



Giunte e Commissioni

RESOCONTO STENOGRAFICO

n. 1

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

2^a COMMISSIONE PERMANENTE (Giustizia)

**INDAGINE CONOSCITIVA SUL TEMA DELLE
INTERCETTAZIONI**

11^a seduta: giovedì 12 gennaio 2023

Presidenza del presidente BONGIORNO

INDICE**Audizioni del Presidente dell'Associazione nazionale dei magistrati, del Presidente dell'Unione delle camere penali italiane e di un consulente di informatica forense**

PRESIDENTE	Pag. 3, 6, 7 e <i>passim</i>	* CAIAZZA	Pag. 10, 16, 17
RASTRELLI (<i>FdI</i>)	7, 24	REALE	17, 19, 25 e <i>passim</i>
SALLEMI (<i>FdI</i>)	15, 24	SANTALUCIA	3, 7, 10
* SCALFAROTTO (<i>Az-IV-RE</i>)	14, 23		
SCARPINATO (<i>M5S</i>)	6, 9, 12 e <i>passim</i>		
STEFANI (<i>LSP-PSd'Az</i>)	13		
ZANETTIN (<i>FI-BP-PPE</i>)	6, 14, 21		

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 dell'Associazione nazionale magistrati, dottor Giuseppe Santalucia, il presidente dell'Unione delle camere penali italiane, avvocato Gian Domenico Caiazza, e il consulente di informatica forense, ingegner Paolo Reale.

I lavori hanno inizio alle ore 9.

SULLA PUBBLICITÀ DEI LAVORI

PRESIDENTE. Comunico che, ai sensi dell'articolo 33, comma 4, del Regolamento del Senato, 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 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.

PROCEDURE INFORMATIVE

Audizioni del Presidente dell'Associazione nazionale dei magistrati, del Presidente dell'Unione delle camere penali italiane e di un consulente di informatica forense

PRESIDENTE. L'ordine del giorno reca l'indagine conoscitiva sul tema delle intercettazioni.

È oggi prevista per prima l'audizione del Presidente dell'Associazione nazionale dei magistrati, che ringrazio per essere qui.

Faccio presente che tutto ciò che nella seduta odierna non potrà essere espresso per ragioni di tempo o per altro motivo, potrà essere raccolto in successive memorie che verranno depositate presso gli uffici della Commissione e che saranno prese in considerazione.

Cedo quindi la parola al presidente Santalucia affinché possa svolgere la sua relazione preliminare, alla quale seguiranno eventuali domande da parte dei commissari.

SANTALUCIA. Signor Presidente, ringrazio lei e tutti gli onorevoli senatori.

L'oggetto della vostra indagine conoscitiva è estremamente ampio. Mi limiterò quindi a concentrare l'attenzione su alcuni aspetti del tema di una possibile riforma delle intercettazioni, ricordando che una delle que-

stioni sensibili è la riservatezza del materiale intercettativo, che può coinvolgere anche terzi estranei alle indagini.

Su questo versante – su cui il Ministro della giustizia, nelle sue dichiarazioni pubbliche, ha molto insistito – vorrei ricordare che vi è stato un significativo intervento di riforma della legislazione in materia di intercettazioni: nel 2017, poi nel 2019, infine nel 2020 con l'approvazione della legge n. 7 di conversione del decreto-legge n. 161 del 2019, che ha apportato modifiche non di poco conto.

Si dice nel codice – la cosiddetta legge Orlando lo diceva in maniera ancora più precisa – che tutto il materiale intercettativo che non rileva a fini di indagini e di prova è segreto ed è affidato a un archivio digitale sotto la direzione e sorveglianza del procuratore della Repubblica. Si pone sostanzialmente un segreto d'ufficio, la violazione del quale comporta responsabilità importanti sotto il profilo penale della rivelazione di segreti d'ufficio.

Con il decreto legislativo n. 51 del 2018, di attuazione della direttiva europea sulla tutela dei dati personali in materia di indagini penali, si è previsto uno strumento a tutela di chiunque sia interessato in atti del procedimento penale dalla divulgazione indebita di propri dati personali, che ha la possibilità di rivolgersi al giudice e chiedere l'eliminazione, la cancellazione e la rettifica del provvedimento – *ex* articolo 14 del decreto legislativo n. 51 del 2018 – che in questa sede l'allora garante per la *privacy*, l'onorevole Soro, disse essere uno strumento importante di tutela della riservatezza dei terzi. Gli indagati avevano già la possibilità di rivolgersi al giudice, ma oggi anche il terzo estraneo alle indagini può rivolgersi al giudice e chiedere che una determinata notizia che lo riguarda sia cancellata, eliminata, rettificata o comunque limitata.

Si tratta di uno strumento importantissimo a tutela della riservatezza. Vi è in più un obbligo per il pubblico ministero di vigilare sulle attività di verbalizzazione, i cosiddetti brogliacci di ascolto della polizia giudiziaria; un obbligo che, ovviamente, essendo funzionale ad evitare indebiti danni alle parti, potrebbe trovare anche una sanzione di ordine disciplinare.

Potrete sentire i pubblici ministeri che, con questi meccanismi di salvaguardia della riservatezza del materiale intercettativo, giocoforza hanno anche in parte diminuito la loro capacità di intercettazione. Infatti, bisogna avere un vaglio, un'attenzione, un controllo, non solo a valle, quando il materiale intercettativo viene consegnato dalla polizia giudiziaria delegata all'ascolto, ma durante l'ascolto; il che significa un dispendio di energie importanti, un controllo e una vigilanza che, non potendo i pm fare tutto, diminuisce la loro capacità intercettativa. Credo che su questo si possa lavorare forse per migliorare i meccanismi di impermeabilità tra il procedimento penale e l'esterno per quanto attiene al materiale irrilevante.

Il materiale rilevante entra nel fascicolo del processo, quindi nel dibattimento, e dunque viene trattato come qualunque altra informazione. Per contro, rispetto al pericolo di una proiezione all'esterno di notizie che

non riguardano i reati né le indagini o il tema di prova, e che possono ledere la riservatezza d'immagine, il decoro, la reputazione, ci sono importanti norme nel codice che possono essere implementate, ma la direzione è chiara: la violazione del segreto e l'individuazione molto precisa del responsabile del segreto, ovvero il procuratore della Repubblica, che è il responsabile della tenuta dell'archivio digitale delle intercettazioni, mi sembrano presidi importanti.

Sul tema dei costi, sentirete certamente i procuratori della Repubblica, che vi diranno meglio di me quali sono le spese. Già con la legge di bilancio, la n. 197 del 2022, c'è stata una diminuzione del *budget* a disposizione delle intercettazioni – se non erro, al comma 880 – proprio perché si sono completati quei meccanismi di controllo sui costi delle prestazioni funzionali alle operazioni di intercettazione. Quindi, già il *budget* è diminuito, ma vorrei anche dire che non si può guardare ai costi delle intercettazioni senza guardare alla capacità dell'amministrazione della giustizia di recuperare le spese processuali.

Abbiamo una capacità di recupero delle spese processuali, cui vengono condannate le parti, che è assolutamente irrisoria; quindi, i costi delle intercettazioni possono apparire, visti in assoluto, molto importanti, ma se si considerasse quanto consentono di recuperare in termini di risorse, e che l'amministrazione della giustizia non è in grado oggi di recuperare, il tema dei costi verrebbe assolutamente ridimensionato.

Credo di non errare se dico che oggi la capacità di recupero dell'amministrazione della giustizia delle spese processuali è dell'ordine del 3-4 per cento. Quindi, non si può fare questo tipo di comparazione senza tener conto del fatto che l'amministrazione della giustizia potrebbe fare di più, recuperando molto di più, diminuendo così l'impressione sui costi.

Quanto al catalogo dei reati, quello contenuto nell'articolo 266 del codice di procedura penale, sta lì da tempo; non credo che si possa diminuire ulteriormente l'area dei reati per i quali è ammissibile l'intercettazione; è una norma che non è stata modificata nel tempo e si riferisce a reati particolarmente gravi.

Alla luce di una giurisprudenza della Corte di cassazione, a Sezioni Unite – la conoscerete certamente – si è limitata ulteriormente la possibilità di utilizzare le intercettazioni per reati che non sarebbero intercettabili (si tratta della cosiddetta sentenza « Cavallo », n. 51 del 2020). Il bisogno di diminuire l'area delle intercettazioni da parte della magistratura – parlo per l'associazione che rappresento – sinceramente non lo vedo; non credo che questa sia una priorità tra le cose da fare, specie quando si tratta di contrastare un crimine che ha, nel contesto omertoso, il suo terreno di coltura.

È stata fatta recentemente la scelta di eliminare i reati contro la pubblica amministrazione dal catalogo dell'articolo 4-*bis* della legge 26 luglio 1975, n. 354: scelta assolutamente legittima, ma vi renderete conto che se si eliminano da quel catalogo, che è l'incentivo alla collaborazione in un contesto di omertà in cui nascono, i reati di corruzione, allora bisogna consentire che gli strumenti investigativi siano tali da superare quel

contesto di omertà. Se, infatti, si disincentiva la collaborazione e si diminuisce la capacità investigativa, su quel versante saremo scoperti. È un dato di logica elementare. Mi fermerei con la mia introduzione.

PRESIDENTE. Do la parola al senatore Zanettin che ha chiesto di intervenire.

ZANETTIN (FI-BP-PPE). Dottor Santalucia, vorrei focalizzare il mio intervento in particolare sul tema del *trojan*.

Come credo lei sappia, perché ha avuto un ampio risalto mediatico, ho proposto di ritornare alla disciplina *ante* spazzacorrotti, e cioè di limitare l'uso del *trojan* soltanto alla logica del doppio binario, che tutti condividiamo, quindi per i reati di mafia e terrorismo, escludendolo invece per i reati contro la pubblica amministrazione (come originariamente previsto dal testo Orlando, tanto per essere chiari).

Nell'immediato questa mia proposta ha destato anche un po' di scandalo, soprattutto fra ex magistrati che poi si sono dati alla politica più di recente, ma ho invece molto apprezzato il dibattito che si è aperto, anche all'interno della magistratura. Cito l'articolo di Nello Rossi, che certamente non le sarà sfuggito, perché, dal punto di vista del mondo associativo e della magistratura, è su una posizione diversa rispetto alla mia militanza politica ma che ha dimostrato di aprire un ragionamento. Nello Rossi è direttore di « Questione Giustizia », una famosa rivista di Magistratura Democratica, tanto per dirlo anche ai colleghi. In questo ragionamento, non dico che la mia proposta sia stata condivisa *in toto*, ma certamente è stata apprezzata.

Vorrei capire se all'interno dell'Associazione nazionale magistrati ci avete ragionato, qual è la vostra posizione e come la pensate, considerando che questo non deve essere un *tabù* perché invece è un tema serio che, lo ripeto, anche all'interno della magistratura è oggetto di dibattito.

SCARPINATO (M5S). Signor Presidente, a proposito delle spese delle intercettazioni, il presidente Santalucia ha giustamente rilevato che c'è il tema del potenziamento della capacità dello Stato di recuperare le spese processuali.

Le chiedo però, presidente Santalucia, se non sia necessario considerare anche un altro fattore e cioè che, grazie alle intercettazioni, lo Stato ha avuto la possibilità di confiscare beni del valore di vari miliardi di euro: ricordo che, nel triennio in cui ho diretto il Dipartimento mafia ed economia di Palermo, abbiamo sequestrato 2,6 miliardi di euro – l'equivalente di una piccola finanziaria. Le chiedo anche se è possibile una limitazione delle intercettazioni in un settore estremamente sofisticato della criminalità, quale quello del riciclaggio, che utilizza metodi molto complessi nel lavaggio del denaro, muovendosi anche nei paradisi fiscali e se la riduzione dell'operatività delle intercettazioni possa, per un verso, diminuire la capacità dello Stato di recuperare risorse e, dall'altro, rivelarsi in un potenziamento delle capacità delle organizzazioni più sofisticate di sottrarsi alle indagini.

RASTRELLI (*Fdi*). Signor Presidente, approfitto anch'io per ringraziare il presidente Santalucia per la presenza e la disponibilità.

Presidente Santalucia, ne approfitto per chiederle alcuni dettagli informativi su un altro tema delicatissimo: la tenuta e la gestione degli archivi. Sappiamo tutti che le intercettazioni telefoniche vengono elaborate e custodite in una serie di archivi digitali e in uno documentale. Sotto questo profilo, la riforma Orlando originariamente aveva immaginato che la tenuta e la gestione degli archivi dovessero essere sotto la responsabilità del pubblico ministero che aveva gestito la specifica indagine; poi è intervenuto il decreto del 2019 che ha spostato questa competenza in capo al procuratore, con la percezione di un equivoco, per cui ogni singola procura poi informa a criteri tutti propri la gestione, l'accesso e la fruizione di questi archivi, senza che vi sia una cornice-quadro entro la quale disciplinare l'accesso e la fruizione dei dati contenuti negli archivi.

Le chiedo quindi se e in che misura, a suo avviso, questo potenziale *vulnus* rispetto a dati estremamente sensibili possa essere colmato.

PRESIDENTE. Se non ci sono altri interventi, mi limito a integrare con un paio di brevissimi quesiti.

Presidente Santalucia, ha fatto cenno alla segretezza che hanno alcuni dati, che riguardano le intercettazioni telefoniche. Tuttavia, spesso questa segretezza purtroppo viene violata e, quando si fanno denunce, non si riesce mai a ricostruire da dove viene la talpa, se ce n'è stata una, o se sono gli avvocati che fanno uscire le intercettazioni.

A me interesserebbe in termini propositivi un suo intervento per capire se e come questo aspetto può essere migliorato.

Sempre visto che siamo quelli che si occuperanno della materia, abbiamo compreso il suo pensiero, ma nella pratica lei può dare qualche suggerimento su interventi normativi o ritiene che sia meglio lasciare la legislazione così com'è?

SANTALUCIA. Inizierei dall'osservazione del senatore Scarpinato, perché concordo con quello che ha detto: le intercettazioni sono uno strumento importantissimo per accertare reati di criminalità economica significativi e ovviamente, se venissero depotenziate e diminuisse la capacità di intercettare quel tipo di criminalità, anche la capacità di sequestrare e confiscare patrimoni illeciti verrebbe depressa. La comparazione dei costi va fatta quindi sia sulla capacità dell'amministrazione della giustizia di recuperare le risorse e le spese a cui vengono condannati i soggetti – ed è una capacità talmente modesta, che meriterebbe l'attenzione dell'amministrazione e del Parlamento, perché bisogna innalzare la percentuale di capacità di recupero – sia sotto il versante della capacità di intercettare patrimoni illeciti di rilevante entità.

Su questo, la sua domanda era suggestiva, nel senso che già conteneva la risposta, su cui convergo.

Quanto alla domanda sul *trojan* del senatore Zanettin, che mi sembra più complessa, è vero che si è aperto un dibattito interno i cui risul-

tati non sono in grado di consegnare oggi alla Commissione. Vi è la posizione di « Questione giustizia », che ha ricordato il senatore Zanettin, del collega Rossi, e vi sono altre voci contrastanti. Avrò modo, anche solo con uno scritto, di segnalare lo stato dell'arte.

Vorrei dire che la legge Orlando non ha creato un doppio binario, così come anche l'articolo di Nello Rossi ha indicato, nel senso che in essa si dice che il *trojan* sui dispositivi elettronici portatili può essere uno strumento d'intercettazione ambientale tra presenti: ai sensi dell'articolo 266, comma 2, si è intercettabili tra presenti in tutti i casi in cui lo si è ai sensi dell'articolo 266, comma 1; cioè per tutti i reati per cui oggi si è possibile oggetto d'intercettazione si diventa possibile oggetto d'intercettazione tra presenti. L'intercettazione tra presenti si può fare anche con un *trojan* inserito su un dispositivo elettronico portatile, anziché con la microspia nella cornetta telefonica.

Ovviamente, in ambito domiciliare, salvo che non si tratti di reati di mafia, si deve avere la prova che si stia consumando un'attività criminosa. Questo è venuto meno con la legge spazzacorrotti, cioè un'equiparazione totale dei delitti di mafia e terrorismo e dei delitti di corruzione, quindi, anche se non c'è la prova della consumazione in atto di un'attività criminosa di corruzione e concussione, si può violare il domicilio, ma è solo questa la differenza. Credo che nell'articolo di Nello Rossi ci sia qualche imprecisione.

Dopodiché, farò certamente il mio dovere consegnandovi il dibattito, perché bisogna indagare – ma su questo i procuratori della Repubblica potranno dire meglio – quali siano le connessioni tra crimine organizzato, delitti di corruzione e reati contro la pubblica amministrazione giacché, se il legame è così stretto e connesso, un doppio binario molto più accentuato potrebbe essere un pericolo per le indagini.

Sulla tenuta degli archivi, credo che l'articolo 89-*bis* delle disposizioni di attuazione del codice di procedura penale, che regola l'accesso all'archivio, sia particolarmente preciso.

Dopodiché, ho controllato il sito del Ministero della giustizia proprio ieri e ho visto le ultime circolari datate settembre 2020 del dipartimento dell'organizzazione giudiziaria che assicura il completamento della messa in sicurezza informatica (e non solo informatica) degli archivi (sono stati testati anche dal garante per la *privacy*). Se ci sono problemi, se ci sarà da uniformare le direttive di accesso all'articolo 89-*bis*, credo che l'amministrazione della giustizia può certamente intervenire. Se avete la pazienza vedrete che nel tempo sono state emanate varie circolari dal dipartimento dell'organizzazione giudiziaria e l'ultima, che data settembre 2020, ci assicura dell'avvenuta messa in sicurezza di tutti gli archivi. Inoltre, i soggetti possono entrare con una scheda che ne traccia l'ingresso e ciò è regolamentato a livello sia di legislazione primaria, sia di normazione circolare; se ci sono falle, su questo il Ministero della giustizia potrà intervenire più precisamente, in modo da dare direttive per la tenuta dei registri informatici e documentali. Non credo che ci siano interventi sotto questo profilo; l'articolo 89-*bis* mi sembra importante.

Il Presidente mi chiedeva se avessi suggerimenti per migliorare la tenuta della segretezza. Mi sento di dire che bisogna esser chiari sulla premessa: è un problema se vengono rivelate notizie irrilevanti e l'irrelevanza si stabilisce dentro il processo; tuttavia, se vengono rivelate notizie apprese nelle intercettazioni che sono rilevanti per le indagini, questo non è un *vulnus* alla segretezza, a meno di non introdurre per il materiale intercettativo uno statuto di segretezza diverso da quello di qualunque altro atto d'indagine. Mi viene da dire che se io ho una testimonianza, so qual è il regime di pubblicità dell'atto: l'articolo 114 del codice di procedura penale stabilisce chiaramente qual è il regime di pubblicità delle testimonianze. A meno che il legislatore non voglia creare una differenza tra la notizia che io apprendo dal teste e quella che apprendo dalla telefonata, io so perfettamente, senza lacune o falle, che se la telefonata è rilevante, quello è lo strumento, come indica lo statuto di pubblicità di cui al citato articolo 114: fino a un certo punto non possono essere pubblicate, dopo possono esserlo perché il processo è pubblico. Il problema sono le notizie irrilevanti. A mio avviso c'è una differenza tra la normativa attuale, che è frutto delle modifiche apportate al decreto legislativo n. 216 del 2017 e la cosiddetta legge Orlando nella sua formulazione originaria, in cui l'area della segretezza era un po' più chiara e precisa: se io violo un segreto d'ufficio e ho un soggetto che è responsabile della tenuta del segreto, credo che a livello di individuazione del centro d'imputazione delle violazioni non ci siano grandi difficoltà. Il procuratore della Repubblica deve vigilare sulla segretezza dell'archivio; se quell'archivio è segreto, è un segreto d'ufficio e non un segreto investigativo, perché viene tenuto il segreto sul materiale irrilevante, cioè su un materiale che non serve e pertanto la ragione del segreto è la tutela delle persone ed è un segreto d'ufficio. Se si fa un testo a fronte tra la cosiddetta legge Orlando e la legge attuale, che ha stemperato alcune disposizioni che erano più precise, si può chiarire quello che comunque è previsto: se è segreto, la violazione del segreto ha una responsabilità penale anche significativa.

PRESIDENTE. Presidente, mi scusi ma la interrompo un attimo, anche se di solito non lo facciamo, perché forse il senatore Scarpinato vuole integrare la sua domanda.

SCARPINATO (M5S). Signora Presidente, a proposito di questo tema volevo chiedere al presidente Santalucia se gli risulta che, proprio a causa del regime di segretezza stabilito dall'ultima legge sulle intercettazioni, si è verificato un grave problema per la Procura nazionale antimafia e antiterrorismo, nel senso che i procuratori della Repubblica distrettuali non si ritengono autorizzati dalla legge vigente a trasmettere le intercettazioni al Procuratore nazionale antimafia e antiterrorismo. Ciò sta provocando gravi problemi di coordinamento delle indagini, sino a quando non ci sarà un intervento legislativo che dirà che i procuratori della Repubblica non violano il segreto se trasmettono le intercettazioni

al Procuratore nazionale antimafia e antiterrorismo. Chiedo quindi se non ci sia un'esigenza di rimeditare anche l'apertura di canali istituzionali che, per un eccesso di segretezza, determinano una complicazione nella gestione di compiti istituzionali.

PRESIDENTE. Ringrazio il senatore Scarpinato. Tra l'altro, ovviamente il presidente Santalucia può rispondere, ma credo che noi audiremo direttamente il Procuratore nazionale antimafia e antiterrorismo la prossima settimana.

SANTALUCIA. Non ho notizie dirette da parte della Procura nazionale antimafia e antiterrorismo, ma comprendo il tema dell'area della segretezza. Ovviamente, poiché la legge afferma che quel materiale è segreto, se fossi un procuratore della Repubblica avrei difficoltà a superarla anche per esigenze di coordinamento, quindi mi rendo conto che il problema può sussistere.

PRESIDENTE. Ringrazio il presidente Santalucia ed attendiamo il contributo che ci ha promesso.

L'ordine del giorno prevede ora l'audizione del presidente dell'Unione delle camere penali, avvocato Gian Domenico Caiazza, cui do il benvenuto della Commissione.

Ringrazio il presidente dell'Unione delle camere penali, che è già stato sentito da noi su un altro tema, tra l'altro credo anche in altre legislature, quindi sa perfettamente come si svolgono i lavori.

Il tema di oggi è ampio e riguarda le intercettazioni. La Commissione, oltre a voler conoscere le sue idee e i suoi eventuali suggerimenti, chiede sempre qualche spunto concreto per fare in modo che poi le vostre idee possano trovare attuazione.

Lei ha già inviato una memoria che, ovviamente, sarà inserita negli atti della Commissione. Questa, infatti, è un'indagine conoscitiva e in tale sede qualsiasi memoria inviata sarà sempre lasciata agli atti. La memoria è a disposizione, pertanto chi vuole può prenderla anche adesso. I commissari naturalmente potranno fare ulteriori domande che prescindono dalla memoria, nei limiti in cui poi il Presidente vorrà e potrà rispondere.

A livello organizzativo temporale, sarà svolta per prima la sua esposizione, che si dovrebbe contenere in circa nove minuti, poi ci saranno delle domande, per un totale di quindici o venti minuti.

CAIAZZA. Signora Presidente, intanto ringrazio la Commissione per questo invito.

Il tema è ampio, quindi procederò rapidamente per punti sulle riflessioni che ci è parso più utile condividere con voi.

Il tema di cui si sta discutendo sono le intercettazioni preventive, l'anticipazione nella fase di polizia. Noi comprendiamo lo spirito e le intenzioni che animano questa proposta (ne abbiamo anche parlato direttamente con il Ministro), tuttavia riteniamo che essa rechi in sé dei peri-

coli. Il tema delle intercettazioni si misura con i principi fondamentali della Costituzione, della tutela della libertà di conversazione e di riservatezza; pertanto, l'idea di risolvere le abnormità del tema, le criticità dello strumento, anticipandole in una fase investigativa senza il controllo giurisdizionale, quindi di fatto ampliando la possibilità dell'ascolto e della violazione del principio costituzionale della riservatezza, è fortemente rischiosa. È vero che appartiene a democrazie mature, a sistemi giudiziari che funzionano; la verità è che noi non pensiamo di avere ancora una cultura democratica tanto strutturata per poter gestire uno strumento così delicato. Questo è, molto sinteticamente, il nostro punto di vista sul tema.

Apprezziamo molto, invece, l'intenzione del Governo e della maggioranza di rilanciare il tema. Rispetto alle possibili soluzioni concrete, alle vere ragioni di queste dinamiche che non funzionano e spesso anche dell'abuso di questo strumento, noi dobbiamo fare riferimento, tra l'altro anche ad arresti giurisprudenziali molto importanti (la sentenza a Sezioni Unite cosiddetta « Cavallo »), che hanno già stabilito un punto fermo, ma noi dobbiamo rafforzare quei principi e andare oltre. La nostra idea è che possono essere utilizzate solo le intercettazioni per i reati per i quali esse sono state autorizzate. Anche dopo l'intervento della sentenza cosiddetta Cavallo, è opportuno spezzare la catena dei reati connessi, dei reati che prevedono l'arresto obbligatorio, eccetera; occorre interrompere il percorso che permette la rete a strascico o la contestazione strumentale di reati più gravi per poter utilizzare le intercettazioni: è il caso classico della contestazione di associazione per delinquere in qualunque tipo di reato purché ci siano tre persone.

Il primo intervento forte a nostro avviso deve essere questo: l'intercettazione è utilizzabile solo per i reati per cui il giudice l'ha autorizzata. Tuttavia si dice che, ascoltando le intercettazioni, si può accertare che vi sia l'indizio della commissione di un reato più grave; ma questa allora sarà una notizia di reato, che imporrà un approfondimento investigativo. Da lì potranno nascere intercettazioni telefoniche disposte e autorizzate dal giudice, ma quell'intercettazione non deve diventare elemento di prova, perché altrimenti questo percorso non riusciamo a interromperlo.

Un tema a noi molto caro è quello delle conversazioni del difensore con l'assistito, ovviamente indirette. Naturalmente, se il difensore è indagato, ci mancherebbe altro, nessuno vuole uno stato di impunità; però qui stiamo parlando delle conversazioni indirette. Anche su questo occorre, a nostro avviso, un intervento decisivo, in cui si stabilisca che le conversazioni con il difensore sono sacre. Vorrei ricordare che la sentenza della Corte costituzionale sulla vicenda Napolitano, nel fissare il principio che non potevano essere nemmeno ascoltate le conversazioni del Presidente della Repubblica (estensore Frigo), non a caso, in un *obiter dictum*, dice che il Presidente della Repubblica è uno di quei casi, come il confessore nel confessionale e il difensore, che semplicemente devono essere protetti da ogni possibilità di ascolto. Cosa accade invece? Si viene ascoltati, la conversazione viene ascoltata dalla Polizia giudiziaria e dal pubblico ministero, viene valutato dal pubblico ministero se la conversazione

ha veramente per oggetto il mandato o se per caso non scantona dal mandato e, dopo questa valutazione, si ragiona se essa sia utilizzabile o meno. Nel frattempo io sono stato ascoltato e le mie strategie difensive sono state ascoltate. Anche su questo punto noi diciamo che si deve dare effettività al testo normativo, che seccamente dice che le intercettazioni tra difensore e cliente non sono utilizzabili.

Ci sono molte altre cose, ma forse è meglio rispondere alle domande. C'è poi il tema della pubblicazione; anche qui non possiamo continuare a girarci intorno. Facciamo l'esempio classico di un'ordinanza di custodia cautelare o di un decreto di sequestro che contiene, nella motivazione, alcune intercettazioni telefoniche. Si dice che, dal momento in cui è stata notificata, l'intercettazione è pubblicabile; ma questa è una logica perversa. Per quale ragione la sola circostanza che il destinatario del provvedimento abbia conosciuto quell'atto deve legittimare che esso sia conosciuto da qualunque lettore dei giornali? È un principio assurdo questa identificazione della pubblicazione con la comunicazione all'indagato. Le intercettazioni, nella fase delle indagini, devono essere coperte da un divieto di pubblicazione severamente punito. Non parliamo di punizioni detentive: si possono immaginare sanzioni pecuniarie fortissime, di tipo diverso, ma la pubblicazione nella fase delle indagini deve essere vietata senza « se » e senza « ma », senza questo ricorso specioso all'idea di pubblicità solo perché l'hanno ricevuta l'indagato e il suo difensore. Questa è una cosa inaccettabile.

PRESIDENTE. Lascio la parola ai colleghi che intendono porre domande.

SCARPINATO (M5S). Presidente Caiazza, lei ha affermato che le intercettazioni dovrebbero essere utilizzate soltanto per i reati per cui sono state autorizzate. Io ho una lunga esperienza in questo campo e la mia esperienza mi dice che, quando noi per esempio iniziamo un'indagine per associazione mafiosa, nel corso delle intercettazioni veniamo a conoscenza di tutta una serie di reati che possono andare dall'estorsione al sequestro di persona, alle percosse ed altro ancora. L'operazione finale poi si conclude con l'individuazione degli autori di questi reati e con i conseguenti arresti. In base alla sua tesi, se l'intercettazione è stata autorizzata soltanto per 416-bis, tutti questi altri reati non dovrebbero essere perseguibili. Per di più, non potranno essere perseguiti perché l'ultima riforma Cartabia prevede che i sequestri di persona, le violenze private e tutti questi reati, anche se c'è l'aggravante di mafia, sono perseguibili a querela. Noi quindi avremmo la conoscenza di una serie di reati, la cui perseguibilità sarebbe rimessa alla querela di un singolo che dovrebbe, con un suo atto d'impulso, sfidare un'intera organizzazione mafiosa chiedendo che quel sequestro di persona, quella percossa o quella lesione vengano perseguiti.

Mi chiedo se questo non può determinare un disarmo unilaterale dello Stato nei confronti di quelle organizzazioni criminali (mi riferisco

alla mafia, al terrorismo, ad associazioni corruttive complesse) che non consumano un solo reato, ma una pluralità di reati. Questo è uno dei motivi per cui in Germania e in altri Paesi, per esempio, non si hanno denunce di reati contro la mafia, perché la tecnica di quelle polizie e di quelle magistrature è di perseguire il singolo reato e di non perseguire l'associazione. Io ho avuto il caso di un ristoratore italiano che ha aperto un ristorante in Germania, a cui hanno fatto una richiesta estorsiva; lui ha denunciato alla magistratura tedesca quella richiesta estorsiva e la magistratura tedesca ha arrestato l'estorsore. Secondo i tedeschi, l'operazione era conclusa. Senonché due mesi dopo è arrivato un altro mafioso e gli ha detto: « Bravissimo, hai denunciato il nostro complice, da questo momento in poi tu pagherai il doppio. Se arrestano me ne verrà un altro, poi ne verrà un altro e poi ne verrà ancora un altro ». La conclusione è stata che il ristoratore ha chiuso il ristorante. In Italia questo non sarebbe successo, perché avremmo fatto delle indagini ad ampio raggio e non avremmo arrestato solo l'estortore, ma tutta la cosca. Questa è la prima considerazione.

La seconda riguarda le conversazioni tra l'avvocato e il cliente. Lei sa che ci sono stati casi recenti di avvocati che sono stati arrestati perché incontravano detenuti al 41-*bis* e portavano all'esterno messaggi di morte e istruzioni? Sono casi clamorosi, che sono finiti sulla stampa. Io mi sono occupato di diversi casi di questo genere.

In terzo luogo, per quanto riguarda la segretezza dei contenuti delle intercettazioni durante la fase delle indagini, le sembra realistico che venga emessa un'ordinanza di custodia cautelare che contiene necessariamente la trascrizione di intercettazioni, che finisce alla stampa e che determina un dibattito pubblico, ma che una parte di questa ordinanza di custodia cautelare, quella che riguarda le intercettazioni, debba essere censurata? Allora si stabilisca che non deve passare alla stampa neanche l'ordinanza di custodia cautelare; ma, come sa, c'è una discussione su questo punto. Questi atti, che hanno un grande impatto sociale, devono restare segreti sino all'udienza preliminare? Allora dobbiamo fare una modifica normativa per cui le ordinanze di custodia cautelare sono atti coperti da assoluto segreto e non devono finire fuori dalle mani dei singoli interessati.

STEFANI (*LSP-PSd'Az*). Buongiorno, presidente Caiazza. La ringrazio innanzitutto per tutte le attività di stimolo e di confronto che continua ad avere puntualmente con il Parlamento e con lo stesso Governo.

Abbiamo appena ascoltato un intervento del Presidente dell'Associazione nazionale magistrati, il quale ricorda una normativa formalmente stringente sulla rivelazione delle informazioni tratte dalle intercettazioni. In verità, sappiamo bene che vi sono delle falle. Anche se la mia è una domanda diabolica (del resto è una prova diabolica), le chiedo, anche in ragione della sua esperienza professionale e del riscontro che può avere da tutto il mondo dell'avvocatura, dove potrebbe esserci la falla.

Ancora, il presidente dell'Associazione nazionale magistrati dice che la rivelazione delle notizie irrilevanti è illegittima, mentre la rivelazione delle notizie rilevanti è legittima. Le chiedo, senza alcun intento provocatorio, se invece la rivelazione della notizia rilevante anche una volta venuto meno il segreto istruttorio, può essere di nocumento per la difesa della persona, tenendo conto che si crea spesso un interesse anche pruriginoso nei confronti di indagati che sono particolarmente esposti.

SCALFAROTTO (*Az-IV-RE*). In realtà, credo che la senatrice Stefani abbia centrato il punto.

Anche rispetto a quanto abbiamo ascoltato prima, sembra che queste modifiche normative siano irrilevanti rispetto al piano della realtà, nel senso che al di là della norma a tutela del segreto, il segreto viene normalmente rivelato; volevo pertanto capire, *de jure condendo*, visto che siamo qui per discutere di possibili modifiche, se il legislatore finora non abbia proprio mancato il bersaglio e cioè non abbia introdotto magari norme più o meno severe, le quali però non andavano a toccare la causa del problema. Il mio collega Scarpinato pochi minuti fa ha detto, ponendo una domanda, che addirittura le norme a tutela della segretezza impediscono ai procuratori della Repubblica di interloquire con il Procuratore nazionale antimafia. Mi chiedo, allora, se la norma non consente ai magistrati di parlare tra di loro, come mai i giornalisti invece le norme le hanno con grandissima semplicità aggirate. Sembra un po' paradossale che la norma sul segreto impedisca alla magistratura di lavorare, ma non impedisca la diffusione di notizie che sono di nocumento alla *privacy* delle persone e alla loro reputazione e non impedisca che magari conversazioni del tutto irrilevanti finiscano con estrema visibilità sui giornali, magari toccando la reputazione e la vita di persone che con l'indagine non c'entrano niente. Forse stiamo sbagliando proprio l'indirizzo, in altre parole stiamo operando sull'organo sbagliato.

ZANETTIN (*FI-BP-PPE*). Premetto che condivido pressoché tutto quello che ha detto l'avvocato Caiazza e quindi non mi dilungo troppo su questo aspetto. Sono stato però sollecitato dall'intervento del senatore Scarpinato con riferimento, in particolare, al fatto che giustifica l'intercettazione degli avvocati tenuto conto che alcuni avvocati – pochi, ritengo – violano gravemente i propri doveri, perché è del tutto ovvio che trasmettere informazioni a dei detenuti costretti al 41-*bis* o fare da tramite con i loro complici configuri una condotta illecita, ma non è che possiamo disciplinare la patologia. In questo caso, credo che poche mele marce non possano condizionare il rispetto assolutamente sacro – almeno per come la vedo io – delle conversazioni con i difensori. È del tutto evidente che in questa materia confliggono due diritti: quello di investigare e quello alla *privacy*. La *privacy* delle conversazioni o della corrispondenza è garantita costituzionalmente, è del tutto evidente che se noi diamo vita ad un « Grande fratello » orwelliano, se adottiamo i criteri che in questo momento pare applichi anche con l'intelligenza artificiale

la Cina per reprimere reati o dissidenti, probabilmente perseguiamo fino all'ultimo qualsiasi reato, ma non credo sia questo quello che vuole uno Stato democratico in cui ci deve essere un equilibrio fra i poteri. È meglio che sfugga alla sanzione penale qualche reato piuttosto che vengano indagati fino in fondo la coscienza e i comportamenti di tutti i cittadini.

Trovo molto sbagliato e addirittura mi spaventa questo approccio. Personalmente, come parlamentare, mi sento di dover garantire, invece, il diritto sancito dalla Costituzione trovando un punto di equilibrio fra le esigenze investigative, che pur ci sono, e la garanzia dei diritti costituzionali di libertà e di *privacy* dei cittadini.

Vengo alla domanda che vorrei fare, che è simile a quella che ho fatto prima al presidente Santalucia. È del tutto evidente che la pervasività in particolare del *trojan* è quella che più mette in discussione il diritto alla difesa. Faccio un esempio che è maturato l'altro giorno, in un'audizione in 4^a Commissione, quella sulle politiche dell'Unione europea, su un regolamento europeo sui diritti dell'informazione, dove ci è stato sollecitato di intervenire per evitare che il *trojan* possa, per esempio, riguardare anche i giornalisti, perché anche i giornalisti hanno delle fonti e quindi evidentemente anche questo diritto deve essere garantito.

Vorrei chiedere a lei, avvocato Caiazza, come valuta l'ipotesi, allo stato attuale, di limitare l'uso del *trojan*.

SALLEMI (*FdI*). Poc'anzi credo di aver intuito che il Presidente dell'Associazione nazionale magistrati abbia spiegato che, qualora delle notizie di carattere privato irrilevanti filtrassero dalle intercettazioni, chi viene danneggiato può comunque rivolgersi all'autorità giudiziaria o iniziare un procedimento nei confronti del responsabile che ha lasciato esfiltrare queste notizie.

Sappiamo, però, che nella fase delle indagini spesso delle notizie esfiltrano e vengono utilizzate, come ha detto lo stesso ministro Nordio, come una clava per attaccare questo o quell'avversario politico, questo o quel sindaco, questo o quell'assessore.

Nel mentre che si cerca di individuare il responsabile, intanto la vita di quel soggetto è stata sostanzialmente distrutta, politicamente azzerata. Qual è, secondo lei, il correttivo in questo senso? Quale può essere la soluzione per limitare quello che credo oggi sia uno dei problemi principali nel nostro Paese in ordine all'utilizzo delle intercettazioni irrilevanti?

PRESIDENTE. Come ha visto, ad alcuni commissari e anche a me interesserebbe il suo pensiero soprattutto sul tema della sistematica violazione della segretezza su atti irrilevanti. Come spesso avviene, le norme ci sono ma non vengono applicate e a mio parere il vero problema in Italia è che ormai bisogna predisporre norme per far applicare le norme. Le chiedo se può esplicitare in modo un po' più elementare, al di là dei massimi sistemi, la sua perplessità o la sua riserva rispetto all'allargamento delle intercettazioni preventive e se lei, rispetto al catalogo dei re-

ati previsti per le intercettazioni, ha rilievi da fare o meno. Io conosco la sua posizione anche su questo, ma vorrei che ci spiegasse meglio. Ovviamente può parlare genericamente o rispondere ai vari senatori.

CAIAZZA. La ringrazio, Presidente, perché avevo dimenticato questo punto cruciale, che è anzi una priorità per noi, e cioè, la riduzione del catalogo dei reati per i quali siano autorizzabili le intercettazioni. È un passo molto importante perché ancora una volta – rispondo anche al senatore Scarpinato – dobbiamo comprendere che l’intercettazione è un mezzo eccezionale perché violativo di un principio costituzionale.

Se girassimo tutti microfoni sicuramente le indagini sarebbero molto più semplici e la criminalità sarebbe fortemente prevenuta, ma vivremmo in un Paese nel quale io personalmente sarei terrorizzato a vivere. Quindi, o ci misuriamo con il limite costituzionale oppure è chiaro che qualunque limitazione che poniamo sembra una limitazione al potere d’investigazione.

Devo ribadire che quando si parla di inutilizzabilità per un reato diverso da quello che è stato autorizzato non parliamo d’impunità per quel reato; si dice che l’intercettazione per il reato diverso diventa una preziosissima *notitia criminis* in ordine alla quale, a partire da quella, si apre l’indagine anche sull’altro reato, ma non è utilizzabile quella specifica intercettazione che ha dato la *notitia criminis*.

Lei non deve rappresentare una proposta secondo la quale ci disarmino rispetto ai reati che emergono, perché è una deformazione di quello che diciamo.

Mi riporto a quanto detto dal senatore Zanettin per quanto concerne il colloquio avvocato-cliente: non è che, dato che ci sono avvocati mascalzoni, ascoltiamo tutti gli avvocati perché ci potrebbe essere un mascalzone; non si ragiona mai così nel diritto penale, e non solo nel colloquio con gli avvocati.

Sul ragionamento – che mi pare di aver capito abbia fatto il presidente Santalucia – in ordine alla rilevanza o meno, come facciamo questa distinzione? Chi la fa? E quando la facciamo? Dopo che l’intercettazione è stata pubblicata diciamo se era rilevante o irrilevante? Quello della rilevanza è un concetto molto fluido; quindi, qual è la proposta? Mi pareva di averlo detto e lo ripeto: nessun divieto funziona se non è sanzionato in modo serio.

Gli articoli 114 e 329 del codice di procedura penale comportano una multa irrisoria per chi pubblica l’intercettazione; allora, il divieto c’è ma è sanzionato in modo ridicolo. Non ci spaventiamo se poi si parla di legge bavaglio perché non è tale: è una legge che difende un diritto costituzionale. Quindi, la soluzione è molto semplice: una sanzione non detentiva, non la rappresentiamo come un’ipotesi di reato; parliamo di sanzioni pecuniarie per l’editore e diamo effettività a quel divieto.

In ordine alle intercettazioni preventive, è un discorso suggestivo; l’abbiamo detto anche nell’incontro che abbiamo avuto con il ministro Nordio, perché il ragionamento è chiaro: il tema non sarà mai utilizzabile

come prova, però diffondiamo in modo sostanzialmente incontrollabile. Se infatti non c'è il controllo giurisdizionale – se non c'è un giudice che dice all'investigatore cosa può ascoltare e cosa no – si tratta di uno strumento che può diventare di controllo anche politico in mano alle Forze di polizia. Quindi, da un lato, c'è la garanzia che quelle intercettazioni non potranno essere processualmente utilizzate ma, dall'altro, ampliando lo strumento dell'intercettazione investigativa, forniamo all'Esecutivo – a questo punto i soggetti coinvolti sono Polizia e Ministero dell'interno – una massa di informazioni acquisibili liberamente nelle conversazioni private; il che spaventa.

Non abbiamo sentito un ragionamento sul limite delle preventive, che non può essere solo il limite dell'inutilizzabilità, pur importantissimo, ma deve riguardare a monte l'eseguitività stessa dell'intercettazione.

PRESIDENTE. Presidente, è stato assolutamente completo.

È stata depositata una memoria, che è una sorta di esplicitazione di quanto è stato detto oggi, con qualche spunto, che potremo analizzare.

CAIAZZA. Sì, abbiamo allegato un nostro documento del 2020 dopo la cosiddetta riforma Bonafede; quindi, mi pare che il quadro sia abbastanza completo.

PRESIDENTE. La ringrazio ancora.

L'ultima audizione è quella dell'ingegner Reale, consulente d'informatica forense, che ringrazio per essere qui con noi.

Il tema è sempre quello delle intercettazioni, quindi, essendo lei esperto d'informatica, ci parlerà dei profili di suo interesse.

Per ragioni organizzative le chiedo di contenere la sua esposizione in tempi brevi, in modo che i commissari possano poi intervenire per porre domande e osservazioni alle quali potrà a sua volta rispondere.

REALE. Signor Presidente, ringrazio la Commissione tutta per l'invito a essere qui in questa sede prestigiosa.

Sono un tecnico, mi occupo di informatica forense in generale; non sto a descrivere il mio *curriculum*, eventualmente lascerò una nota scritta *a latere* in cui raccogliere questi elementi.

Venendo al tema in oggetto, negli ultimi anni in particolare ho lavorato sul captatore informatico: parliamo dello strumento che viene inoculato all'interno dei cellulari e da qui può acquisire le informazioni presenti all'interno, a partire dal microfono, quindi dall'ascolto delle conversazioni. Prima ancora di parlare del captatore, mi piace fare un passo leggermente indietro perché, molto spesso, mi capita di riscontrare, non solo sul captatore ma anche in tanti aspetti dell'informatica forense, che c'è una sorta di difficoltà a comprendere che il mondo digitale è molto diverso da quello fisico.

Siamo abituati nel nostro mondo fisico a capire al volo tutto quello che abbiamo intorno, i meccanismi, perché vediamo la maniglia, vediamo

l'ingranaggio; sappiamo e non abbiamo sostanzialmente sorprese perché vediamo e tocchiamo.

Nel mondo digitale non si può né vedere né toccare; le informazioni sono in uno stato invisibile; sono quindi meccanismi che non possiamo conoscere. Il punto di partenza è quindi la necessità di muoverci su questo terreno con un nuovo paradigma, con una nuova mentalità, con un approccio che necessariamente tenga conto di questa esperienza di tipo diverso.

Dico questo perché – e vengo direttamente al tema del captatore – mi è capitato di analizzare recentemente un sistema che, per come mi era stato descritto, raccoglieva i dati dal cellulare, intendendo per dati le conversazioni: trasmetteva come se Internet fosse semplicemente un tubo e queste venivano riversate sul *server* della procura di riferimento. Ebbene, con un'indagine laboriosa e complicata – devo dire che ha richiesto tempo e competenze – siamo riusciti a capire che in realtà i dati non andavano a finire al *server* della procura di riferimento, ma da un'altra parte, in un *server* che, per un certo periodo di tempo, era stato collocato addirittura presso un'azienda esterna. Questa cosa ha suscitato, tra l'altro, molta attenzione anche mediatica, e probabilmente ha costituito il punto di riferimento per cui nella nuova normativa si fa esplicito riferimento – all'articolo 3 – al fatto che non ci debba essere l'impiego di « sistemi informatici interposti di trattazione degli stessi » (dati). Questo è un altro punto: nel mondo digitale non è un dramma che esistano strumenti interposti, l'importante è che siano noti e che si sappia cosa facciano; sono necessari e in un sistema di questo tipo siamo riusciti a capire dove andavano a finire i dati proprio perché non era stata offuscata la rete di acquisizione. Ciò è importante perché ci si può accorgere che c'è un captatore attivo e dove magari sta inviando i dati. Anche in questo caso non si sa come lo strumento funzioni, la descrizione è inadeguata, però, attraverso l'analisi, quando si scopre che le cose funzionano diversamente, ciò crea un momento di difficoltà.

Questo significa che l'effettivo funzionamento di tali strumenti non è noto a nessuno: né alla procura che li richiede né al tecnico che li analizza, perché deve scoprirli attraverso tutta una serie di indagini tecniche. Peraltro, è anche ragionevole, perché le industrie e le aziende che si occupano di questo investono in innovazione, in competenza e in sistemi che necessariamente non potrebbero essere noti a tutti, pena la vanificazione stessa dello strumento. Abbiamo quindi un problema di bilanciamento: da un lato, non possiamo permetterci di non conoscere esattamente come funziona il sistema; dall'altro, occorre anche tutelare chi opera in questo settore.

Sempre richiamandomi al discorso del digitale (quanto al fatto che non si sa cosa fanno i nostri strumenti), il *trojan* è forse l'esempio più adatto: è un sistema che viene installato con l'inganno, di fatto, perché l'utente che a volte se lo autoinstalla, magari indotto da una chiamata del gestore telefonico che gli dice che c'è un problema nella trasmissione dei dati e gli consiglia come agire alla ricezione di un apposito messaggio

per attivare il suo programma, quando lo attiva, quel programma appare essere tutta un'altra cosa: l'icona c'è e se si schiaccia fa qualcosa, ma tutt'altro. Nel frattempo, in maniera del tutto invisibile e nascosta e senza che ci siano tracce di quello che sta succedendo, sta accendendo il microfono, accedendo alla messaggistica e facendo un'altra serie di operazioni assolutamente invisibili.

È importante questo, perché nel mondo reale probabilmente ci accorgeremmo di qualcuno che è entrato in casa e sta trafugando qualcosa, dato che vedremmo che le cose sono state messe fuori posto; nel mondo digitale, questa possibilità non esiste.

Per ultimo, sempre in quest'accezione che spesso si fa fatica a comprendere perché siamo abituati al mondo reale e la fisicità ha un senso, per noi è importante che il *server* stia presso la procura di riferimento; per un tecnico informatico, non importa, i dati si possono mettere sul *cloud* o in qualunque altra parte del mondo; ciò che importa è capire com'è collegato col resto del mondo, chi accede e come accede e quali sono i sistemi di sicurezza che sono stati messi in atto, affinché solo chi ha diritto di accedere possa farlo e chi non ne ha non lo faccia.

Se ci pensiamo un attimo, materialmente la procura che ha un pezzo di ferro all'interno della propria sede, che può fare? Può solo staccare la spina o staccarlo da Internet, ma, una volta che è acceso e attaccato a internet, sa cosa sta facendo quel pezzo di ferro? Evidentemente no, quindi anche questo passaggio della fisicità dev'essere necessariamente superato nel mondo digitale con qualche normativa che comunque descriva altri aspetti che non sono quelli strettamente fisici.

Non credo sia necessario descrivere cos'è il *trojan*, perché credo che lo conosciamo tutti.

PRESIDENTE. No, no: due parole le dica.

REALE. Due parole le dico, allora. Innanzitutto, non sono tutti uguali; alcuni si occupano solamente di accendere e spegnere il microfono e registrare. Anche qui, ci sono piccole differenze tra mondo reale e mondo digitale: nelle normative si parla del fatto che è il *server* presso la procura che deve registrare; con un *trojan* necessariamente chi registra è il telefono o il cellulare, cioè l'applicativo che è stato installato registra sul cellulare, crea i *file* e poi, in un secondo momento, li trasmette opportunamente alla rete, che poi andrà a confluire. A seconda però della tipologia appunto di *trojan*, sono diverse le possibilità di accesso che ha ai dati, quindi non solo può accendere il microfono ed eventualmente la telecamera, ma anche scattare foto e creare video, leggere gli sms e gli mms, accedere addirittura al contenuto della messaggistica istantanea (quindi parliamo di *chat* come WhatsApp e quant'altro) e al GPS (quindi alla geolocalizzazione del dispositivo) e ispezionare i contenuti (quindi vedere le immagini, i video e i documenti presenti), addirittura anche della navigazione su Internet, come le ricerche che sono state fatte.

In alcuni casi, se vogliamo, ancora oltre, laddove il tipo di *trojan* è in grado di acquisire i cosiddetti privilegi di amministrazione del cellu-

lare, può anche modificarlo. Non voglio descrivere questo scenario come reale, ma non può essere escluso che un domani un *software* di questo tipo, che ha accesso in scrittura, possa alterarne i contenuti.

Qual è il problema? Il passaggio successivo è che questo *trojan* può essere rimosso da remoto senza lasciare tracce neanche all'analisi di un tecnico informatico: vi assicuro che a me è capitato di analizzare cellulari su cui avevo il provvedimento del registro delle intercettazioni telefoniche (RIT) con cui era stata autorizzata la captazione, ma non ho trovato tracce nel cellulare stesso, quindi non sapevo esattamente che cos'era stato fatto al suo interno.

Tra l'altro, in questi casi si parla di « *trojan* di Stato », ma in realtà sono aziende private, come dicevamo prima, quindi c'è anche da fare attenzione al fatto che alcune di queste siano addirittura società straniere.

Per rimanere nei tempi che ci eravamo detti, vado agli ultimi punti che mi ero segnato come tecnico. In primo luogo mi sono chiesto quanti captatori sono attivi, anche per avere una statistica e capire come funzionano da un punto di vista operativo. Siccome questi captatori confluiscono nel capitolo delle prestazioni funzionali, che ne comprendono tutta un'altra serie, come le classiche intercettazioni ambientali, audio-video, GPS, le localizzazioni, a livello economico è un capitolo macro, ma a livello di dettaglio non c'è traccia quindi non sappiamo dire a livello centrale quanti sono attivi e per quanto tempo. Alcune procure so che si sono mosse e hanno creato registri appositi, ma sono iniziative autonome, fatte *ad hoc*.

Un primo punto è capire di quale fenomeno esattamente stiamo parlando, perché non abbiamo un tracciamento puntuale (almeno, io non sono riuscito a trovarlo).

Non solo, nel decreto del 28 dicembre 2017, l'articolo 7 proponeva l'istituzione di un tavolo tecnico che avrebbe dovuto costantemente monitorare le prestazioni funzionali sotto il profilo sia economico sia della stessa funzionalità. Questo tavolo doveva essere composto dal Ministero e dai cosiddetti *stakeholders*, quindi anche fornitori di servizi, tecnici, esperti e via dicendo, ma non è mai stato istituito e sarebbe stato decisamente importante dare attuazione a un tavolo di questo tipo, proprio perché potrebbe essere il primo punto dove avere il polso della situazione su una tematica come questa.

Un altro punto che mi sono segnato è che la normativa approvata adesso, a dicembre 2022, prevede tutta una serie di obblighi per i fornitori delle prestazioni, che agli articoli 3 e 4 sono descritti puntualmente. Il fatto è che mancano le verifiche: ci sono gli obblighi, ma chi garantisce che vengano rispettati? Ci sono sempre le autodichiarazioni.

In questo senso, ricordo a me stesso che a casa mia devo far venire un tecnico a controllare la caldaia, scrivere il libretto di manutenzione e mettere un bollino blu, un autovelox dev'essere tarato, altrimenti la rilevazione che fa non ha alcun valore; sembra però che nell'ambito delle intercettazioni non possa esistere un meccanismo analogo di certificazione da parte di un soggetto terzo, che mantenga, da un lato, la tutela

dell'investimento industriale che viene fatto, ma, dall'altro, garantisca a tutti, *in primis* allo stesso pubblico ministero, che il sistema che sta acquistando è conforme proprio agli *standard* di legge che sono stati definiti.

A questo proposito, avevo proprio preso il riferimento di un articolo pubblicato su « Sicurezza e Giustizia » nel 2021 da parte del dottor Giovanni Russo, che è un ex procuratore nazionale antimafia, di cui condividevo ogni parola, perché esponeva proprio questa necessità, cioè rendere le intercettazioni legali là dove c'è la certificazione di un ente terzo estraneo, quindi assolutamente fuori dal processo di costruzione, ma che garantisca questo.

Se questo è un punto importante come certificazione – tra l'altro, in Italia c'è già un primo ente che lo sta facendo secondo gli standard ISO 17020, ma, non essendoci alcun obbligo, ovviamente non c'è un'ampia partecipazione – l'altro aspetto è che, chiarito che lo strumento ha le sue certificazioni, d'altra parte, è importante capire che venga usato nelle modalità previste dalla legge. Per non ritrovarci quindi nella situazione in cui non riusciamo neanche a capire che il cellulare – come mi è capitato – è passato attraverso un captatore, occorrerebbe avere un tracciamento puntuale di tutte le attività che vengono svolte dal captatore in maniera sicura e imm modificabile, affinché venga congelato questo registro di tutto quello che è stato fatto con quel *trojan*, in modo che a posteriori si possa esattamente comprendere come, quando e perché è stato usato e ricostruire, cosa che non è sempre facile.

La cronaca politica la leggete tutti meglio di me, quindi avrete sicuramente notato quante difficoltà ci sono state a ricostruire, perché sono state attivate in certi momenti e non in altri le captazioni e via dicendo.

Ecco questi sono i punti che mi ero rappresentato per rimanere tempi indicati.

PRESIDENTE. Se ci sono intanto commissari collegati, mi facciano presente se vogliono fare domande, perché ho già stilato un elenco.

ZANETTIN (*FI-BP-PPE*). Signor Presidente, ringrazio l'ingegner Reale perché ci ha aperto un mondo che potevamo intuire, ma di cui non avevamo mai avuto cognizione. Siamo tutti certamente non nativi digitali e siamo entrati in questi mondi con difficoltà; evidentemente, le cose che ci ha detto non esito a definirle agghiaccianti nel senso che da cittadino, oltre che da avvocato e da parlamentare, non può che spaventare un utilizzo solo apparentemente regolamentato di meccanismi così complessi.

In questo momento intanto le chiedo se lei, che è molto esperto, può darci qualche suggerimento, magari attraverso una nota successiva, su eventuali integrazioni normative che per certi versi possono sfuggirci. Noi, infatti, percepiamo solo la superficie di questo problema, mentre in realtà lei ha sottoposto alla nostra attenzione questioni molto diverse, perché, come ci ha detto, i sistemi sono diversi, hanno modalità di utilizzo diverso, sono in continua evoluzione, quindi c'è difficoltà proprio a capire cosa viene usato.

Un dato che lei ha segnalato e che ora sottopongo alla Presidente riguarda l'inerzia di un tavolo tecnico da parte del Governo, che doveva essere istituito, ma non è stato creato. Forse questa Commissione ha anche il senso di supplire a questa inerzia: noi non potremo creare esattamente un tavolo tecnico, ma certamente se il Governo non ci ha pensato o non ne ha avuto il tempo, magari noi in questa nostra indagine conoscitiva potremmo approfondire, per esempio, quanti captatori informatici sono stati utilizzati e quanti sono utilizzati attualmente. Questo è un dato che come Commissione potremmo chiedere nell'ambito di questa nostra indagine conoscitiva; sarebbe molto significativo per avere un'idea di cosa sta succedendo nel nostro Paese e credo che anche l'opinione pubblica abbia interesse a capire.

La domanda vera e più facile è la seguente: che garanzia di genuinità abbiamo rispetto ai dati che possono essere acquisiti nei procedimenti giudiziari, alla luce delle problematiche che lei ha espresso? Abbiamo questa garanzia? Nel mondo del *web* esiste infatti la possibilità di manipolare i dati, tanto che lei a un certo punto ha detto che non possiamo escludere che si riesca ad intervenire all'interno con i privilegi di amministratore di sistema (lei ha dato una spiegazione, ma io mi esprimo in modo atecnico) per praticare delle alterazioni. Noi sappiamo che, almeno dal punto di vista mediatico, in alcune inchieste si è avuta l'impressione che il captatore sia stato acceso e in certe ore spento secondo logiche non sempre spiegabili e che siano stati identificati alcuni soggetti e non altri. Certamente può esserci stato un problema tecnico, ma non si può neanche escludere *a priori* che ascoltare una certa conversazione, o identificare un certo soggetto, sia stata una scelta investigativa. Il tema principale è proprio questo: la genuinità dei dati acquisiti che poi hanno effetti dirompenti sulla vita e anche sul buon nome di un soggetto indagato con questi strumenti.

SCARPINATO (*M5S*). Signora Presidente, la mia domanda è la seguente: tenuto conto che le società che noleggiavano i *server* e gli strumenti che servono per le intercettazioni appartengono a privati, il personale di queste società è in grado di conoscere i contenuti digitali sonori delle intercettazioni?

Le faccio questa domanda perché ho fatto una veloce ricognizione e mi sono accorto che vi sono stati dei casi eclatanti di fughe di notizie durante il segreto delle indagini, che erano state causate da titolari di queste società. Mi riferisco, per esempio, alla famosa conversazione tra Fassino e Consorte, quando Fassino era segretario dei Democratici di Sinistra e, parlando con l'amministratore delegato di Unipol, ha fatto il seguente commento: « Abbiamo una banca? ». C'è una sentenza definitiva della Cassazione che ha condannato il titolare della società di noleggio, perché era stato lui a dare a Silvio Berlusconi (questo è scritto nella sentenza della Cassazione) la notizia, che era stata poi pubblicata sul quotidiano « il Giornale ». In questi giorni c'è la notizia di un altro processo, questa volta conclusosi con sentenza assolutoria, in capo al titolare di

un'altra società di noleggio, che pure si è scoperto avere un *server* che era sfuggito alla ricognizione.

PRESIDENTE. Se c'è assoluzione magari non diamo notizia del nome.

SCARPINATO (M5S). Certo. C'è l'assoluzione perché non c'era il dolo, però si è scoperto.

PRESIDENTE. Capisco che per lei è una grande sconfitta, ma prendiamone atto.

SCARPINATO (M5S). Resta il fatto che questo canale non era conosciuto e che i suoi contenuti potevano essere leggibili e conosciuti dai titolari di questi servizi, pertanto il problema esiste. C'è un modo per impedire che chi gestisce questi strumenti possa conoscere i contenuti intercettati? Se non c'è, possiamo pensare di istituire delle società di Stato, che magari acquistano la tecnologia dai privati, ma che poi gestiscono in proprio dei *server* che non siano assolutamente permeabili?

In secondo luogo le vorrei chiedere se lei, in base alla sua esperienza, sa che tipo di tecnologia utilizzano i nostri Servizi segreti. Esiste, infatti, una normativa che consente ai Servizi segreti civili e militari di ottenere delle intercettazioni senza fare alcun riferimento ad alcun reato, che non vengono controllati da nessun giudice. Le chiedo se lei sa se utilizzano strumenti propri o strumenti gestiti da privati; inoltre, poiché queste intercettazioni non vengono distrutte alla presenza di un giudice che si assume la responsabilità, le chiedo se esiste la possibilità di conservare una copia digitale di tutte le intercettazioni fatte, al di là degli adempimenti formali.

SCALFAROTTO (Az-IV-RE). Signor Presidente, vorrei rivolgere al nostro audito due domande molto tecniche. Dato che nei nostri telefonini c'è tutto, dal conto corrente, alle foto della fidanzata, a dove si è andati in vacanza, vorrei capire se tecnicamente sarebbe possibile stabilire *a priori* che un captatore di questo genere possa essere utilizzato solo se tarato in modo da non entrare all'interno di una serie di applicazioni. Mi riferisco, cioè, a un modello per il quale si preveda che si possono sentire le telefonate, ma non si può andare a vedere se si ha l'amante; sarebbe del tutto legittimo, giacché sono affari personali. Posso quindi immaginare che ci sia una sorta di customizzazione dello strumento, in modo tale che all'autorità giudiziaria venga consentito soltanto di accedere a certe cose e possiamo verificare che poi questo succeda?

Il captatore, il cosiddetto *trojan*, è una sorta di cimice semovente; vorrei capire se è tecnicamente possibile customizzare di nuovo questo captatore, per esempio con il GPS, per evitare che sia utilizzato in alcuni luoghi fisici. Mi riferisco in particolare al Parlamento della Repubblica, dove nessuno sarebbe mai autorizzato a mettere una cimice all'interno di

un ufficio o di un'Aula. Qualora, ad esempio, la Presidente in questo momento decidesse di segretare questa seduta, ma il telefonino dell'ingegnere avesse un captatore, la decisione della Presidente di segretare l'audizione sarebbe posta nel vuoto. Nessuno può mettere una cimice nel mio ufficio al Senato, ma se il mio visitatore viene e ha con sé una cimice, io poi me la ritrovo nell'ufficio; pertanto vorrei capire se, per esempio attraverso il GPS, si può fare in modo di disegnare tecnicamente il captatore in modo da evitare il più possibile la sua utilizzazione illegittima o illegale.

RASTRELLI (*FdI*). Signora Presidente, in realtà il tema che vorrei trattare è lo stesso che ha sollevato il senatore Scalfarotto. Intendevo fare due domande in supplemento all'ingegnere.

In primo luogo vorrei chiedere come viene inoculato il *trojan*, se deve essere extra-oculato o se rimane all'interno del dispositivo.

Secondo. Il *trojan*, una volta introdotto all'interno di un dispositivo digitale e una volta che sia riuscito a infettarlo, può contenere potenzialmente qualunque tipo di « istruzione maligna »? È lo stesso concetto di quali funzioni fisicamente può attivare sul dispositivo infettato.

Terzo. In funzione della sua esperienza diretta con specifico riferimento al « *trojan* di Stato », cioè di inoculazioni autorizzate dall'autorità giudiziaria, con una verifica informatica digitale *ex post* sul dispositivo infettato, in che limiti lei o i tecnici informatici siete riusciti ad avere accesso, come quantità e qualità, alle informazioni raggiunte dal *trojan*?

PRESIDENTE. Vorrei porle anche io due domande. Da quello che ho capito il captatore, in alcuni casi, potrebbe anche trasformare il contenuto di ciò che capta, il che significa che in astratto, se ciò fosse possibile, si potrebbe inventare un mio messaggio che io non ho mai mandato. Premesso questo, se è possibile questa attività di trasformazione, poi rimane traccia dell'eventuale attività di trasformazione? Cioè si riesce a ricostruire che il messaggio è stato inventato e creato artificialmente oppure non c'è traccia della manipolazione?

Seconda domanda. Mi sembra che lei stia spiegando che questi captatori presentano caratteristiche totalmente diverse rispetto alle normali intercettazioni e che quindi probabilmente richiederebbero un tipo di disciplina diversa rispetto a quella delle intercettazioni. La pregherei di rispondere, anche brevemente, un po' a tutte le nostre curiosità.

SALLEMI (*FdI*). Mi scusi, Presidente, vorrei chiedere solo un chiarimento, stimolato proprio dal suo intervento. Nel momento in cui ritengo o suppongo che un messaggio sia stato alterato, proprio per quello che diceva il Presidente, oltre al fatto di capire se vi fosse realmente la possibilità di sapere se è stato alterato, quanto costerebbe a un cittadino, intercettato e incappato in questa rete di spionaggio assurdo, riuscire a dimostrare tecnicamente che quel messaggio è stato alterato? Qual è la competenza specifica che possa riuscire a fare questo, per esempio in un

processo penale in cui io debba dimostrare che qualcuno ha alterato una comunicazione all'interno del mio telefonino?

REALE. Innanzitutto non volevo essere un terrorista nell'esposizione, ma ritengo sempre che sia meglio preoccuparsi un po' di più che un po' di meno, anche perché – questa è sicuramente la mia esperienza personale e già parzialmente risponde a diverse domande – non ho avuto mai nessuna indicazione diretta, attraverso le varie analisi che ho fatto (e ne ho visti diversi di *trojan*), che ci sia stata una manipolazione di qualche tipo o un utilizzo improprio in maniera diretta. Questo non mi è capitato. Mi sono capitate però tantissime situazioni che potenzialmente facevano capire la possibilità esistente. Faccio un esempio: c'è un procedimento in corso su uno di questi *trojan*, in cui i dati venivano conservati addirittura su un *server* di Amazon in Oregon. Quindi potenzialmente, se qualcuno sapeva come muoversi, poteva in teoria andare a prendere tutti i dati che venivano intercettati (sapendo come muoversi). Ma non è successo, quindi è più una questione in potenza. Stiamo già vedendo il verificarsi di tante situazioni in cui il problema non è il dolo, ma problematiche tecniche non gestite adeguatamente. Potete facilmente immaginare che le aziende private che lavorano in questo settore, incalzate continuamente dalla necessità di essere al passo con i tempi, al passo con i sistemi e in grado di intercettare praticamente qualunque cosa, hanno la necessità di muoversi con delle dinamiche che magari a volte non riescono a contemplare la messa in sicurezza di qualunque aspetto. E questo preoccupa di per sé. Questo mi richiama – ma lo farò in tanti altri punti, nelle varie risposte – all'importanza di avere una certificazione, che non sarà certamente risolutiva, ma intanto ci dà una piattaforma comune in cui si richiedono una serie di requisiti di base che consentono almeno di escludere l'incuria, l'errore e la mancata attenzione. Il dolo rimane sempre da un'altra parte, evidentemente.

Senatore Zanettin, sicuramente preparerò una nota scritta *a latere*, in cui non solo rappresenterò quello che ho avuto modo di dire, ma anche le mie risposte; sicuramente metterò a disposizione il materiale e le cose che ho detto.

Per quanto riguarda la genuinità dei dati e quindi la garanzia dei dati acquisiti e se esiste la possibilità di manipolarli, dicevo che potenzialmente questa possibilità esiste. Nella pratica – ripeto – non ho avuto occasione di riscontrare nessuno di questi fenomeni. La preoccupazione semmai è che, poiché il mondo digitale è in continua evoluzione, quando una cosa è possibile farla prima o poi qualcuno la farà; questo è un po' la regola generale.

Il senatore Scarpinato parlava delle società private di noleggio, chiedendo se possono essere in grado di conoscere i contenuti digitali. Sì, la fuga di notizie e la sentenza che lei ha citato dimostrano che è possibile. Anche qui una certificazione *ad hoc* potrebbe consentire di verificare che queste modalità non siano neanche possibili, perché tecnicamente si può. Lei chiedeva se si può impedire che i contenuti intercettati possano es-

sere ascoltati e letti: tecnicamente si può. Già oggi abbiamo a disposizione, nei nostri dispositivi, dei canali di messaggistica che creano delle chiavi di criptazione che fanno sì che solo il mittente e il destinatario riescano a decodificare il messaggio.

PRESIDENTE. Il senatore Scarpinato chiede se attualmente le società private hanno questa criptazione.

REALE. No, in questo momento non c'è; ma si può fare. Quello che mi è capitato di vedere nei sistemi è che l'audio era sostanzialmente in chiaro. Veniva trasmesso lungo un canale di trasmissione criptato ma, nel momento in cui era depositato, tornava a essere in chiaro e quindi era possibile ascoltarlo. Però lo si può impedire.

Per quanto riguarda la possibilità di accentrare tutto in una società di Stato, questa possibilità si scontra con problematiche di altra natura, che sono quelle che conosciamo abitualmente, anche in tanti altri settori. Non c'è nessuna demonizzazione dalla società privata, assolutamente; l'importante è semplicemente che si attenga alle disposizioni e che ci siano degli strumenti di controllo, per quella che è la mia personale visione. Portarle in un'unica società di Stato potrebbe non garantire molte possibilità di acquisizione, dal momento che è un mondo molto veloce quello di queste aziende, che investono in competenze e in tecnologie. Vi faccio solo un esempio: molto spesso, per riuscire ad accedere a un dispositivo e ad acquisire certi privilegi, è necessario in qualche modo (fatevi usare dei termini un po' insoliti) « bucare » alcuni meccanismi di protezione, che sono stati scoperti magari da qualche persona in rete e che li ha messi in vendita in una sorta di mercato nero, in cui chi vuole acquisire quel tipo di informazione la paga e deve necessariamente investire per poter poi sfruttare questa vulnerabilità cosiddetta del sistema al proprio scopo, per costruire il proprio sistema. In questo senso, probabilmente, la soluzione di Stato può non essere la soluzione ideale. Per quanto riguarda invece i Servizi segreti, non ho nessuna informazione e non mi è mai capitato; posso garantire che rimangono segreti, almeno per quanto mi riguarda.

Il senatore Scalfarotto aveva giustamente fatto notare come nel telefono c'è di tutto e chiedeva se è possibile limitare l'utilizzo. Sì, lo si può sicuramente limitare. Alcuni di questi *trojan* si occupano solo di attivare e disattivare il microfono, quindi siamo sicuri che questo è l'unico tipo di ascolto; nel caso, la scoperta dell'amante avviene solo perché ci parla, eventualmente, ma non perché gli ha mandato una foto o per un altro motivo. Quindi sì, esiste la possibilità di limitare il *trojan*, laddove appunto è costruito per utilizzare e accedere solo a certe risorse del telefono.

Per quanto riguarda le possibilità di verifica, di solito si riesce comunque a capire cosa fa il *trojan*, perché nel telefono rimangono tracciate le cosiddette autorizzazioni, quelle che poi spesso capitano a ognuno di noi quando si installa una *app*, che chiede l'autorizzazione al-

l'uso del microfono, all'accesso alle immagini o alla macchina fotografica. Queste autorizzazioni rimangono tracciate, quindi si vede almeno dove l'applicazione poteva accedere. Una limitazione comunque è tecnicamente possibile.

Quanto al fatto che sia una cimice semovente e quindi può andare dappertutto, se in questo momento il mio cellulare fosse effettivamente intercettato – mi auguro di no – si potrebbe usare sicuramente il GPS per definire delle aree di non copertura, posto che comunque anche il GPS ha i suoi limiti, se non è attivo non è neanche in grado di capire esattamente la posizione. Per questo può essere importante il tracciamento di cui parlavo prima, perché avere sempre la lista di tutte le attività che sono state svolte con quel *trojan* può comunque *a posteriori* consentire di capire se era stato acceso e dove era stato acceso. *Ex post* il tracciamento potrebbe sopperire facendoci capire cosa è successo veramente, *ex ante* invece il GPS può non essere risolutivo, ma sicuramente può aiutare a limitare tutta una serie di casistiche.

Il senatore Rastrelli chiedeva come può essere inoculato il *trojan*, se può contenere anche funzioni maligne. Effettivamente sì, sempre in linea potenziale, ma appunto per questo la certificazione può aiutare a comprendere se il prodotto fa esattamente quello che deve fare. Per quanto riguarda l'inoculazione, esistono diverse modalità. Non sempre è possibile inoculare qualunque tipo di *trojan* in qualunque tipo di telefono, ci sono talmente tante casistiche che il listino prevede anche la possibilità che l'inoculazione non vada a buon fine, quindi può essere complicato sotto questo punto di vista. Quello che sicuramente richiede – questa è una mia personale riflessione che vi consegno – è l'inganno: la persona viene ingannata perché le viene inibito l'accesso alla rete dati e quindi viene in qualche modo spinta ad autoinstallarsi il *trojan* e questo lo trovo sempre una cosa un po' curiosa, perché di fatto significa avere una complicità dello stesso ascoltato, come è avvenuto in moltissimi casi di quelli che mi è capitato di conoscere.

Per quanto riguarda le inoculazioni autorizzate con la verifica *ex post*, in alcuni casi siamo riusciti ad avere accesso alle informazioni del *trojan*, in altri casi non siamo riusciti neanche a vedere che era passato di lì il *trojan*, quindi se non c'è un tracciamento previsto dalla normativa che imponga che si sappia esattamente cosa è passato, cosa ha fatto, quando e in che modo, potrei trovarmi, come tecnico forense, pur avendo fisicamente in mano il telefono che è stato intercettato, a non essere in grado di ricostruire non solo che cosa è stato fatto, ma addirittura, in alcuni casi, che c'è stato un *trojan*.

Il presidente Bongiorno chiedeva se è possibile trasformare il contenuto e, nell'eventualità, se rimarrebbe traccia di questo. Come dicevo prima, innanzitutto stiamo parlando di ipotesi del tutto astratte, ma sappiamo che oggi esistono i *deep fake*, che per chi non lo sapesse sono tecnologie che, anche attraverso l'uso dell'intelligenza artificiale, consentono di manipolare l'immagine e l'audio, magari facendo apparire sovrainpressa all'immagine del mio volto quella del viso di un attore o alla

mia voce quella di un doppiatore. Spesso è capitato nel programma televisivo « Striscia la notizia » di vedere esempi di questo tipo, che sono effettivamente molto realistici. Ora, col passare del tempo, sarà sempre più possibile con la tecnologia accedere a questo tipo di situazioni. Potenzialmente, quindi, è possibile trasformare il contenuto, il problema è che non è detto che si possa poi rilevare la traccia di questo. A maggior ragione, certificazione e tracciamento rimangono gli unici strumenti a livello base per poter prevenire da una parte, e poi verificare *a posteriori* come è stato usato il prodotto.

Quanto alla diversa disciplina delle intercettazioni per la tipologia del captatore informatico, è evidente che quello è uno strumento completamente diverso dalla classica intercettazione telefonica, con cui non ha niente a che vedere; è uno strumento invasivo che va a toccare praticamente tutti gli aspetti della nostra vita, perché oggi effettivamente il nostro cellulare contiene qualunque informazione relativa ai nostri appuntamenti o ai nostri figli, quindi sicuramente una disciplina diversa sarebbe auspicabile proprio per questo motivo.

Infine, quanto al costo eventuale per un cittadino di verificare un'altezza, devo premettere che potrebbe non essere neanche possibile *a posteriori*, anche perché io stesso ho incontrato delle difficoltà. Mi richiamo all'esempio che ho fatto inizialmente, in cui l'azienda aveva segnalato che i dati venivano presi dal cellulare e, attraverso il tubo, andavano a finire sul *server* della procura. Io ero consulente di parte di un imputato, ci è stato detto che così era e quindi quella era la verità. Ebbene, l'attività è costata mesi di lavoro, ovviamente sono stato costretto anche a far pagare economicamente tutto questo e siamo riusciti, non solo per la competenza, ma anche per certe soluzioni forse tecnicamente non perfette e anche con un po' di fortuna, a individuare e capire che i dati andavano a finire in un *server* diverso. Non è stato facile, anzi è stato difficile, costoso e anche fortuito, quindi il punto è che effettivamente questa dimostrazione tecnica potrebbe non essere accessibile per i cittadini.

PRESIDENTE. Ingegnere, la ringraziamo per il suo contributo. Considerato che molti passaggi del suo intervento avevano natura tecnica e hanno suscitato interesse da parte della Commissione, le chiedo, se possibile, di farci pervenire una nota tecnica ma accessibile anche a persone che non hanno delle conoscenze specialistiche, che potrebbe essere oggetto di approfondimento da parte dei commissari.

REALE. Preparerò sicuramente questa nota e la metterò a disposizione della Commissione.

PRESIDENTE. Dichiaro così concluse le audizioni odierne.
Rinvio il seguito dell'indagine conoscitiva ad altra seduta.

I lavori terminano alle ore 10,40.