una cosa del genere, quindi ci vuole qualcuno che preventivamente analizzi il codice del *trojan* e il codice del *server*, certificando che quel programma di captazione non faccia ciò che non deve fare e faccia bene ciò che deve fare. Questo tra l'altro sgraverebbe anche i procuratori della Repubblica dalla responsabilità di dover garantire il funzionamento dei *software* che acquistano, perché basterebbe acquistarne uno certificato. È esattamente quello che avviene, ad esempio, con i registratori di cassa o con un qualsiasi misuratore di tipo fiscale: sono preventivamente certificati.

Ovviamente, tutto ciò va fatto nelle more della delicatezza, della riservatezza e delle caratteristiche tecniche di un sistema del genere. Ad esempio, un sistema fiscale va ricertificato ad ogni modifica. In questi casi potrebbe capitare, ad esempio, un aggiornamento del sistema operativo del telefono che blocca il funzionamento del *trojan* e, dunque, la necessità di intervenire tempestivamente per ripristinare il funzionamento, prevedendo pertanto un eventuale funzionamento in deroga. A tal fine, do un altro suggerimento e mutuo l'esperienza dell'Agenzia per l'Italia di-

gitale (Agid), che non è solo un'autorità indipendente che emana norme, ma un vero e proprio punto di riferimento e centro di competenza per le amministrazioni pubbliche. Basta vedere i corsi che pubblicano i loro *forum*. Si potrebbe costituire a livello centrale un gruppo di riferimento, un centro di competenza, che possa servire anche come interlocutore per i responsabili dei CED delle diverse procure, i quali oggi non hanno interlocutori diversi se non i tecnici delle ditte che gli forniscono gli impianti. La costituzione di un gruppo del genere potrebbe irrobustire tantissimo il sistema.

BAZOLI *(PD-IDP)*. Signor Presidente, ringrazio il nostro audito, che ci ha raccontato di un caso nel quale è consulente di parte. Ovviamente, qui non siamo in un'aula di tribunale, non abbiamo la possibilità di avere un confronto tra consulenti e quindi non siamo in grado di apprezzare gli elementi che ci ha riferito riguardo al caso concreto illustratoci. Mi pare di aver capito peraltro che si trattasse di un caso antecedente alla normativa introdotta con il ministro Orlando, quindi forse non ci aiuta molto da questo punto di vista.

Lei, ingegnere, ci ha dato alcuni suggerimenti che però credo non fossero rivolti tanto a noi come legislatori, quanto forse al Ministero in sede di regolamentazione tecnica delle strumentazioni che devono essere utilizzate per la captazione, soprattutto tramite i captatori informatici. Mi pare che siano tutte cose che ci hanno detto anche altri auditi: la certificazione delle operazioni, la certificazione dei *software*, il controllo *ex post* delle operazioni fatte. Sono tutte cose che hanno più il livello del rango della normazione secondaria, regolamentare, che non quello della regolamentazione all'interno di un codice di procedura penale.

Lei però ha detto una cosa che a me sembra in contraddizione, se non l'opposto, di quanto ci ha riferito l'audito che abbiamo ascoltato prima di lei. Ci è stato detto infatti da chi l'ha preceduta che i *file* che vengono captati attraverso il captatore informatico vanno direttamente nel *server* delle procure che hanno autorizzato l'intercettazione, quindi senza passaggi intermedi, *server* intermedi, *cloud* e quant'altro. I *file* vanno direttamente nel *server* delle procure, quindi gli operatori privati non hanno alcuna disponibilità, neanche momentanea, di quei dati. Mi sembra invece che lei ci abbia detto una cosa diversa, cioè che in realtà transitano attraverso *server* loro e che quindi in sostanza non si potrebbe escludere in ipotesi addirittura la possibilità di un accesso e di una manipolazione di questi dati. Su questo vorrei un chiarimento.

SCARPINATO *(M5S)*. Signor Presidente, il senatore Bazoli mi ha in parte preceduto, quindi limito le mie domande.

Abbiamo capito – mi corregga se sbaglio, ingegner Della Pietra – che dopo la riforma Orlando-Bonafede tutto finisce direttamente nei *server* delle procure. Tuttavia, ho letto che c'è un problema di risorse, per cui molte procure non hanno *server* capaci di contenere tutte le intercettazioni e sono costrette pertanto a noleggiare *server* esterni. Vorrei sapere

innanzitutto se è così, perché questo diventa un problema di risorse che incide sulla sicurezza.

Se possibile, poi, ingegnere, vorrei che lei approfondisse i miglioramenti che ci sono stati rispetto a queste problematiche dopo l'entrata in vigore della legge Orlando, perché questo passaggio non mi è molto chiaro.

ROSSOMANDO *(PD-IPD)*. Signora Presidente, alcune delle domande che intendevo porre sono già state formulate dai colleghi che mi hanno preceduta, per cui ridurrò il mio intervento veramente all'essenziale, solo al fine di fare chiarezza su alcuni elementi che saranno poi oggetto della nostra riflessione.

Il caso che lei ci ha illustrato è evidentemente attinente ad una vicenda processuale: potrebbe indicarci soltanto la data precisa alla quale si riferiscono le attività di cui lei si è occupato?

DELLA PIETRA. Maggio 2019.

ROSSOMANDO *(PD-IPD)*. La ringrazio. Come direbbe anche la presidente Bongiorno, non ho nessun'altra domanda.

RASTRELLI *(FdI)*. Ingegner Della Pietra, vorrei soltanto un chiarimento.

Lei ha evidenziato una tematica specifica di ordine tecnico, ma è chiaro che questa tematica ha poi un'enorme ripercussione sotto l'aspetto politico per le implicazioni che produce. Lei ha detto che tecnicamente il *trojan* è un *software* che viene introdotto in un dispositivo: le chiedo se più correttamente può essere definito un *malware*, cioè un tipo di programma che va a modificare in profondità il dispositivo nel quale si inserisce.

Lei ha parlato poi della necessità di certificazione, tanto dei *software* che delle procedure che, come ci è stato riferito, è già in realtà il presupposto per le aziende private che forniscono questi dispositivi alla pubblica autorità. Vorrei quindi comprendere se, dal punto di vista del rimedio, il tema che ha posto un suo collega, cioè la garanzia della *blockchain* per una tracciatura *ex post*, può almeno in parte sanare il tema delle anomalie, colpose o dolose, nella gestione dei dati oggetto della captazione.

PRESIDENTE. Ingegner Della Pietra, vorrei rivolgerle anch'io alcune domande.

Innanzitutto, lei ha esposto una serie di anomalie in un caso da lei esaminato; sarebbe giusto sapere se poi c'è stata una sentenza che ha aderito a questa ricostruzione oppure se è la versione della difesa. Tuttavia, a prescindere da questo, mi interessa capire a che cosa siano ascrivibili le anomalie da lei riscontrate, anche se magari poi non sono state recepite. Lei ha sollevato degli interrogativi: sospettiamo che siano state le società ad alterare?

Inoltre, tutti i tecnici parlano della necessità di certificazioni di qualità e della necessità di tracciamento. Mi pare che l'ingegner Reale abbia parlato della possibilità di manipolare i dati nel momento in cui arrivano ad una « nuvola », per così dire, prima di giungere al *server* finale; l'audito che l'ha preceduta ha detto, invece, che c'è una specie di passaggio diretto, per cui nessuno può manipolare niente, nemmeno in astratto.

Premesso che tutti hanno detto che in concreto non c'è prova che si sia verificato, in astratto, secondo lei, ad oggi un *software* può essere costruito per manipolare? In caso affermativo, in base a quello che lei ha detto, sarebbe possibile prevenire questo con dei certificati di qualità? Questo è ciò che si intende dire?

DELLA PIETRA. Innanzitutto ritengo che sia opportuno un chiarimento, perché si è parlato di *server* e *server* in procura. Tutti i *server* che fanno parte di un processo di intercettazione sono in procura, cioè vengono comunque fisicamente allocati nei *data center* delle procure, eventualmente gestiti dalle aziende, le quali effettuano dei servizi di manutenzione sugli stessi.

Vi sono a questo punto due livelli: c'è il *server* che gestisce le programmazioni, le invia al *trojan* e riceve le captazioni, e poi c'è il sistema dell'archivio generale delle intercettazioni che è gestito dallo Stato, che assomiglia un po' alla conservazione sostitutiva, una sorta di archivio digitale di Stato. Quando finisce lì dentro, è sigillato per sempre; però, tutte le operazioni avvengono su *server* che sono fisicamente all'interno delle procure. Tutto il mio discorso di verificare gli accessi delle aziende era inteso quindi a verificare gli accessi su *server* fisicamente allocati all'interno delle procure.

Quanto alle risorse, di cui mi è stato chiesto prima, francamente non so rispondere; sono un consulente di parte e non appartengo al sistema della giustizia, per cui mi dispiace, ma non sono in grado di fornire una risposta.

In merito invece alla definizione di *malware* del *trojan*, bisognerebbe capire che cos'è un *malware*. Per me chiaramente qualcuno che registra quello che dico sta facendo qualcosa che non voglio; il *trojan* deve fare ciò che chi lo ha acquistato – e quindi lo Stato – gli chiede di fare, per cui bisogna mettersi in condizione di non acquistare mai un *software* che contenga pezzi di codice che modifichino il contenuto del telefono e torno di nuovo al discorso delle certificazioni. Possono essere inseriti all'interno dei *software* inviati sui telefonini. Tuttavia, un *software* fatto per manipolare un telefonino non è un *trojan*, ma uno strumento di criminalità informatica e quindi bisogna fare in modo che tale non sia ciò che viene acquistato.

In merito alla *blockchain*, si tratta chiaramente di uno dei sistemi che possono essere utilizzati per garantire l'integrità di tutta la catena di prove; l'importante però è che questo processo venga fatto su macchine esterne alla gestione dell'azienda, nel senso che i dati devono uscire quanto prima possibile – nella loro forma intera o comunque sotto forma

di dettagli del *file* – dai *server* delle aziende ed essere esportati verso *server* che sono sotto il controllo delle procure.

Ho proposto che, non appena arriva la captazione, ogni trenta minuti, ad esempio, il *server* dell'azienda depositi presso un *server* esterno i dati caratteristici della captazione.

PRESIDENTE. Quindi c'è un rimbalzo?

DELLA PIETRA. Non c'è un rimbalzo, il dato resta nel *server* dell'azienda; viene inviato fuori però una specie di segnale nel quale si dice, ad esempio, che alle ore 17,30 è arrivata una certa informazione, senza esportare tutta l'informazione. Quando poi si andrà a sversare l'informazione nell'archivio definitivo, si verificherà che i dati corrispondono con quelli che sono stati inviati al momento. Spero di essere riuscito a chiarire.

PRESIDENTE. Questo al fine di evitare cosa?

DELLA PIETRA. Questo al fine di non lasciare i dati all'interno del *server* ed evitare che possano essere manipolati. Anche se i dati restano là dentro, il fatto di esportare una caratteristica del dato su un *server* terzo impedisce qualsiasi manipolazione dopo che l'esportazione è avvenuta.

PRESIDENTE. Chi può fare questa manipolazione?

DELLA PIETRA. Può farla chi ha la possibilità di accedere al primo *server*, vale a dire quello che è in procura ed è gestito dall'azienda.

PRESIDENTE. Mi scusi ancora, ingegner Della Pietra, ma vorrei provare a fare un po' di ordine, visto che c'è una richiesta che è venuta un po' da tutti. I *server* ai quali si può accedere per manipolare, dove sono e chi può fare la manipolazione in astratto? Le chiedo di spiegarcelo in maniera chiara.

DELLA PIETRA. I *server* sono fisicamente all'interno delle procure e sono i primi con cui il *trojan* è a contatto. Le aziende hanno accesso per manutenzione a questi *server*, che non fanno ancora parte dell'archivio dell'intercettazione.

SCARPINATO *(M5S)*. Mi scusi, parliamo di manutenzione con accesso dall'esterno?

DELLA PIETRA. Parliamo di manutenzione, con possibilità di accedere da fuori perché, se si verifica un guasto alle ore 3 di notte, si deve intervenire. Per questo è necessario videoregistrare l'intervento.

PRESIDENTE. Per capirci tutti, visto che si tratta di una questione molto tecnica, lei dice: se potessimo avere una videoregistrazione, non fatta dalla stessa azienda (altrimenti coinciderebbero controllore e controllato), ma una sorta di videoregistrazione terza, potremmo avere la certezza che, nel momento in cui l'azienda facesse un accesso per una presunta manutenzione, non si andrebbe ad alterare. È corretto?

DELLA PIETRA. Esattamente. In questo modo ci sarebbe la possibilità di verificare quel che è accaduto.

RASTRELLI *(FdI).* Ho soltanto una domanda: ma la videoregistrazione di cosa?

DELLA PIETRA. Di tutto l'intervento, come se si facesse la registrazione del *monitor* dell'operatore e di tutto quello che fa.

RASTRELLI *(FdI).* Di tutti i comandi...

DELLA PIETRA. Esattamente.

PRESIDENTE. Ingegner Della Pietra, visto che il suo intervento è stato tecnico, può lasciarci della documentazione?

DELLA PIETRA. Signor Presidente, chiaramente questa è una consulenza di parte privata e credo ci siano ancora delle indagini in corso. Posso lasciare la mia consulenza, che contiene tutti i dettagli, se lei...

PRESIDENTE. No, se ci sono dati di una persona privata, non posso metterli a disposizione della Commissione. Assolutamente non posso.

DELLA PIETRA. Allora lascerò una sintesi dell'intervento.

PRESIDENTE. Ma senza nomi e cognomi.

DELLA PIETRA. Certamente.

PRESIDENTE. Ingegner Della Pietra, la ringrazio per la disponibilità e per il suo contributo.

Audizione del professor Gianluigi Gatta

PRESIDENTE. L'ordine del giorno reca infine l'audizione del professore Gian Luigi Gatta, professore ordinario di diritto penale.

Professore, a nome di tutta la Commissione, la ringraziamo del tempo che ci sta dedicando. La Commissione sta svolgendo un'indagine conoscitiva sul tema ampio delle intercettazioni telefoniche. A noi interessa conoscere il suo pensiero su questo strumento, pertanto avrà la possibilità di fare un intervento orale espositivo, da contenere possibilmente in circa dieci minuti. Seguiranno delle domande da parte dei commissari, dopodiché lei avrà di nuovo la parola per concludere il suo intervento più o meno nello stesso tempo indicato per la relazione introduttiva.

Cedo dunque la parola al professor Gatta.

GATTA. Signora Presidente, onorevoli senatori, permettetemi in primo luogo di ringraziarvi per l'invito a questa audizione e di esprimere i miei apprezzamenti anche sul piano del metodo per l'avvio di un'indagine conoscitiva sul tema delle intercettazioni.

Come ben sapete meglio di me, la giustizia penale è un terreno talmente complesso, al di là dei tecnicismi, che non c'è miglior metodo se non quello dell'analisi, dello studio dei fenomeni e dei problemi, come quello che state compiendo.

Sempre sul piano del metodo, come studioso della giustizia penale, mi permetto di dire che credo occorra evitare un rischio su questo tema, come su altri, che è quello della cosiddetta tela di Penelope, cioè di riformare ambiti senza tenere adeguatamente conto di precedenti riforme e senza misurarne gli effetti. In questo caso, la riforma delle intercettazioni, come sapete, è entrata in vigore nel 2020, ma ci sono anche altri ambiti: la riforma del processo penale, la riforma dell'abuso d'ufficio, la riforma della prescrizione. Come osservatore del sistema, credo che a livello di metodo sia importante, quando si riaprono dei cantieri, tenere conto dei lavori che sono già stati svolti e anche degli approfondimenti che sono già stati fatti.

Le intercettazioni sono un mezzo di ricerca della prova particolarmente insidioso perché lesivo del diritto alla riservatezza, alla libertà e alla segretezza delle comunicazioni. Sono uno strumento al crocevia dei diritti fondamentali, perché abbiamo: il bene fondamentale della riservatezza; gli interessi delle vittime dei reati da tutelare (vittime che attendono risposte dai procedimenti penali); l'interesse della collettività alla prevenzione della criminalità, perché le intercettazioni sono anche uno strumento di prevenzione; e poi abbiamo l'interesse della stampa alla narrazione dei fatti e delle vicende, che costituisce, come sappiamo, il sale della democrazia, con riferimento alla possibilità dei cittadini di conoscere i fatti e le vicende anche giudiziarie.

Il vero nodo problematico è pertanto quello di trovare un punto di equilibrio tra questi diritti fondamentali attraverso una serie di principi di cui tiene conto la nostra legislazione: la ragionevolezza, la necessità, la proporzionalità, la temporaneità e il controllo giudiziale. Mettere mano alla disciplina delle intercettazioni significa alterare degli equilibri; lo si può fare per raggiungerne di migliori – questo senza dubbio – però bi-

sogna fare attenzione a non creare dei disequilibri tra i diritti fondamentali in gioco.

Quanto alla proporzionalità, non è un caso che le intercettazioni siano l'unico mezzo di prova che può essere disposto solo subordinatamente al reato per cui si procede. Questo riflette appunto l'idea della proporzione dell'invasività dello strumento. Deve trattarsi, come sapete bene, di reati di una certa gravità: non solo quelli di mafia e terrorismo, ma tutti quelli puniti con l'ergastolo (per esempio, un omicidio premeditato comune), qualsiasi delitto non colposo punito con la reclusione superiore nel massimo a cinque anni, per cui abbiamo tutta una serie di reati tra cui la violenza sessuale anche di gruppo, lo *stalking*, il *revenge porn*, i furti in abitazione, il furto aggravato, l'inquinamento ambientale, il traffico di rifiuti, l'incendio boschivo, la calunnia, la contraffazione di monete, il caporalato, il favoreggiamento dell'immigrazione clandestina e anche l'istigazione per motivi di discriminazione razziale etnica e religiosa.

Le intercettazioni si possono disporre anche quando si procede per delitti contro la pubblica amministrazione, puniti con il massimo non inferiore a cinque anni, e altri reati (stupefacenti, pornografia e reati finanziari) che ben conoscete. Quindi si possono disporre anche per la criminalità dei colletti bianchi e questo mi sembra importante sottolinearlo, perché anche nel dibattito di questi giorni mi è parso che non sia stato sottolineato sufficientemente: penso, ad esempio, a grandi reati come la manipolazione del mercato e l'*insider trading*.

C'è un fenomeno che nella legislazione penale si è registrato negli anni scorsi, cioè quello di tendere a elevare le pene per consentire le intercettazioni. Anche questo è un fenomeno al quale bisogna fare attenzione. Più che limitare l'ambito delle intercettazioni, si potrebbe valutare se non sia il caso di stemperare qualche eccesso sanzionatorio, andando a incidere sulle pene.

Dicevo, non vedo una particolare esigenza di ridurre il novero dei reati (quelli che ho indicato sono già reati molto gravi), men che meno sul terreno della corruzione. Qui rischieremmo anche di andare in contrasto con le convenzioni internazionali, che ci richiedono uno sforzo anche sul punto delle indagini. Dobbiamo anche tenere conto di due fattori: un rapporto OCSE eccessivamente critico nei confronti dell'Italia e della magistratura italiana, che però purtroppo è stato depositato in occasione dell'ultima visita; in secondo luogo, proprio sul tema della corruzione internazionale, la vicenda a tutti nota di questi ultimi mesi. Sul piano internazionale, un passo indietro rispetto all'utilizzo di intercettazioni e per il contrasto della corruzione sarebbe avvertito molto negativamente.

Alcune cose si potrebbero fare: ad esempio, anche se può essere forse una curiosità, segnalo che è rimasta l'ingiuria nel catalogo per il quale sono ammesse le intercettazioni. Non è più un reato perché è stato depenalizzato, quindi andrebbe tolto.

Dicevo che le intercettazioni sono uno strumento lesivo da usare con estrema cautela e responsabilità sulla base di stringenti presupposti, che

conoscete e su cui poi vi lascerò un testo scritto: un controllo sull'esistenza dei gravi indizi di reato è un primo baluardo per evitare abusi; l'indispensabilità ai fini della prosecuzione delle indagini è un altro tema sul quale i giudici sono chiamati a un controllo; la responsabilità della polizia giudiziaria, che è la prima che ascolta; la responsabilità del pubblico ministero, che ne cura la trascrizione, e dei giudici; l'importanza del contraddittorio degli avvocati.

Non mi soffermo – perché la conoscerete benissimo – sulla riforma Orlando e sul sistema che è stato introdotto. La riflessione che farei in questa materia è di valutare se e quanto sia necessario modificare a livello normativo per migliorare la disciplina ed evitare possibili abusi, e quanto invece dipenda dai comportamenti, quindi dalla violazione di regole che sono già previste e che devono essere opportunamente sanzionate quando sia il caso.

Sarebbe interessante – forse lo avete già fatto e quindi quanto sto per dirvi potrebbe risultare inutile – acquisire, per esempio, i dati sui procedimenti disciplinari nei confronti di tutti gli attori coinvolti: penso ad eventuali ispezioni del Ministero nei confronti della magistratura, ai procedimenti disciplinari avviati anche nei confronti dei giornalisti o degli stessi avvocati o all'esame dei dati sui procedimenti penali derivanti dalla pubblicazione di atti arbitrari. Un'indagine conoscitiva dunque, a mio avviso, dovrebbe anche guardare i comportamenti.

Sottolineo poi l'importanza della formazione, anche in qualità di componente del Comitato direttivo della Scuola superiore della magistratura, che ogni anno organizza dei corsi per i magistrati anche sul tema delle intercettazioni, oltre che sulla deontologia. È opportuno che la formazione venga svolta anche per gli operatori della polizia giudiziaria, che magari hanno una cultura più legata all'individuazione dei fatti e della responsabilità, per cui si preoccupano meno delle garanzie, mentre dovrebbero essere i primi ad avere una sensibilità nel rapportarsi con il pubblico ministero su quali fatti sono irrilevanti ai fini del procedimento specifico. La formazione dovrebbe riguardare poi anche i giornalisti e gli avvocati.

Credo che il dato culturale sia molto importante nel nostro Paese, vale a dire la consapevolezza della gravità del mezzo che si sta usando, che potendosi equiparare ad un'arma, va usata con estrema cautela: ciò vale per il diritto penale, in specie, e per le intercettazioni, in particolare.

Scusandomi se mi sono dilungato troppo, chiudo questo mio intervento fornendovi alcuni dati, che forse già conoscete – non so se avete già acquisito dei dati statistici dal Ministero – e che mi sono preso cura di leggere e di provare a interpretare. I dati ci dicono che le intercettazioni dal punto di vista dei bersagli, quindi del numero di persone intercettate, sono in calo e non in aumento: c'è stato un picco nel 2013, quando furono 141.169; nel 2021, in base all'ultimo dato disponibile, risultano 94.800, per cui sono diminuite. Il dato del 2021, peraltro, è prossimo a quello del 2004.

Certamente si può fare un paragone con dati di Paesi stranieri, come ho visto che è stato fatto proprio ieri sera in un programma televisivo; ammesso che non so se quei dati siano attendibili o meno, c'è però una differenza sostanziale nel nostro Paese, che ha aree con infiltrazioni di criminalità organizzata a livelli tali che altri Paesi verosimilmente non hanno, quanto meno quelli europei che si sono confrontati. È interessante notare come il 38 per cento delle intercettazioni è effettuato dalle Direzioni distrettuali antimafia e che i distretti in cui le intercettazioni vengono maggiormente effettuate sono quasi sempre del Sud. Nel 2021, ad esempio, il 52 per cento di tutte le intercettazioni è stato effettuato in sei distretti italiani (Napoli al primo posto, poi Roma, Palermo, Milano, Catania, Bari), mentre il 55 per cento delle intercettazioni del 2021 è stato fatto in distretti del Sud; le stesse intercettazioni ambientali hanno visto Roma al primo posto, poi Napoli e Palermo.

Il Ministero dal 2021 ha anche i dati sulle intercettazioni informatiche e sui *trojan*. Per quanto riguarda specificamente i *trojan*, parliamo nel 2021 del 3 per cento delle intercettazioni, mentre il 5 per cento ha riguardato le intercettazioni informatiche, il 15 per cento quelle ambientali e il 76 per cento quelle telefoniche.

È verosimile che possano crescere le intercettazioni informatiche con uso di *trojan* per cui è sicuramente opportuno che l'impiego di questo strumento venga regolato meglio. È in grado, come so che è stato riferito a questa Commissione, di svolgere delle funzioni ben diverse dalla mera captazione di conversazioni: nel caso dell'acquisizione di *file*, ad esempio, a parte il problema della modifica, bisogna vedere come questi documenti entrano poi nel processo penale.

Direi che molti altri sono gli interventi puntuali che possono essere fatti, sempre però con questa prospettiva.

ZANETTIN *(FI-BP-PPE).* Benvenuto, professor Gatta, e grazie per la sua relazione.

Cercherò di essere molto sintetico, limitandomi a dare degli spunti.

Come lei ha detto, i presupposti per le intercettazioni sono certamente i gravi indizi di reità: parliamo dunque di presupposti teoricamente e astrattamente stringenti. Ciò premesso, le chiedo di illustrare alla Commissione la sua posizione sulle intercettazioni cosiddette a strascico e, soprattutto, sull'utilizzabilità in sede extrapenale dei risultati di queste intercettazioni. In base all'esperienza – è inutile citare i casi a lei, che è espertissimo – sappiamo che la fattispecie astratta ipotizzata dal magistrato è grave ed è quella che giustifica le intercettazioni, ma poi magari quella cade e quelle stesse intercettazioni vengono utilizzate in sede civile, penale, amministrativa, disciplinare. Vorrei sapere che cosa pensa lei al riguardo, visto che è un illustre studioso e ha avuto anche esperienze come consulente di Ministri e nelle commissioni ministeriali proprio in materia di revisione della normativa vigente.

Lei ha detto – e lo apprezzo molto, perché lei è uno studioso molto profondo – che lo strumento del *trojan* merita delle modifiche norma-

tive. Noi siamo qui anche per questo, per cui gradiremmo sapere se lei ha qualche idea da suggerire alla Commissione per migliorare la legislazione e renderla di maggiore garanzia per i cittadini.

Da ultimo, mi consenta una battuta polemica sul rapporto OCSE: sappiamo da dove quel rapporto è nato, vale a dire da un magistrato che ha visto le sue tesi non avvalorate in sede di dibattimento e si è lamentato perché il nostro Paese ha poche condanne in una certa materia, dimenticando che comunque in Italia abbiamo la presunzione di non colpevolezza e quindi non possiamo valutare la lotta alla corruzione o ad altro fenomeno criminale sul numero delle condanne comminate dai nostri tribunali.

SCARPINATO *(M5S)*. Professor Gatta, premesso che concordo interamente con la sua relazione, lei ha giustamente rilevato che il numero di intercettazioni giudiziarie in altri Paesi è inferiore rispetto a quello dell'Italia, anche perché in altri Stati non c'è la mafia, per esempio. Le chiedo, però, se le risulta che in altri Paesi, come la Francia, le intercettazioni utilizzate come prova processuale – e traggo questo dato dal lavoro svolto dalla Commissione giustizia nell'ambito di una precedente indagine conoscitiva del 2006 – sono effettuate solo in parte dalla magistratura (si parla di un 40 per cento), mentre il 60 per cento verrebbe effettuato dal Ministero dell'interno o da altra autorità, per cui la comparazione statistica dovrebbe essere fatta tenendo conto di tale dato.

C'è poi un secondo aspetto. A proposito del problema delle intercettazioni a strascico, mi chiedo se non sia necessario riflettere sul fatto che esistono delle forme criminali « a strascico ». Per esempio, quando io conducevo indagini sulla mafia, partivamo da un reato, che poteva essere un'estorsione, e durante l'ascolto venivano fuori manipolazioni di appalti pubblici, omicidi, truffe, perché appunto parliamo di un'associazione criminale che commette reati a strascico. Lo stesso può valere per comitati di affari dediti alla corruzione in modo seriale. Si tratta quindi di valutare se limitare le intercettazioni per il reato originario non significhi perdere le prove per tutti i reati a strascico che vengono consumati.

Infine, si è parlato oggi giustamente del principio della proporzionalità e cioè del fatto che il mezzo deve essere proporzionato alla gravità del reato. Tuttavia, leggendo l'articolo 266 del codice di procedura penale, mi accorgo che ci sono reati come l'ingiuria, la minaccia, la molestia o il disturbo alle persone con il mezzo del telefono per i quali non si è seguito il criterio della proporzionalità, ma forse un altro. Quello che intendo dire è che ci sono certi reati che non possono essere accertati se non con il telefono: penso, al caso, ad esempio, di una minaccia telefonica. Quindi forse il criterio della proporzionalità deve essere abbinato al criterio della natura del reato. Se i colletti bianchi non sparano in mezzo alla strada e non fanno rapine, ma fanno accordi nel segreto delle stanze, non è forse una metodologia di reato nella quale bisogna prendere in considerazione anche la modalità della condotta criminale, oltre che la proporzionalità?

BAZOLI *(PD-IDP)*. Signor Presidente, anch'io ringrazio e saluto il professor Gatta, che abbiamo un po' conosciuto e frequentato nella scorsa legislatura durante la fase della riforma Cartabia.

La mia è una domanda alla quale lei, professore, in parte ha già risposto e in parte era già stata formulata da altri colleghi. Lei ha detto che, sul piano comparativo, probabilmente il fatto che altrove risultino meno spese e meno bersagli intercettati rispetto all'Italia dipende dal fatto che in Italia c'è la criminalità organizzata, che altrove non c'è. Sotto questo profilo, le chiedo: a lei risulta, sul piano comparativo, che negli altri Paesi, dal punto di vista del perimetro di utilizzabilità delle indagini, ci sia una rilevante differenza rispetto all'attuale disciplina che c'è nel nostro codice di procedura penale? Sul piano comparativo, abbiamo una disciplina eccessivamente dilatata, che concede l'utilizzo delle intercettazioni in maniera troppo estensiva rispetto agli altri Paesi, oppure anche sul piano comparativo c'è una certa analogia che ci rende sostanzialmente in linea con quello che accade negli altri Paesi?

La mia domanda tocca quindi un tema che è un corollario dell'aspetto che riguarda il presunto eccessivo utilizzo delle intercettazioni nel nostro Paese.

SCALFAROTTO *(Az-IV-RE)*. Professor Gatta, vorrei porre anche a lei una domanda che ho fatto al Presidente dell'Autorità garante per la *privacy*. Siamo davanti a un caso in cui lo Stato è tenuto a contemperare beni giuridici differenti, che talvolta sono anche contrastanti l'uno con l'altro. Dal suo punto di vista di studioso del diritto penale e più ampiamente del nostro ordinamento costituzionale, lei ritiene che questi valori siano tutti perfettamente equiparabili o possiamo pensare che esista una gerarchia, nel senso che la violazione di uno di questi beni giuridici in discussione possa essere considerato un'eccezione rispetto alla regola?

SISLER *(FdI)*. Professor Gatta, ho ascoltato le sue parole e la mia è una domanda semplice che deduco da quanto lei ha detto. Innanzitutto apprezzo il fatto che anche lei ritenga sia necessario trovare un equilibrio tra il necessario dovere di combattere la criminalità e i diritti delle persone comuni a non vedersi violato un diritto fondamentale come quello della *privacy.* Anche perché – e riprendo una sua affermazione – le intercettazioni possono essere considerate un'arma; come tale, l'arma è pericolosa e va disciplinata, perché può essere utilizzata per combattere il male, ma anche contro un nemico politico, e credo sia un po' interesse di tutti che ciò non accada.

È interessante una sua affermazione: bisognerebbe indagare su quanti procedimenti ci sono nei confronti degli operatori del diritto globalmente considerati, e che esito hanno questi procedimenti. Evidentemente sono procedimenti che nascono perché si ritiene ci sia stata una violazione delle norme oggi esistenti sull'utilizzo delle intercettazioni. Chiedo se lei ha questi dati e alla Presidente domando se sia possibile acquisirli, perché ritengo sia importante comprendere.

PRESIDENTE. Senatore Sisler, in occasione del prossimo Ufficio di Presidenza chiederò ai vari Capigruppo, alla luce di questo primo ciclo di audizioni, se intendono chiedere dei dati, visto che molti degli auditi vi hanno fatto riferimento. Gli uffici hanno già fatto un elenco dei dati che sono stati oggetto di attenzione degli auditi; io stessa solleciterei l'acquisizione di alcuni dati. Al prossimo Ufficio di Presidenza ciascuno dei Capigruppo potrà chiedere e stileremo un elenco di tutti i dati che vorrete acquisire.

SISLER *(FdI)*. Concludo con un'altra domanda.

Professore, secondo lei, le norme poste a tutela e da cui scaturiscono poi i procedimenti sono efficaci? È chiaro che lo comprenderò dai dati statistici che riceveremo, ma vorrei una sua opinione circa l'efficacia. Le anticipo che personalmente ritengo che ciò non sia, ma questa è una mia opinione.

ROSSOMANDO *(PD-IDP)*. Signora Presidente, c'è una questione che scaturisce da quest'ultima domanda, ma che peraltro aleggia ormai in questi giorni più volte, comprensibilmente perché la materia è complicata. È una domanda un po' retorica. Premettiamo che l'impiego dello strumento è vincolato a precisi presupposti stabiliti dalle norme, ossia vi sono delle tipologie di reati anche in relazione alla pena irrogata e, a seconda della tipologia di reati, discutiamo anche di quale mezzo può essere impiegato. Stiamo discutendo molto, credo anche opportunamente, sotto il profilo tecnico dell'impiego del *trojan*, perché ha delle potenzialità ed alcune di esse le stiamo anche apprendendo (forse in futuro ne apprenderemo delle altre). La stessa normativa oggi vigente distingue ben tre diverse tipologie di impiego del *trojan*, dopo la riforma Orlando e dopo l'intervento del 2019.

Tra l'altro, segnalo a memoria di tutti che proprio al Senato abbiamo introdotto un'ulteriore limitazione che riguarda i reati contro la pubblica amministrazione. Era stata introdotta e ampliata la possibilità circa l'utilizzo del *trojan* rispetto alla riforma Orlando, ma proprio qui in Senato abbiamo introdotto un paletto in più, perché bisogna comunque indicare le ragioni. Ricordo inoltre che questo è avvenuto con uno specifico emendamento del Partito Democratico.

Detto questo, un conto sono i presupposti per poter effettuare le intercettazioni delle comunicazioni, ambientali e non ambientali, e i presupposti di legge per l'utilizzo di alcuni mezzi. Qui c'è ovviamente la sanzione processuale innanzitutto; e se c'è una violazione di questo tipo, ci sono una serie di conseguenze. Un altro conto è la violazione in merito alla pubblicazione – qui i dati statistici possono essere interessanti –, che riguarda una disciplina che ha avuto un'evoluzione. Ne abbiamo avuto riprova nella precedente esposizione del consulente tecnico, che ci ha ampiamente intrattenuto su un caso specifico in cui è stato consulente di parte, a proposito di tutta una sequenza di questioni avvenute nel 2019. Ricordo che la riforma Orlando è entrata in vigore dal 2020 e ri-

guarda fatti commessi a partire dal 2020; quindi, se si stava svolgendo un'indagine per un fatto del 2018, la riforma del 2020 non era applicabile. Pertanto abbiamo bisogno anche di questi dati per fare delle riflessioni. Questa è una distinzione da tenere presente.

Lei, professore, ci ha illustrato una serie di dati statistici. Può darsi che mi sia distratta, ma non ricordo se lei ha riferito anche della percentuale di intercettazioni che vedono l'impiego del *trojan*.

PRESIDENTE. Ha parlato di un 3 per cento, specificando di aver comunque preso il dato dal Ministero.

ROSSOMANDO *(PD-IDP)*. Perfetto.

Tra l'altro, signora Presidente, lei sulle intercettazioni ha una storia; direi che abbiamo un trascorso, che ricordo molto bene.

Faccio un'ultima osservazione. Siccome si è parlato più volte della regolamentazione del *trojan*, tema che è venuto più volte in evidenza anche nelle parole del Procuratore nazionale antimafia, che ha accennato proprio a questo, vorrei capire meglio. Quando si fa riferimento alla regolazione dello strumento – e su questo c'è una traccia normativa, visto che qualcosa si era detto anche nella riforma Orlando – si intende la regolamentazione dello strumento tecnico, cioè l'insieme di quei paletti e di quelle accortezze necessari affinché sia possibile solo un certo tipo di captazione e non un altro o vengono tenuti in considerazione anche altri aspetti? È venuto fuori, infatti, che sarebbe astrattamente e tecnicamente possibile addirittura programmare o modificare. Vorrei una risposta su questo.

RASTRELLI *(FdI)*. Professor Gatta, intervengo rapidamente per rivolgere al professore due domande, considerando la sua esperienza e l'autorevolezza della dottrina che rappresenta.

Vorrei sapere, innanzitutto, se ritiene opportuno incidere a livello propositivo sul catalogo dei reati, di cui all'articolo 266 del codice di procedura penale, con riferimento particolare a quelli indicati alle lettere *e)* e seguenti e poi se a livello sistemico la convince, al comma 2-*bis* con riferimento ai captatori, quella sorta di parallelo che c'è tra i reati ad altissimo allarme sociale e quelli contro la pubblica amministrazione.

PRESIDENTE. Professor Gatta, mi riallaccio ai quesiti che sono stati formulati sull'impiego del *trojan*, perché lei ha fatto riferimento alla possibilità di integrare la disciplina vigente.

Ricordo a tutti che uno degli scopi dell'indagine conoscitiva che la Commissione sta conducendo è proprio quello di suggerire eventualmente al Ministero delle regole e delle norme. Tra i vari strumenti di intercettazione forse il *trojan* è quello che personalmente mi ha colpito di più. Le chiedo dunque – mi pare glielo abbia chiesto anche il senatore Zanettin – in senso propositivo e costruttivo che cosa potrebbe proporre sul punto.

GATTA. Signora Presidente, ringrazio lei e tutti coloro che sono intervenuti per porre domande, alle quali spero di riuscire a rispondere in modo sufficientemente soddisfacente, anche perché so di non sapere tutto e molti di voi ne sanno più di me per l'esperienza maturata come magistrati, come avvocati e naturalmente anche come parlamentari.

Inizio proprio dalla sua ultima osservazione, signora Presidente, di natura propositiva. Premesso che naturalmente gli operatori, quindi i magistrati e gli avvocati, possono dare un contributo ben maggiore rispetto a quello di uno studioso, che comunque all'inizio della propria professione ha respirato un po' di polvere delle aule giudiziarie, alcune criticità riguardano indubbiamente le garanzie per gli avvocati – non l'ho sottolineato prima, ma lo faccio ora – quindi una maggiore attenzione all'effettività del contraddittorio.

Il riferimento è, innanzitutto, all'accesso materiale e fisico ai verbali delle intercettazioni o alle intercettazioni stesse, per cui bisogna vedere, ad esempio, come sono organizzate le stanze delle segreterie della procura. Occorre assicurare, inoltre, l'effettività dell'udienza stralcio, che si svolga e possa essere veramente funzionale a una selezione delle intercettazioni rilevanti e allo stralcio di quelle irrilevanti. Ci sono casi in cui, infatti, l'udienza stralcio – almeno questo mi è stato riferito e lo riporto *de relato* – di fatto salta a seguito della conclusione delle indagini preliminari (articolo 415-*bis* del codice di procedura penale) o per una richiesta di giudizio immediato. C'è dunque anche il tema dell'effettività dell'udienza stralcio.

Ci può essere poi un problema di disciplina del captatore informatico, come è emerso anche dalle domande. Direi che più che lasciare alla giurisprudenza il compito di definire a che titolo sono acquisibili i risultati captati del *trojan*, sarebbe opportuno che lo dicesse la legge. Bisogna considerare, infatti, che il *trojan* non consente solo di ascoltare, ma anche di riprendere e di acquisire documenti, che non sono un flusso di comunicazioni, ma sono altro: penso, ad esempio, ad un *file* di Excel prelevato da un telefonino in cui è diligentemente appuntata una serie di fatture false; sarebbe opportuno che l'acquisizione fosse disciplinata per legge.

Quanto al tema dello strascico, cui pure si è accennato, a rilevare è l'utilizzo del *trojan* in contesti domiciliari che nascono in indagini per reati non di criminalità organizzata. Può accadere – così come riferito da molti pubblici ministeri e come diceva anche il senatore Scarpinato – che si individui un reato di criminalità organizzata, partendo da indagini sul reato di criminalità comune. Così, se a casa la sera il marito racconta alla moglie di aver dovuto cedere a pressioni mafiose e di natura estorsiva, il *trojan* non può essere messo, perché in quel momento nella cucina di casa non si sta realizzando un reato: è un esempio che traggo, oltre che dallo studio su libri, anche dalla conversazione con avvocati e magistrati.

Un altro tema, che è stato toccato anche dalle domande, attiene al rischio, che è della legislazione penale in genere, di creare dei binari paralleli, spesso anche molto vicini: così vi è una disciplina per la crimi-

nalità organizzata, una per la corruzione, una per il terrorismo, una per i reati di violenza contro le donne. Tutto questo va benissimo, ma, al di là del fatto che in una logica di equilibri e di contemperamento tali regimi possono legittimare qualche deroga, non bisogna però dimenticare che non è sempre semplice, soprattutto in chiave investigativa, individuare qual è il reato di cui si sta parlando.

Quello del cosiddetto strascico effettivamente è un problema e ciò che mi sento di dire da questo punto di vista è cercare di uniformare e rendere omogenea la legislazione, perché che esistano tanti diritti e procedure penali, a seconda dell'ambito di cui parliamo, a livello di sistema può creare delle rotture, al di là del rischio che si dica che la mafia o la corruzione sono dappertutto, per esempio, in modo tale da poter applicare un certo regime a fenomeni diversi. Bisogna dunque stare attenti anche a questi eccessi.

Per quanto riguarda le questioni poste dal senatore Zanettin, concordo con il fatto che le intercettazioni inutilizzabili a fini penali dovrebbero esserlo anche a fini diversi, almeno in via di principio.

Quanto all'OCSE – peraltro sono stato audito personalmente, anche se il mio contributo, ma direi quello della dottrina in generale, non è stato molto valorizzato: non ci hanno fatto parlare molto per usare un eufemismo – è comunque un po' una pietra che pesa a livello internazionale. Sarà quindi opportuno trovare risposte adeguate, però è un tema politico, non tecnico, sul quale dunque non mi soffermo.

Quanto alle domande del senatore Scarpinato, effettivamente è vero che le intercettazioni di natura preventiva – quindi fatte dal Ministero dell'interno o dai Servizi segreti – in altri Paesi sono molte di più che da noi, per quanto ci è dato sapere e conoscere, perché dati non ce ne sono, che io sappia. Sicuramente concordo sul fatto che la forma preferibile è quella che ha un controllo giurisdizionale, questo mi sembra evidente.

D'altra parte, mi sembra altrettanto evidente che, nei limiti dell'estrema necessità, siano ammissibili anche quelle forme di intercettazione che non servono a cercare la prova, ma dovrebbero servire a evitare la commissione di reati. Se i Servizi segreti stanno intercettando per evitare che venga messa una bomba in una piazza, benissimo, che lo facciano anche al di fuori della procedura che conosciamo.

Il senatore Scarpinato ha fatto bene anche a precisare che il catalogo dei reati per i quali sono ammesse le intercettazioni non è pensato solo ed esclusivamente in rapporto alla gravità del reato. L'esempio lampante è quello della contravvenzione che lei ha citato, ossia le molestie telefoniche: in questo caso è la tipologia del reato che richiede l'intercettazione. Aggiungerei anche – questo potrebbe essere un consiglio – di valutare con attenzione se sono ammesse le intercettazioni per tutti i reati informatici o comunque effettuati spesso tramite la rete Internet, perché sulla rete oggi, come sappiamo, si verificano molte forme di criminalità, anche quelle che mettono a rischio soprattutto i ragazzi, i bambini e an-

che i giovani che passano le loro giornate, più di noi, con il telefono in mano.

La domanda del senatore Bazoli era sempre relativa al perimetro delle intercettazioni. Tutto sommato, a parte qualche aggiustamento, non interverrei; piuttosto penserei ai reati, a questa stortura che abbiamo vissuto nel sistema, ad esempio con la prescrizione: prima si aumentavano le pene per evitare che i reati si prescrivessero; poi si aumentavano per consentire la custodia cautelare e le intercettazioni. Tutto ciò dimenticando che invece il massimo edittale – almeno nella mia prospettiva, da penalista sostanzialista – dovrebbe principalmente, se non unicamente, segnare il disvalore penale del tipo del fatto. Questa è una stortura del sistema che non va alimentata; semmai, va ridotta.

Senatore Scalfarotto, per quanto riguarda la gerarchia dei valori, non sono un costituzionalista però nella giurisprudenza costituzionale è un principio oramai diffuso quello per cui non c'è un diritto tiranno rispetto agli altri; la via è quella del bilanciamento. Naturalmente nel bilanciamento c'è sempre qualcosa che pesa di più e qualcosa che pesa di meno. Qui davvero la materia è complicatissima. Credo che la materia delle intercettazioni sia tra le più complesse della procedura penale e della giustizia penale in senso lato per tanti motivi; intanto perché c'è un livello di tecnicismo più elevato del solito, e poi perché sono in gioco una serie di diritti fondamentali – come ho ricordato prima – e tanti valori. Bisogna quindi trovare delicati punti di equilibri e compromessi.

I dati che ho citato sono del Ministero della giustizia, e specificamente della Direzione generale di statistica (DG-Stat). Quando stavo al Ministero ho scoperto il sito Internet della DG-Stat, che è pubblico (però si fa fatica a trovarlo), e fornisce dei dati storici sulle intercettazioni: vanno dal 2004 al 2021 e contiene anche i dati del 2021, poi divisi per distretto. Sono dati che si trovano su Internet in una bella presentazione, in un Power Point del 2020, del Ministero. Se non li avete acquisiti, potrebbe esservi utile farlo.

Non ho i dati sui procedimenti disciplinari, ma secondo me sarebbe interessante acquisirli. Anche qui, da penalista sostanzialista rispetto al tema delle responsabilità dei giornalisti, ma anche dei magistrati (va detto che c'è anche il reato di rivelazione di segreti d'ufficio), ritengo sarebbe interessante su questo tema – e, se posso permettermi un leggero sconfinamento, anche su quello dell'abuso d'ufficio – considerare non solo la risposta penale, ma anche le possibili risposte extrapenali, quindi quanto le responsabilità di tipo diverso, come ad esempio quelle disciplinari, possano incidere.

Ho letto una bella intervista del presidente dell'ordine dei giornalisti, il dottor Bartoli, che conteneva degli accenni a questa materia e alla necessità di riformare il loro procedimento disciplinare, che è un qualcosa di cui mi aveva accennato quando ero al Ministero come consigliere della ministra Cartabia.

Penso di aver risposto anche alle domande del senatore Rastrelli e della senatrice Rossomando.

PRESIDENTE. Lei è stato consulente del ministro Cartabia?

GATTA. Consigliere, sì.

PRESIDENTE. La ringraziamo moltissimo per il suo intervento e per il contributo offerto ai nostri lavori.

Dichiaro concluse le audizioni odierne e rinvio il seguito dell'indagine conoscitiva ad altra seduta.

I lavori terminano alle ore 16,15.

Licenziato per la stampa dall'Ufficio dei Resoconti

€ 4,00